LOGIX ACADEMY
Learn from PhDs

STUDY NOTES

Cyber Security
From Beginner to Expert

Supporting Notes

Supplement the learning process with these study notes

PRESENTED BY
Dr. Usman Ashraf

https://t.me/learningnets

FOUNDATIONS

NETWORK SECURITY

CYBER ATTACKS

WEB APPLICATION SECURITY

MALWARE

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

Connect with us for discussions and Course Updates

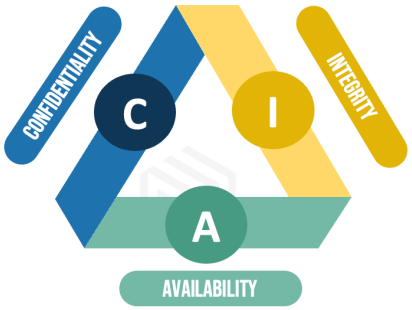
Join Today

Join Today

Join Today

https://t.me/learningnets

The CIA Triad



Confidentiality

- Ensuring data is accessible only to authorized users
- Primarily enforced through encryption techniques
- Common violations: packet sniffing, breaking encryption, unintentional human errors

Integrity

- Ensures the accuracy and completeness of data
- Assurance that data has not been improperly modified or omitted
- Enforced through the use of hashes
- Violations can occur through unauthorized data modification during transit

Availability

- Data must be available when needed by authorized users
- Achieved through implementing redundancy
- Violations include hardware damage and Denial of Service (DoS) attacks

https://t.me/learningnets

IAM – Identity & Access Management

IAAA: Identification, Authentication, Authorization, Accountability

Concept	Description
Identification	Entity identification without authentication. It involves claiming an identity (e.g., ID badge, camera scans)
Authentication	Verifies identity through methods like passwords, PINs, or biometrics, after identification
Authorization	Determines access levels post-authentication, via control lists or clearances
Accountability	Ensures actions are traceable to entities, through audits and log reviews

Authentication Factors

- Type I (Knowledge): Passwords, PINs
- Type II (Possession): Smart cards, mobile SIM
- Type III (Inherence): Biometrics like retina or fingerprint scans

Multi Factor Authentication (MFA)

- Combines multiple authentication types for enhanced security
- Ranges from single-factor to multifactor setups, improving defense against unauthorized access

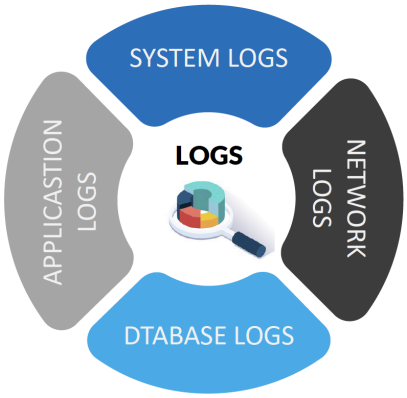
Authorization vs Accountability

Authorization determines who is allowed to perform specific actions, ensuring users have access only to what is necessary for their roles. Accountability, on the other hand, involves logging user activities to hold individuals responsible for their actions. This dual approach enhances security and ensures users' access rights are tightly controlled and monitored.

https://t.me/learningnets

IAM – Identity & Access Management

Need to Know & Least Privilege



The principles of ***Need to Know*** and ***Least Privilege*** limit access and permissions to the minimum necessary for individuals to perform their duties, thereby minimizing potential risks.

- **Need to Know:** Limits access to information strictly necessary for job functions.
- **Least Privilege:** Restricts operational permissions to the least amount needed.

Addressing Privilege Creep

Privilege creep, the accumulation of access rights over time, poses a significant risk. Regular audits and reviews are essential to maintain security.

- Regular audits and privilege reviews to prevent unauthorized access

Accountability Through Audits

Accountability is enforced through regular log and account audits, monitoring all user activities to detect unauthorized actions.

- Log and account audits to trace user activities
- Monitoring tools to detect suspicious activities

https://t.me/learningnets

IAM – Identity & Access Management

Identity Federation

Identity Federation simplifies user access across different systems using a single set of credentials. This approach enhances user experience and security by reducing password fatigue and streamlining authentication processes.

Token Based Authentication

Involves systems like web servers authenticating users through tokens post successful login, facilitating secure requests and responses between the application and the server.

Identity Federation

- Leverages credentials from one account to log onto multiple systems, exemplified by using a Gmail account to access different websites without re-registering
- This avoids the need for multiple accounts and IAM systems, streamlining access management

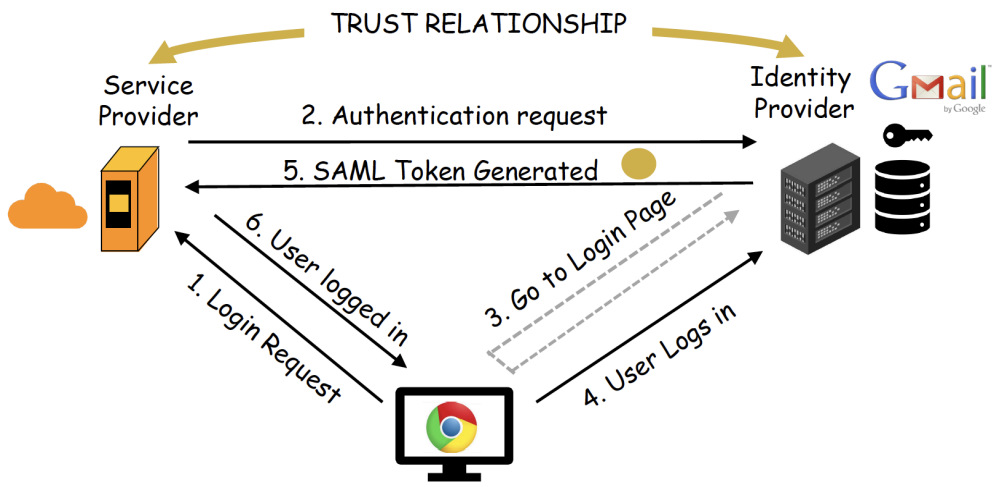
Trust Relationship & SAML Token

Process	Description
Trust Establishment	Between Service Provider and Identity Provider, facilitating authentication requests and SAML token generation
User Authentication	User is authenticated and logged in, allowing access to services

https://t.me/learningnets

Single Sign-On (SSO)

SSO allows users to log in once and access multiple applications within an organizational boundary, simplifying user access within enterprises.



Identity Federation vs. Single Sign-On

While similar, SSO is a subset of Identity Federation, with the latter being broader and spanning across organizations, unlike SSO's intra-organizational focus.

Protocols: SAML, OIDC, OAuth

- **SAML (Security Assertion Markup Language):** Standard for SSO implementations, facilitating authentication between parties.
- **OAuth:** Authorization framework that allows third-party services to exchange web resources on behalf of a user.
- **OIDC (OpenID Connect):** Built on OAuth, providing a standard for SSO implementations.

https://t.me/learningnets

Policies, Standards, and Guidelines

Policies

Policies are organization-wide directives that define the overarching security stance, laying the groundwork for long-term security objectives and responsibilities.

Standards

Standards provide specific rules to achieve the policies' intent, ensuring a uniform approach to implementing security measures.

Procedures & Guidelines

Procedures detail the exact steps needed to comply with the standards, aiming for consistency in security practices. Guidelines offer optional recommendations, enhancing the flexibility of security protocols.

Example: Password Policy

Component	Details
Password Policy	Passwords must be strong, regularly rotated, and securely managed by users.
Password Standard	Minimum of 8 characters, including 2 special characters, changed every 90 days.
Password Change Procedure	Procedure includes logging in, navigating to settings, changing the password, and submitting
Password Guidelines	Recommendations include using a passphrase for strength and avoiding common patterns.

https://t.me/learningnets

Compliance and Intellectual Property

Compliance Overview

Compliance involves adhering to laws, policies, and regulations to protect personal and health information. It includes frameworks like GDPR, HIPAA, and PCI-DSS, each focusing on specific areas of data protection.

Personally Identifiable Information

Information that can be used to identify, contact or locate someone such as:

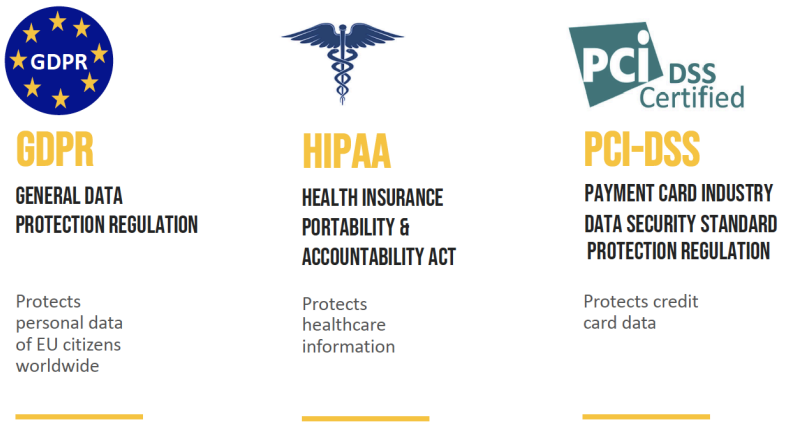
- **Full name**, **driver license number**, **social security number**, **home address**

Intellectual Property (IP) Overview

Intellectual Property (IP) represents creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce.

IP Type	Details
Trademark	Exclusive rights on phrases, symbols, or designs to identify goods/services.
Copyright	Protection for authors of original works, including literary, dramatic, musical, and certain other intellectual works.
Patent	Exclusive rights granted for an invention, providing protection for the invention's use and distribution.

GDPR, HIPAA, PCI-DSS



https://t.me/learningnets

Cryptography

The art of protecting information through encoding, ensuring secure communication.

- **Symmetric Encryption:** Utilizes a single key for both encryption and decryption. Key algorithms include AES, RC5, and Twofish.
- **Asymmetric Encryption:** Involves a public and a private key for secure data exchange and digital signatures.
- **Key Length:** Critical factor in encryption strength - longer keys offer better security.

Symmetric vs. Asymmetric Encryption

- **Use of Keys:** Symmetric uses one key; Asymmetric uses a key pair.
- **Performance:** Symmetric is generally faster; Asymmetric is slower but facilitates secure key exchanges over public networks.
- **Applications:** Symmetric is ideal for bulk data encryption; Asymmetric is used for secure communication and data integrity verification.

Practical Applications

- **Digital Signatures:** Asymmetric cryptography ensures the authenticity and integrity of a message.
- **Secure Key Exchange:** Asymmetric methods like Diffie-Hellman allow for the secure exchange of encryption keys.

Advanced Encryption Standard (AES): A widely adopted symmetric encryption algorithm with key lengths of 128, 192, and 256 bits

Symmetric Encryption	Asymmetric Encryption
Same key used for encryption and decryption	Different keys (a private and public) used for encryption/decryption
Encryption and decryption algorithms are the same	Different encryption and decryption algorithms are used
Cannot always exchange keys safely	Can be done even on public networks
Fast	Slow
Smaller key size offers strong encryption	Longer keys required to ensure strong encryption

https://t.me/learningnets

Hashing & Digital Signatures

Hashing

Hashing involves creating a unique, fixed-size summary (message digest) from input of any size. Key characteristics include:

- Uniquene output for each input
- one-way (cannot retrieve the original document from its hash)

Hashes play a vital role in ensuring file integrity during internet transfers.

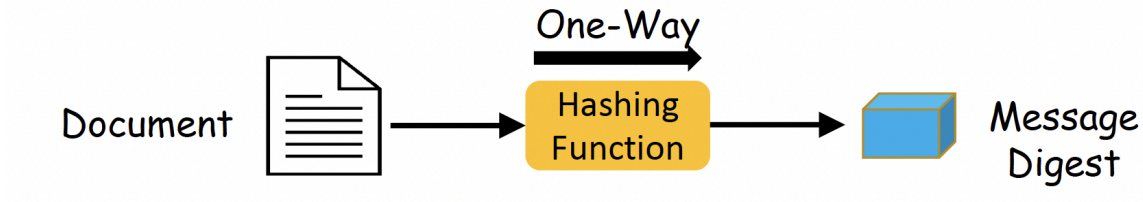
Digital Signatures

Digital signatures utilize a private key to sign a file hash, ensuring the message's authenticity:

- Recipients use the sender's public key to verify the signature, which confirms the message's origin and integrity
- This process not only authenticates the source but also can add an additional layer of confidentiality through encryption.

Popular Hashing Solutions

The handbook reviews various hashing algorithms, including MD5 and SHA-2. It notes MD5's vulnerability to collisions and describes SHA-2's variants (SHA-224, SHA-256, SHA-384, SHA-512) to highlight a progression towards more secure hashing methods.



https://t.me/learningnets

NETWORK SECURITY

https://t.me/learningnets

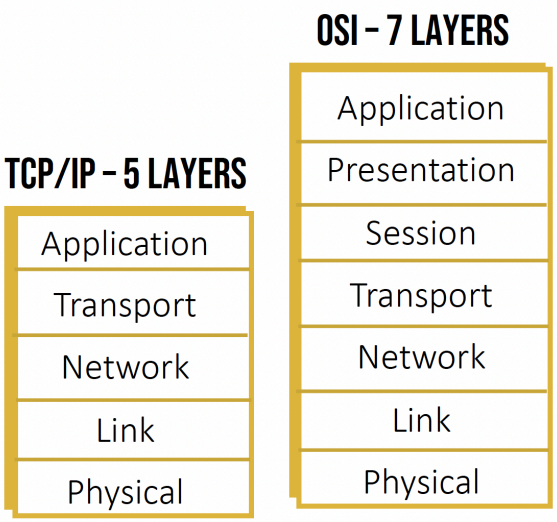
OSI and TCP/IP

Introduction

The OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/ Internet Protocol) models are foundational frameworks for understanding network architecture. The OSI model is a theoretical framework that defines network communication in seven layers, while the TCP/IP model is the practical standard used in today's Internet, with a more concise four-layer structure.

Key Points

- OSI model provides a theoretical framework for understanding network communication across different network functions, offering flexibility in the implementation of networks.
- TCP/IP model, being the de facto standard for modern internet communications, emphasizes a practical approach to packet transmission across the internet.
- Both models emphasize the importance of a layered approach, allowing for the abstraction, segmentation, and independent management of network communication processes.



https://t.me/learningnets

Application and Transport Layers

Application Layer Overview

- Web pages consist of objects like images, text fields, videos, and are essentially HTML pages
- HTTP (Hyper Text Transfer Protocol) is used for web browsing, fetching HTML files and objects, relying on TCP

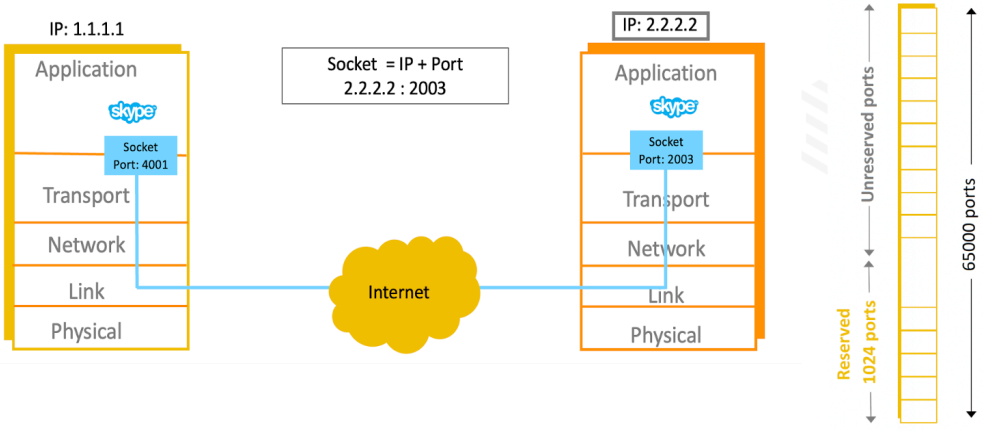
Transport Layer Overview

- TCP (Transmission Control Protocol) offers reliable, ordered delivery, essential for web browsing, file transfers, and emails
- UDP (User Datagram Protocol) allows for unreliable, unordered delivery, suitable for multimedia applications like video streaming and audio calls

Feature	TCP	UDP
Delivery	Reliable/Ordered	Unreliable/Unordered
Use Cases	Web browsing, Emails, File Transfers	Video streaming, Audio calls
Speed	Slower due to ACKs	Faster, tolerates losses

Sockets and Ports

- Sockets are identified by IP address and port number, facilitating communication between devices over a network
- Port numbers range up to 65535, with the first 1024 reserved for specific protocols (e.g., HTTP, FTP, SMTP)



https://t.me/learningnets

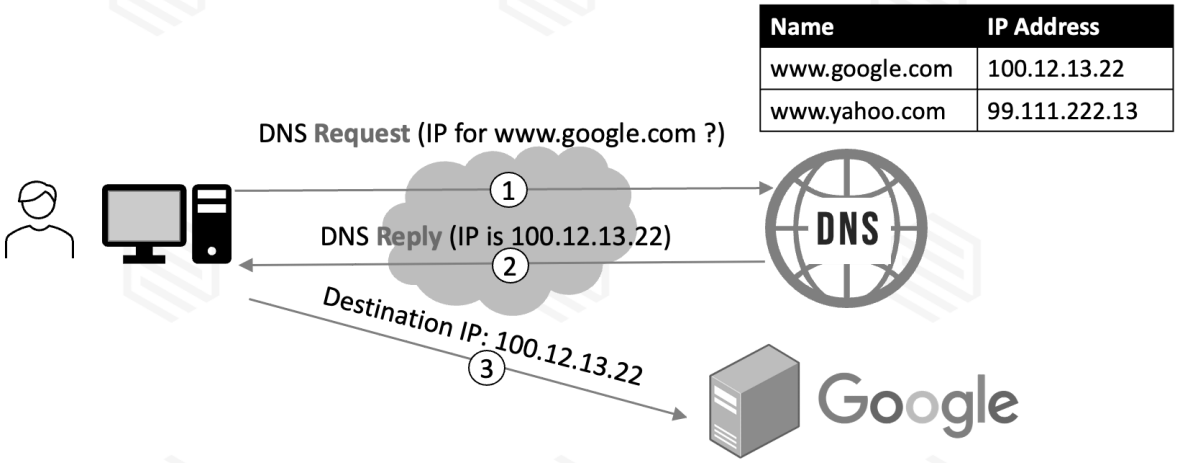
DNS (Domain Name System)

Introduction to DNS

- DNS (Domain Name System) translates human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 12.13.11.12), allowing users to access internet resources by name instead of IP address
- DNS queries use UDP for communication to minimize TCP overhead, with lost queries simply retransmitted

DNS Operation

- A DNS request initiates a query for the IP address of a domain name, leading to a DNS reply providing the corresponding IP
- The process demonstrates the client-server interaction in the DNS resolution process, where a DNS server responds with the IP address for a requested domain name



DNS Server Hierarchy

- DNS relies on a hierarchical system of servers to distribute the load and manage the domain name resolution process efficiently
- This hierarchy includes root DNS servers, top-level domain (TLD) servers, and authoritative DNS servers, each playing a specific role in the domain name resolution process

https://t.me/learningnets

Network Layer

Introduction to Network Layer

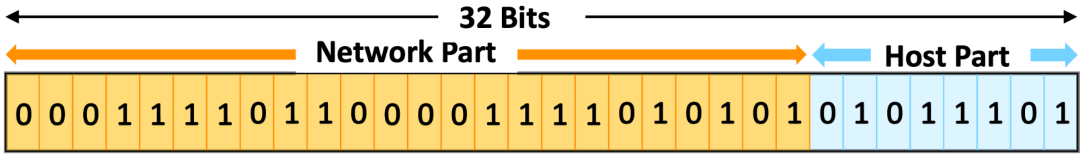
- The network layer is crucial for routing packets across different networks, using IP addresses to identify source and destination
- It employs protocols like IP for packet forwarding and ICMP for error reporting and operational queries

IP Protocol

- Internet Protocol (IP) routes packets from source to destination, supporting both IPv4 and IPv6 addressing schemes
- IP is connectionless, meaning no established connection is required between endpoints for data transmission

IP Addresses

- IP addresses are unique identifiers for devices on a network, divided into public and private addresses, with special ranges for each
- Addresses are categorized into classes (A, B, C) based on the network and host portions



ICMP Protocol

Internet Control Message Protocol (ICMP) is used for error reporting and operational inquiries, such as ping and traceroute commands:

- Used for Error reporting
- Major use of ICMP: Ping and Traceroute

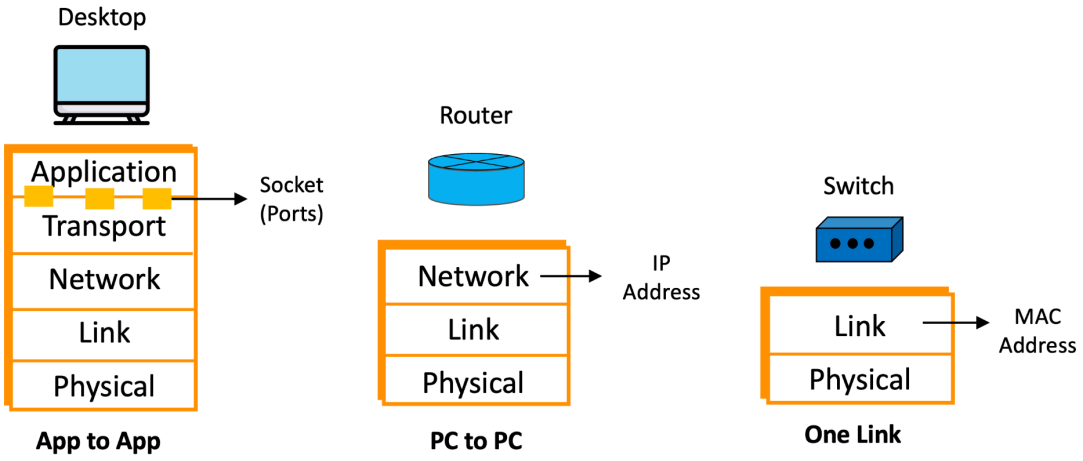
https://t.me/learningnets

Link Layer

Introduction to MAC Layer

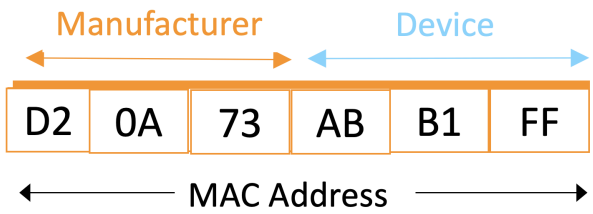
The Link Layer is a fundamental block in network communication, ensuring data packet delivery across a single physical link:

- It utilizes MAC addresses for device identification
- It employs a 12-digit hexadecimal format
- MAC addresses are burned onto devices, like Network Interface Cards (NICs)
- Network layer handles end-to-end routing while link/mac layer handles links



MAC Addresses / Physical Addresses

- 12-digit (48-bits) Hexadecimal Format
- Burned onto the device e.g. Network Interface Card
- MAC addresses can generally not be changed



https://t.me/learningnets

Security Protocols

HTTPS

Ensures secure communication over the internet by encrypting data, making it crucial for protecting user information. It transforms HTTP data transmission from plaintext to a secure encrypted format.

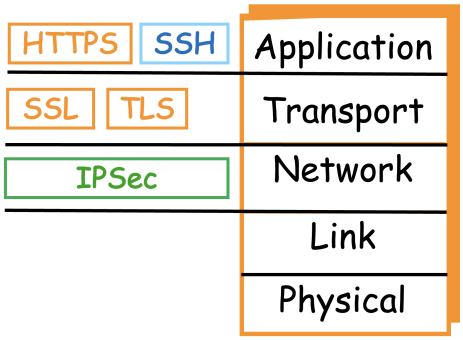
SSL/TLS

Acts as the backbone for secure internet communication, with TLS as the updated, more secure version of SSL. These protocols encrypt data transfers, providing confidentiality and integrity between client-server communications.

IPSec

Operates at the network layer to encrypt and secure IP packets, widely used in VPNs to create secure tunnels over public networks, offering comprehensive security features including authentication, integrity, and confidentiality.

- Application: HTTPS, SSH
- Transport: SSL/TLS
- Network: IPSec



- HTTPS combines HTTP with SSL/TLS to encrypt web traffic.
- SSL/TLS secures data transfers, with TLS using port 443 by default.
- IPSec encrypts at the network layer, ideal for secure VPN connections.

https://t.me/learningnets

Port Scanning

NMAP is an important tools in PenTester's armor and identifies:

- Open Ports
- Services running on those ports e.g., Telnet (23), SQL (1433)

Popular ports:

FTP	SSH	Telnet	SMTP	DNS	HTTP	HTTPS	SQL
21	22	23	25	53	80	443	1433

Types of Port Scans:

- TCP/UDP Port Scans
- Stealth Scans

Key Commands:

- `nmap [target IP]` for common ports
- `nmap -p- [target IP]` for all ports
- `nmap -O [target IP]` for OS detection

https://t.me/learningnets

Network Address Translation

NAT Overview:

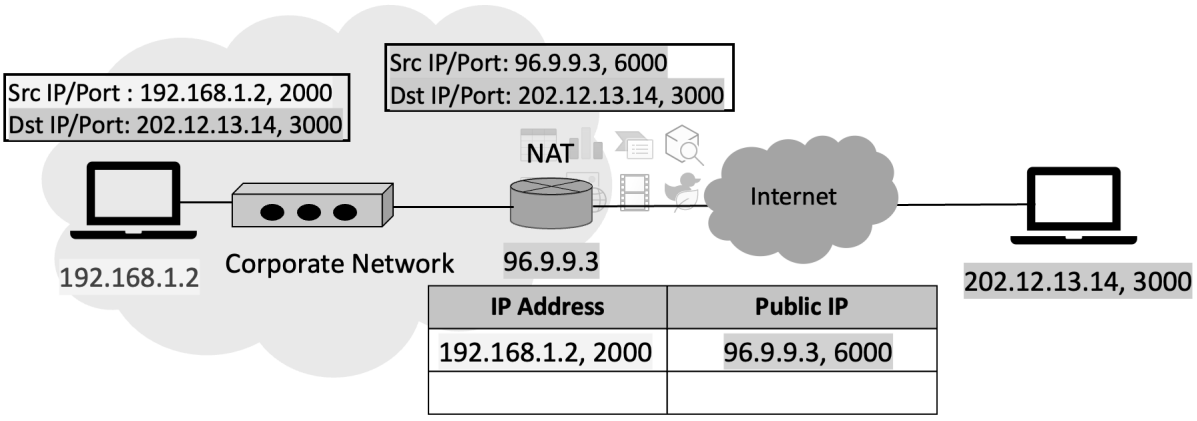
- Allows multiple devices on a private network to access the internet using one public IP address
- Enhances security by hiding internal IP addresses from the external network

Key Points

- **Static NAT**: 1-to-1 mapping, one public IP to one private IP.
- **Dynamic NAT**: Maps multiple private IPs to a pool of public IPs, based on availability.
- **PAT (Port Address Translation)**: Multiple private IPs are mapped to a single public IP but differentiated by port numbers.

Benefits

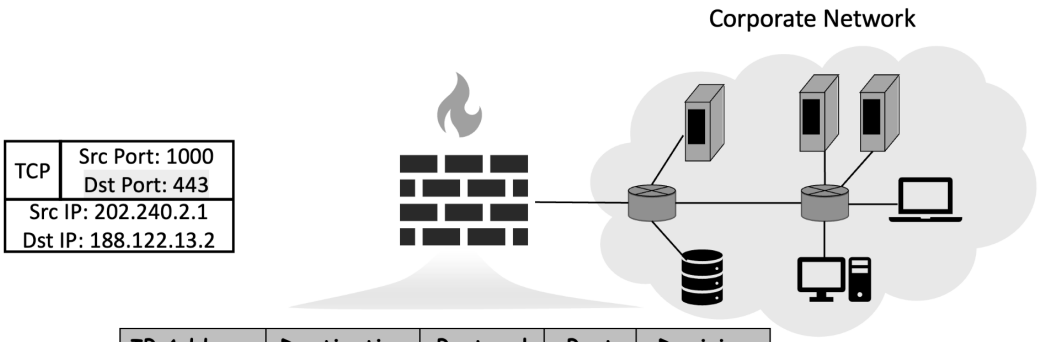
- Efficient use of public IP addresses
- Protects internal network structure by keeping private IP addresses hidden



https://t.me/learningnets

Firewalls

- Function as the primary defense against external threats
- Can be software, hardware, or a combination
- Differentiate between host-based and network-based types



IP Address	Destination	Protocol	Port	Decision
202.240.2.1	ANY	TCP	443	ALLOW
102.110.2.1	ANY	TCP	80	DENY

Operations and Types

- Utilize Access Control Lists (ACLs) to allow or block traffic
- Criteria for rules include IP addresses, ports, and protocols

Host-based vs. Network-based

- Host-based: Protects individual devices, often software-based
- Network-based: Secures an entire network, typically hardware-based

Stateless vs. Stateful

- Stateless: Filters packets based on individual rules without context
- Stateful: Monitors ongoing connections for informed decision-making

Next-Generation Firewalls

- Operate at the application layer, incorporating Deep Packet Inspection
- Capable of specific application controls and enhanced intrusion prevention

https://t.me/learningnets

Wireless LAN (WLAN) Security

Challenges

- Unauthorized access via rogue APs
- Eavesdropping on wireless traffic
- MAC address spoofing

Security Measures

- SSID Hiding: Prevents the broadcast of network name
- MAC Filtering: Allows only known devices to connect
- Encryption: WEP (less secure), WPA-TKIP, and WPA2-AES (most secure)

Protocols Comparison

- WEP: Basic encryption, easily bypassed
- WPA: Improved security with TKIP, stronger than WEP
- WPA2: Uses AES, currently the most secure standard

WEP	WPA	WPA2
Short Keys	Relatively longer keys	Relatively longer keys
Weakest Security	Weak security	Strong security
Static Key	Dynamic Session Key	Dynamic Session Key
RC4	RC4	AES

https://t.me/learningnets

CYBER ATTACKS

https://t.me/learningnets

Password Attacks

This summary provides an overview of key concepts and best practices for mitigating password attacks, focusing on brute force and dictionary attacks.

Brute Force Attacks

- Tries all possible combinations to guess passwords, influenced by password length and character types
- Passwords are hashed and never stored in plaintext, making recovery from hashes impossible
- Less effective online due to account lockout policies and slow processing; more feasible offline with access to database copies
- Use of rainbow tables for pre-computed hashes, though mitigated by salting

Dictionary Attacks

- Utilizes common words or phrases, significantly reducing the time to discover a password
- People often use easily guessable passwords, making dictionary attacks effective

Best Practices for Protection

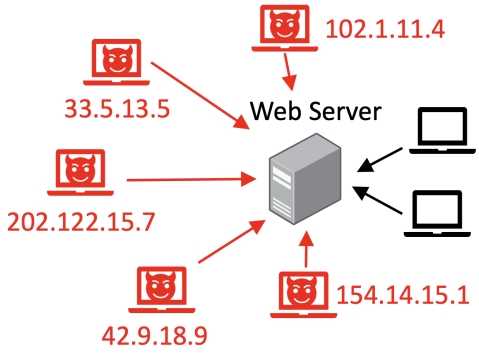
Strategy	Details
Account Lockout	Lock account after X unsuccessful attempts
Force Captcha	Require captcha after Y unsuccessful attempts
Password Policies	Enforce creation of long, complex passwords
Database Encryption	Secure stored data to prevent unauthorized access
Salt	Add random data to hashes to counteract rainbow tables

https://t.me/learningnets

DoS and DDoS Attacks

Overview

- Denial of Service (DoS) makes services slow/unavailable
- Distributed DoS (DDoS) uses multiple IPs, harder to block



Bots and Botnets

Malicious software creates botnets for attacks.

Prevention Techniques

Aspect	Details
Load Balancing	Increases capacity to handle additional load
Attack Patterns	Uses machine learning to detect abnormal behavior
IP Blacklisting	Blocks suspicious IPs using firewalls
CDNs	Cloud-based networks offer protection by load-balancing

DNS Attacks

DNS Poisoning/Spoofing

- Manipulates DNS to redirect users to malicious sites
- Prevention includes ignoring unsolicited DNS responses, using DNSSEC

DNS Reflection Attack

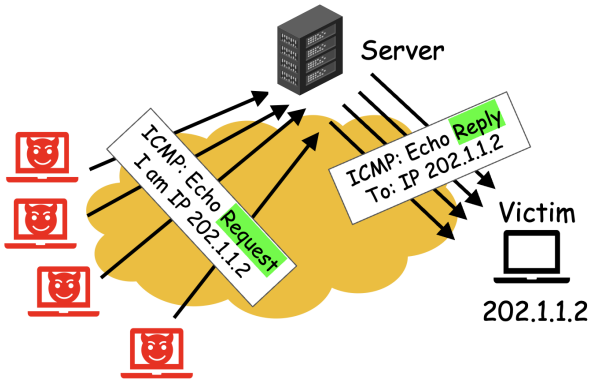
- Uses spoofed IP addresses to flood victims with DNS replies

https://t.me/learningnets

Network Attacks

Smurf Attack

- Floods victim with ICMP ping requests using spoofed IP
- Variation of reflected DNS attack at network layer
- Internal networks use anomaly detection to block Smurf attacks



Teardrop Attack

- Crafts packet fragments with wrong sizes/offsets causing crashes
- Affects older OS like Win 95, NT; keeping them patched is advised

Man In The Middle (MITM) Attacks

Intercepting communication between two parties to steal or manipulate data.

Aspect	Details
IP Spoofing	Masquerading as another by using their IP address.
DNS Spoofing	Tricking users into visiting malicious sites by corrupting DNS queries.
SSL Hijacking	Compromising secure connections by redirecting HTTP requests to HTTPS.
Email Hijacking	Monitoring and sending emails from compromised accounts.

Prevention Strategies

- Use strong encryption on wireless access points.
- Employ VPNs for secure, encrypted remote access.
- Enforce HTTPS to prevent eavesdropping and authenticate using public key

https://t.me/learningnets

Social Engineering & Phishing

Overview

Social engineering exploits human vulnerabilities, often initiating with phishing to extract sensitive information.

Techniques

- Phishing via email, impersonating legitimate entities.
- Vishing through phone calls pretending to be customer support
- Physical tactics like using fake badges to gain access
- Dropping USBs with malware as bait

Prevention

Aspect	Details
Awareness Training	Educate on recognizing phishing emails and suspicious links
Policy Enforcement	Implement IT security policies against phishing
Reporting Mechanisms	Easy reporting of suspicious activities to IT security
Technology Solutions	Use tools like spam filters and anti-malware

https://t.me/learningnets

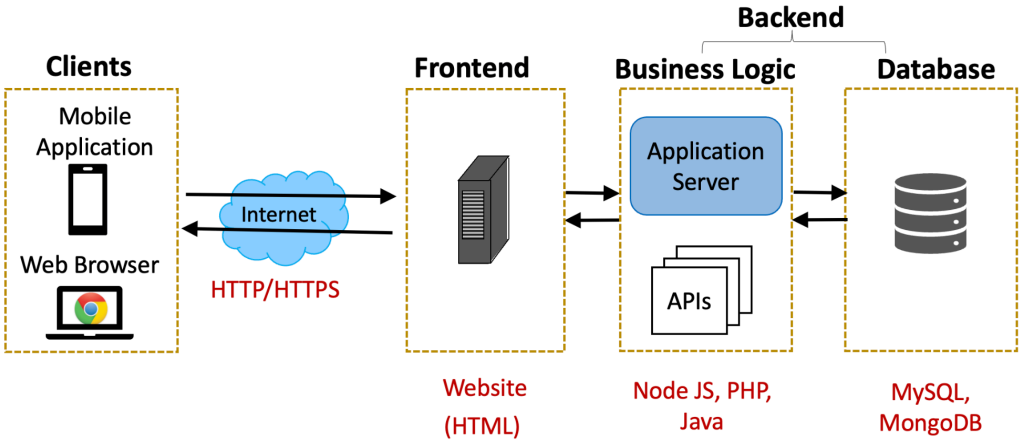
WEB APP SECURITY

https://t.me/learningnets

Web Apps and OWASP Summary

Architecture of Web Apps

Web applications operate on a client-server model, where clients (web browsers, mobile apps) communicate with servers via HTTP/HTTPS. The architecture includes a frontend (user interface with HTML/CSS/JavaScript) and a backend (server, application logic, database) facilitated by APIs.



OWASP Vulnerabilities

Vulnerability	Description
SQL Injection	Malicious SQL code for data theft/manipulation.
Cross-Site Scripting (XSS)	Injecting scripts into web pages viewed by others.
Broken Authentication	Bypassing authentication mechanisms.
Sensitive Data Exposure	Inadequate protection of sensitive data.
XML External Entities (XXE)	Exploiting weak XML processors.
Broken Access Control	Improper user authorization.
Security Misconfiguration	Incorrect security configurations.
Insecure Deserialization	Deserializing untrusted data.
Using Components with Known Vulnerabilities	Exploiting vulnerable components.
Insufficient Logging & Monitoring	Lack of proper logging and monitoring.

https://t.me/learningnets

SQL Injection Summary

Introduction

SQL Injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access.

How It Works

An SQL Injection vulnerability arises when user inputs are insecurely included in SQL queries. Attackers can manipulate these inputs to alter query logic and execute malicious SQL statements.

Example and Prevention

Example: Manipulating user login forms to bypass authentication.

- Correct:
  - SELECT * FROM Users WHERE Name = 'Jack' AND Password = '123'
- SQL Injection:
  - SELECT * FROM Users WHERE Name = '' or '1' = '1' AND Password = '' or '1' = '1'
- SQL Injection:
  - SELECT * FROM Users WHERE Name = '' or '' = ''AND Password = '' or '' = ''

Prevention

Defense Mechanism	Key Features	Benefits
Input Sanitization	Removal of harmful SQL code from user input.	Prevents basic injection attacks.
Prepared SQL Statements	Separates SQL queries from user data.	Eliminates injection points.
Web Application Firewall (WAF)	Monitors HTTP traffic for suspicious activity.	Blocks known attack vectors.

https://t.me/learningnets

Blind SQL Injection

Introduction

Blind SQL Injection occurs when an attacker cannot see the output from the database directly on the webpage but can infer data by sending true/false SQL statements or observing response times.

Types of Blind SQL Injection

Type	Description
Boolean-Based	The output of the page changes based on the query result being true or false.
Time-Based	Delays the database response to confirm data extraction, useful when no output is observed.

Systematic Enumeration and Tools

Blind SQL Injection requires systematic enumeration, trying all possible characters for every part of the injection. While slow, this approach is definitive. Tools like Sqlmap automate this process, supporting various databases and injection types.

XSS (Cross-Site Scripting) Attacks

XSS Type	Characteristics	Impact	Prevention
Persistent XSS	Malicious script stored on the server.	Compromise user data permanently.	Input sanitization, validation.
Reflected XSS	Malicious script reflected off web page.	Steal session data temporarily.	URL parameter validation.
Preventing XSS	-	-	User input sanitization and validation, secure coding practices.

https://t.me/learningnets

MALWARE

https://t.me/learningnets

Malware

Malware, short for malicious software, encompasses various forms designed to infiltrate, damage, or gain unauthorized access to systems. Its primary purposes include theft, espionage, and sabotage, often utilized by hackers.

Types and Purposes of Malware

Type	Purpose
Data exfiltration	Theft, espionage
Spying (RATs, Keyloggers, Spyware)	Surveillance
Ransomware attack	Financial extortion

Infiltration Methods

Malware exploits software vulnerabilities and human weaknesses, such as clicking on malicious links or installing untrusted software, to infiltrate systems.

Malware Delivery: Droppers

Droppers, with a small footprint, represent the frontline of malware attacks, facilitating the download of more sophisticated malware like backdoors and keyloggers.

Safety Tips

Software Vulnerabilities:

- Keep your Operating System updated
- Install applications from trusted sources

Human weakness:

- Do not click on suspicious links in emails -> type the URL yourself
- Do not click on suspicious email attachments unless sure

https://t.me/learningnets

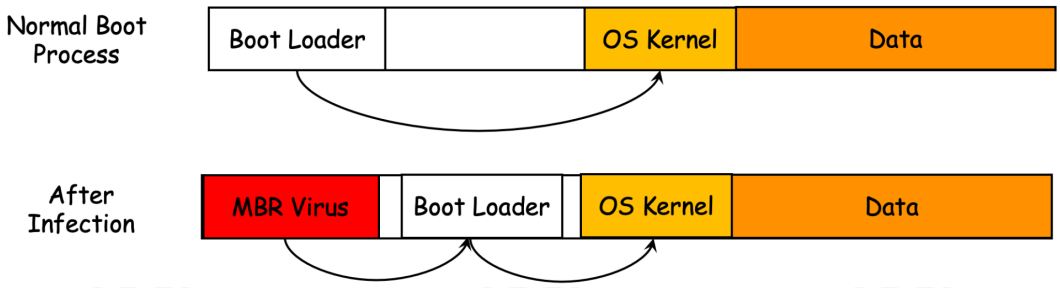
Viruses and Worms

Viruses and worms are types of malware with specific characteristics and behaviors. Viruses require an infected application or file to run and can replicate, destroy data, or launch attacks. Worms, on the other hand, operate independently, can auto-trigger, replicate, and propagate without attaching to a specific application.

Types of Viruses

Boot Sector Virus

Infects the boot sector, loading the virus each time system starts.



Boot Sector Virus

Macro Virus

Targets Microsoft Office documents with scripts for malicious purposes.

Stealth Virus

Evades detection by anti-virus software through various methods.

Polymorphic Virus

Alters its code to avoid detection.

Encrypted Virus

Encrypts itself to evade anti-malware detection.

Worms

Similar to viruses, but worms do not require a host file to spread and can independently replicate and propagate. Notable examples include MyDoom, which is famous for its rapid propagation and significant financial damage.

https://t.me/learningnets

Trojan Malware

Trojans are malicious programs that appear legitimate to trick users into installation, spreading via phishing or email attachments, enabling unauthorized access or damage to systems.

Characteristics

- Appear as legitimate software, deceiving users
- Spread through phishing and email attachments
- Enable remote access via backdoors

Actions

Action	Description
Keylogging	Captures keystrokes to steal information.
Data Manipulation	Modifies or deletes data.
Performance Disruption	Impairs systems or network performance.
DDoS Attacks	Launches attacks using the infected system.
Anti-malware Evasion	Evades detection by security software.

Example: DarkCometRAT

DarkCometRAT, a Trojan offering attackers full control over the system for activities like file manipulation, command execution, and keylogging.

Protection Measures

- Avoid untrusted software.
- Be cautious with email attachments.
- Update antivirus software regularly.

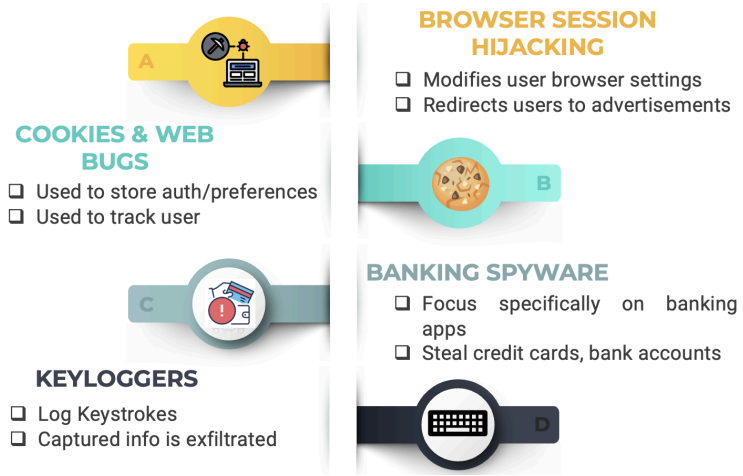
https://t.me/learningnets

Spyware, Adware, and Ransomware

Spyware

Spyware is malware that secretly collects information from a PC without consent. It captures data like internet browsing habits, credentials, and screenshots. Attackers and marketing companies are the primary beneficiaries.

Types of Spyware



Adware

Adware bombards users with unwanted ads, such as popups and banners, often bundled with legitimate software. It can change the homepage, redirect users, and install new plugins for revenue generation.

Ransomware

Ransomware is financially motivated malware encrypting network files with a hacker's key, demanding money for unlocking, potentially causing financial/reputational loss.

Protection Measures

- Avoid unknown software and sources.
- Disable unnecessary browser extensions.
- Use specialized anti-malware software like Malwarebytes.
- Be vigilant about Indicators of Compromise (IoCs).

https://t.me/learningnets

Logic Bombs and Rootkits

Viruses	Self-replicates, causes damage to systems and data
Worms	Self-replicates, propagates over network
Trojans	Look like legitimate software to trick users, install malware and backdoors
Spyware	Steals confidential data such as Internet browsing history
Ransomware	Encrypts and locks down files, demands payment for restoring data
Rootkits	Hidden malware that infects privileged components e.g. OS kernel
Logic Bombs	Triggers on a particular date or event and causes destruction

Protection Measures

- Keep OS and apps patched and up-to-date.
- Monitor for behavioral anomalies.
- Conduct memory dump analysis.

https://t.me/learningnets

Antimalware

Antimalware tools are essential in detecting, protecting against, and removing malicious software. They employ various strategies to identify and mitigate threats, including on-demand and real-time scanning.

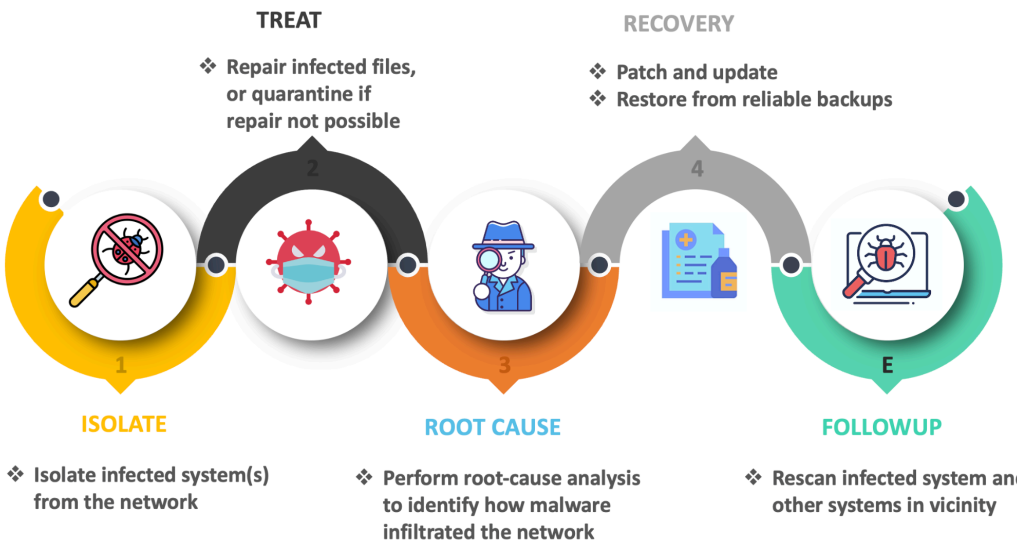
Detection Techniques

- Signature-based: Uses virus definitions to identify malware.
- Anomaly-based: Observes abnormal behavior to detect malware.

Anti-Virus focuses on older, established threats, while Anti-Malware targets more sophisticated and emerging threats.

Remediation Strategies

- Repair infected files or quarantine if repair is not possible.
- Patch and update software regularly.
- Restore systems from reliable backups.
- Isolate infected systems and perform root cause analysis.
- Regular backups and firewalls are fundamental defenses.

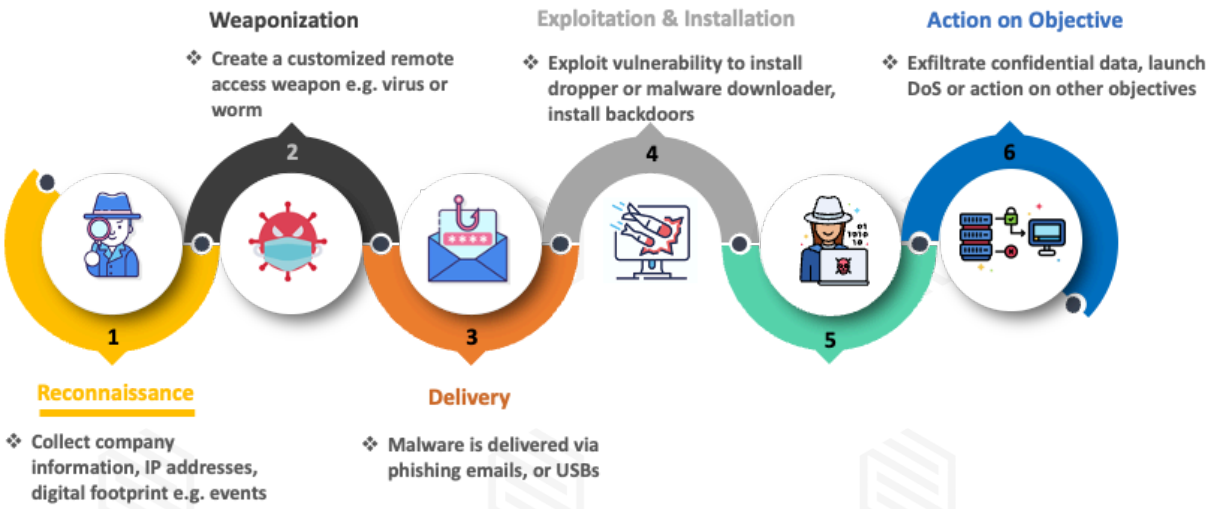


https://t.me/learningnets

INCIDENT RESPONSE AND INTRUSION DETECTION

https://t.me/learningnets

Cyber Kill Chain



The Cyber kill chain documents phases of an attack from inception to action on objectives.

1. Reconnaissance

Reconnaissance refers to gathering information about the target.

- **Passive:** In passive reconnaissance, attackers gather information without direct interaction - includes whois lookups, domain information, company info. There is no footprint, however, the information gathered is limited
- **Active:** In active reconnaissance, attackers gather more detailed information about the target by actively interacting with it. This includes things like port scanning, vulnerability scanning, interactions with firewalls. There is a larger footprint but the information gathered is more detailed

2. Weaponization

The purpose is to create customized malware designed to exploit identified vulnerabilities, e.g., Telnet running on Port 23, or Firewall has unpatched vulnerability. This can also include things like preparing phishing emails, preparing botnets.

3. Delivery

In the delivery phase, the malware that was prepared is now delivered to the target.

https://t.me/learningnets

There are a number of ways that this is achieved:

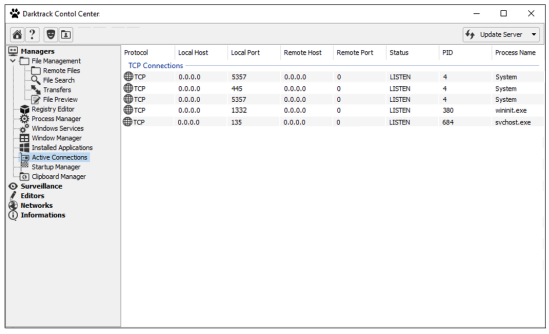
- **Phishing emails:** Phishing emails entice employees by leveraging social engineering e.g., based on upcoming company events, Christmas bonus
- **Drive-by-Downloads:** Links lead to malicious website with
- **USB Drive:** Malicious USB purposefully dropped on company premises
- **Direct Hacking:** This attack vector involves directly targeting open ports e.g., Telnet (Port 23)

4. Exploitation and Installation

- Exploit vulnerability and infiltrate the target e.g., Metasploit
- **Dropper:** Malware with small footprint, leads to download of subsequent, more advanced malware
- **Privilege Escalation:** Attempt to gain elevated privileges (admin)
- **Lateral Infection:** Attempt to gain access to systems in vicinity
- **Backdoors:** A Backdoors are opened to allow for remote control

5. Command and Control

Special Trojans, called Remote Access Trojans create backdoor channels to the remote commander and provide Persistent Access



6. Action on Objectives

- Data Exfiltration, Denial of Service, Ransomware, Passive espionage

https://t.me/learningnets

Incident Response Lifecycle

The IR lifecycle lists the phases that security specialists follow to respond to a cyber attack. Typically, each phase is in response to a step of the Cyber Kill Chain.

Phase 1. Preparation

It is the most important part of the IR lifecycle and includes preparing:

- Incident Response Plan and IR team with roles and responsibilities
- Processes to handle incidents
- Incident management forms
- Trainings - mock drills
- **Jump bag:** IR Plan and checklists, laptops, scanning and forensic tools

Phase 2. Identification

Decide whether a security event is a security incident ?

- Abnormally high system response time
- Anomalous system activity
- Presence of suspicious files or executables
- Unusual outbound network activity

https://t.me/learningnets

Phase 3. Containment

This phase relates to attempts to limit the damage as well as the spread:

- **Short-Term Containment**
    - Isolate affected systems to prevent further spread.
    - Disable compromised accounts or credentials.
    - Lock malicious IPs, domains, or IOCs at firewall or endpoint
    - Preserve volatile data (e.g., memory dumps) before shutting systems
- **Long-Term Containment**
    - Apply temporary fixes or patches to mitigate vulnerabilities.
    - Segregate affected systems from production until remediation completes
    - Restrict unnecessary access to critical infrastructure
    - Increase logging and alerting for enhanced monitoring

Phase 4. Eradication

- **Remove** malware, backdoors, and malicious accounts
- **Scan** systems, apps and DBs to ensure there is no residual malware
- **Restore** servers, systems and databases from backups
- **Reimage** applications and operating systems from trusted images
- **Inform** relevant personnel about the ongoing eradication activities

Phase 5. Recovery

Monitor the infrastructure, databases and applications to ensure there is no recurrence. Validate that the system state and data have been properly restored after the incident. Install patches and upgrades on systems, firewalls & applications. Document the recovery procedures that were performed

Phase 6. Lessons Learned

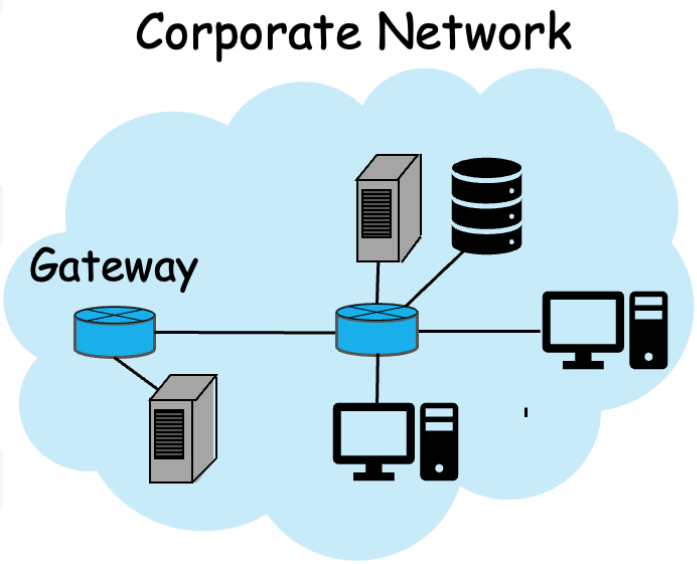
This phase corresponds to doing a more thorough offline investigation to identify why the incident happened in the first place and more importantly, what can be done to avoid such an incident in the future.

https://t.me/learningnets

Intrusion Detection Systems (IDS)

Listens to network traffic and detects intrusions such as Exploits against the OS and applications, SQL injections, Cross-Site Scripting, data theft.

- **IDS -** Only Detect Intrusions
- **IPS (Intrusion Prevention Systems) –** Detect and stop intrusions

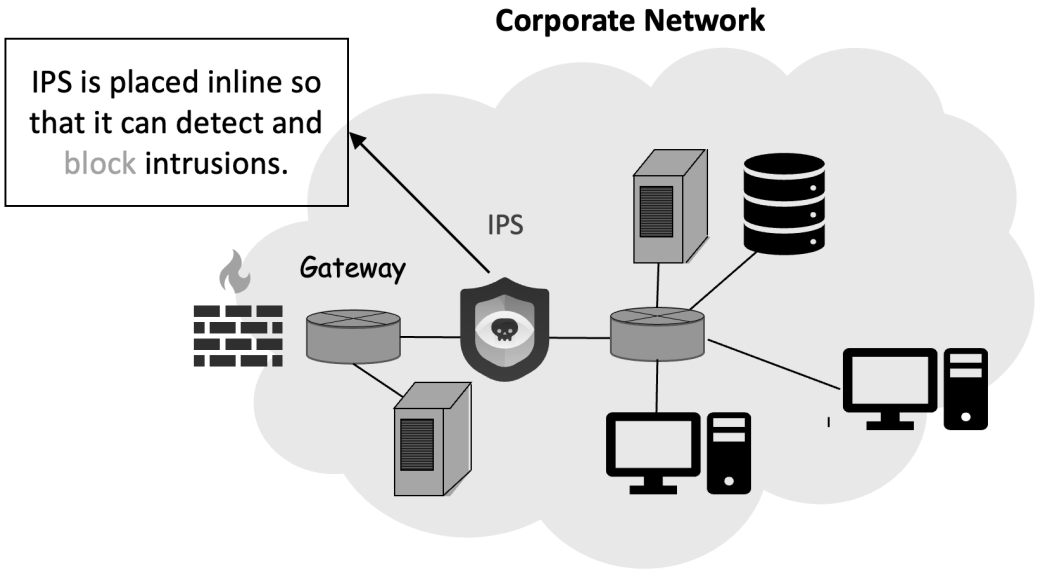


- **HIDS (Host-Based IDS) :**
  - Installed on end systems
  - Monitors incoming /outgoing traffic from a host
  - Monitor log files located on the end system
- **NIDS (Network-Based IDS):**
- **Installed on the network**
  - Monitors network traffic
  - Monitor network-wide log files stored on servers
- **Challenges:** Can only detect intrusions since they only receive a copy of the packet so it cannot block malicious traffic but only generate an alert.

https://t.me/learningnets

Intrusion Prevention Systems (IPS)

Listens to network traffic and not only detects intrusions, but also has the capability of blocking malicious traffic. IPS is usually placed inline to be able to intercept traffic.



Comparison of IDS vs IPS

Feature	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Core Function	Detects threats and alerts administrators	Detects threats and **blocks them in real-time**
Traffic Placement	Out-of-band (monitors copies of traffic)	Inline (sits in path of actual traffic)
Action Taken	Sends alerts only	Blocks, drops packets, resets connections
Impact on Traffic	No interference or delay	May introduce slight latency
Risk with False Positives	Alerts only (less disruptive)	May block legitimate traffic
Best Use Case	Monitoring & forensic analysis	Real-time protection and automated prevention

https://t.me/learningnets

Snort (Intrusion Detection and Prevention)

One of the most popular, open-source intrusion Detection and Preventions Systems (IDPS) in the industry.

- Simple and easy-to-write rules
- Rich set of existing rules
- Very flexible custom rules

Versions:

- **Snort1 ->** Basic
- **Snort2 ->** More advanced, most widely used
- **Snort3 ->** multi-threading, C++ for fast performance, custom plugins

Writing Snort Rules

Rule Action: Alert , Drop , Pass , Reject

Protocol: TCP , UDP , IP, ICMP

Src IP & Port: 1.1.1.1. , Range of IPs , IP Class, Port Negation ![443]

Direction: Incoming (→), Outgoing (←), bi-directional (<>)

Dst IP & Port: 1.1.1.1. , Range of IPs , IP Class, Port Negation ![443]

Sourcing Rules

Rule creation can be done in one of the two ways:

- Manually
- Leveraged off existing threat intelligence sources

Examples of threat intelligence platforms include sources as www.misp-project.org

https://t.me/learningnets

NETWORK FORENSICS

https://t.me/learningnets

Network Forensics

The process of collecting and analysing network events for the purposes of information gathering or intrusion detection.

Network Evidence

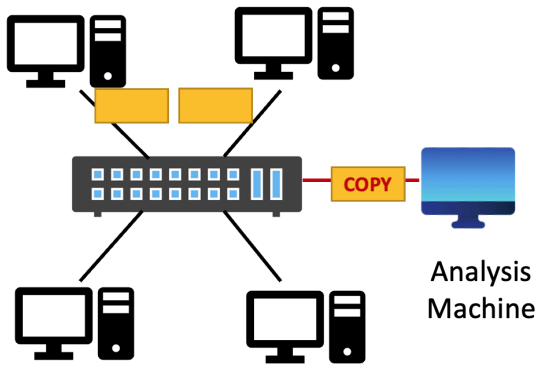
Network evidence can be collected in one of the two days:

- **Network Traffic Analysis:**
  - Full packet capture
  - TCPDump, Wireshark
- **Log Analysis:**
  - Routers
  - Proxy Servers
  - Web Servers

Popular Packet Sniffers

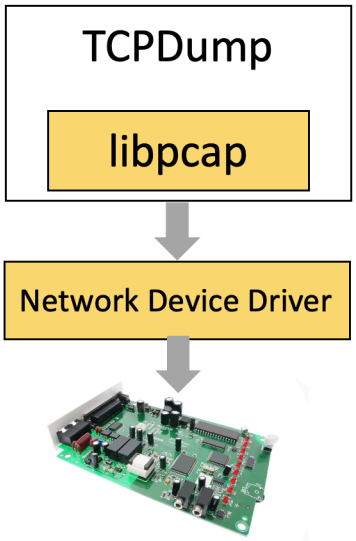
TCPDump, Wireshark, Ethereal

SPAN Ports



- Switched Port Analyzer (SPAN)
- Dedicated Port on Switch
- Copies every packet and sends it to a machine for analysis or logging
- Also helps in troubleshooting

https://t.me/learningnets



Network Interface Card

Tcpdump

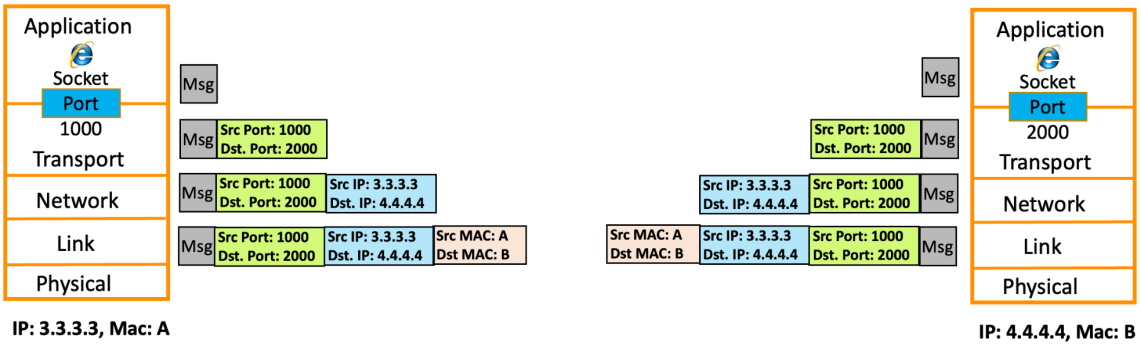
One of the most popular packet sniffing tools that is widely used in the industry.

Packet capture and filtering Engines

- **Libpcap:** Pioneering library developed for Unix, used by TCPDump and Libpcap
- **WinPcap:** Porting of Libpcap from Unix to Windows Operating Systems

Packet and Protocol Analysis

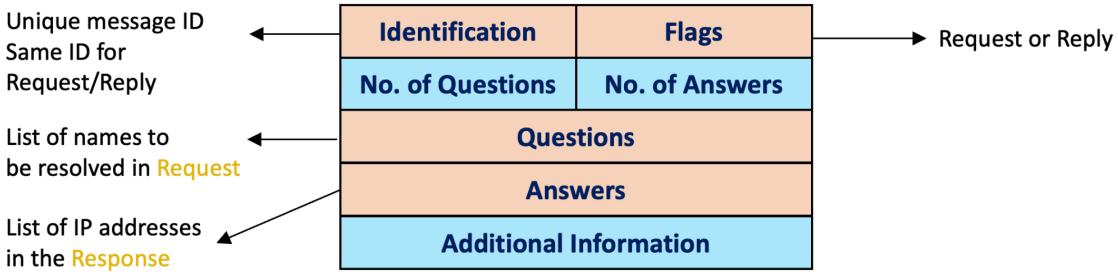
To understand network forensics, it is important to have a basic understanding of the protocol stack, the headers at different layers and how they interact.



https://t.me/learningnets

DNS Message Header

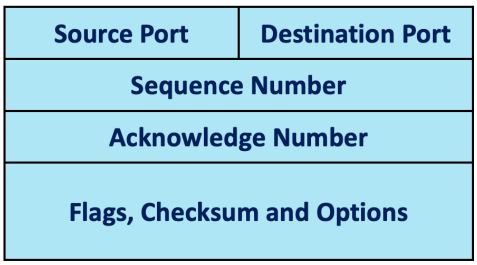
DNS is an application layer protocol and is used to resolve hostnames to IP addresses.



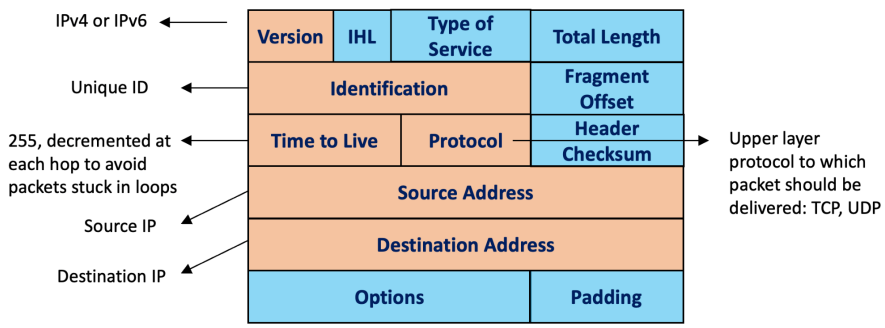
TCP Header

TCP header is one of the most popular protocols at the transport layer.

- **Source and Destination Ports:** specify which ports are being used at the source system and at the destination system between the transport layers and the upper application layers
- **Sequence Number and ACK Number:** The Sequence and Acknowledgement numbers are used to track the amount of data communicated between the source and the destination.



IP Header



https://t.me/learningnets

TCP Dump Commands

Listen to All Traffic on an Interface

```
sudo tcpdump -i docker0 -v
```

(-i – interface on which tcpdump should listen)
(-v – verbose mode, shows more details of packet headers)

Filter on Destination Port

```
sudo tcpdump -i docker0 -v dst port 80
```

Filter on Host (dst or source)

```
sudo tcpdump -i docker0 -v host 172.17.0.2
```

Filter on Host (dst)

```
sudo tcpdump -i docker0 -v dst host 172.17.0.2
```

Filter on Protocol (icmp)

```
sudo tcpdump -i docker0 -v icmp
```

Reading from Packet Capture file instead of interface

```
sudo tcpdump -r tcpdump/capture.pcap -v icmp and src host
172.17.0.2
```

Filter on Protocol and Destination Port (DNS messages from Kali to nginx)

```
sudo tcpdump -r tcpdump/capture.pcap -v udp and dst port 53 and src
host 172.17.0.1 and dst host 172.17.0.2
```


https://t.me/learningnets

ACCESS CONTROL MODELS

https://t.me/learningnets

Access Control Models

Access Control Models control the permissions in an organization. They define which subjects have access to which resources as well as the type of access.

Discretionary Access Control (DAC):

- **Ownership based -** The owner has complete discretion to delegate permissions to a resource that they own
- **Example:** You create a Google Docs document, so now it's up to you to define who gets access and the type of access (read, edit)
- **Advantages:** Super simple and flexible
- **Disadvantages:**
    - Trojan Horse Problem (delegating access opens up abuse possibility)
    - Less centralized control (a central authority is not involved)
    - Scalability issues (hard to scale in large-scale enterprises)

Mandatory Access Control (MAC):

- Opposite of DAC
- A central authority gets to decide the labels or classification of subjects as well as objects

- This is like a top-secret government agency. A central authority (the "boss" or administrator) sets very strict rules based on "clearance levels" or "security

https://t.me/learningnets

labels." Users and resources are given labels, and only matching labels allow access. Users can't change these rules themselves.

- **Example:** A secret government document is labeled "Top Secret." Only someone with "Top Secret" clearance can read it, even if a lower-level person created it.

Role-Based Access Control (RBAC):

- Most widely used access control model (used by over 80% mid-large sized orgs)
- Instead of assigning permissions to users, we create groups or **roles** which have specific permissions and then we assign users to those roles
- This is very common in businesses. Access is granted based on your job role or function within an organization. Instead of giving "John" permission to do something, you give "Manager" permission, and then you make "John" a "Manager."
- **Example:** All "Sales Representatives" can access the customer database, while only "Accountants" can access the financial system.

Attribute-Based Access Control (ABAC):

- Instead of Roles, we check the attributes (characteristics) to decide
- Access isn't just based on who you are or your job, but on a combination of different "attributes" (characteristics). These could be things like:
    - **User attributes:** Your department, location, seniority.
    - **Resource attributes:** The sensitivity of the data, its creation date.
    - **Environmental attributes:** The time of day, the device you're using.
- **Example:** A doctor can access patient records (user attribute: doctor, resource attribute: patient record) but only from a hospital computer (environmental attribute: secure device) during working hours (environmental attribute: time).

https://t.me/learningnets

GOVERNANCE, RISK AND COMPLIANCE (GRC)

https://t.me/learningnets

Governance, Risk and Compliance

GRC is an organizational strategy to manage governance and risks while maintaining compliance with industry and government regulations (IBM).

Governance

- Policies and standards manage information security
- Ensures cybersecurity aligns with business strategy
- The roles, responsibilities and accountability is clear

Policies

- Organization-wide, high level and broad scoped
- Defined for long terms (several years)
- Define responsibilities for management and user

Standards

- Rules to achieve the intent of the policy

Procedures

- Specific steps
- Train employees and ensure consistency in security related business processes

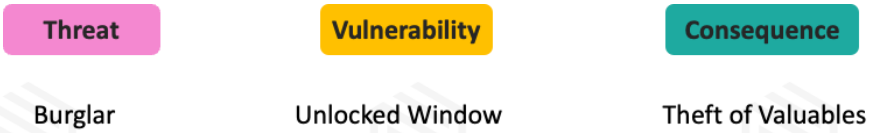
Guidelines

- Optional recommendations

https://t.me/learningnets

Risk

Risk is the possibility that a **threat** will take advantage of a **weakness** (vulnerability) and cause **harm**.



Security Control Types

Security controls are safeguards or measures put in place to protect systems, data, and networks from threats and unauthorized access.

Managerial (Administrative) Controls

- Set policies, procedures, and guidelines
- **Examples:** Security Awareness Training, Data Classification, Access Control Policies

Technical (Logical) Controls

- Software and hardware mechanisms for IT protection
- **Examples:** firewalls, encryption, patch management

Physical Controls

- Aim to protect the physical infrastructure
- **Examples:** Security guards, door locks, CCTV

Security Controls By Function

Preventive - Aim to prevent the attack or threat from materialising e.g., firewalls

Detective - Aim to help detect any threat or suspicious activity e.g., IDS

Corrective - Aim to mitigate the impact of threat e.g., anti-virus

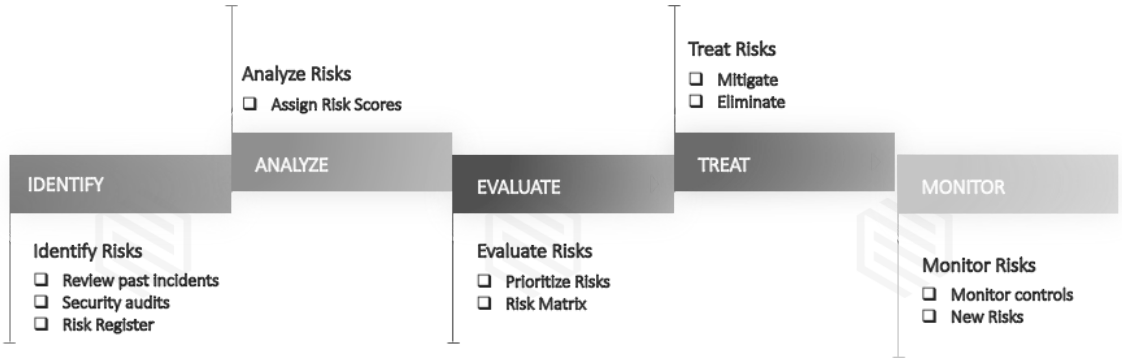
Deterrent - Aim to discourage the attackers e.g., security guards, guard dogs

Compensating - Used when the correct control is unavailable e.g., sensors to alert when putting a lock is not possible.

Recovery - Aim to help perform long-term recovery from attacks e.g., DR plans.

https://t.me/learningnets

Risk Management Lifecycle



Step 1 - Identifying Risks

There are several sources that you can consult to help you identify risks:

- Identify and Inventory Assets
- Review Historical Incidents
- Security Assessments and Audits
- Review compliance regulations

Risk Type	Description
Operational	Risks due to internal processes, systems or people. Examples include System outages or downtime, misconfigured firewalls, weak backup and recovery processes, insider threats and lack of staff training in security practices
Technical/IT	Directly related to information systems and technology Examples include malware, ransomware, spyware attacks, DDoS attacks impacting availability, vulnerabilities in web applications, unpatched software or outdated systems and poor access control or password practices
Strategic	Risks that impact long-term goals of an organization Examples include failure to invest in secure systems, relying on

https://t.me/learningnets

	unvetted third-party vendors, ignoring cybersecurity in digital transformation plans
Compliance	Risk of being non-compliant to laws or standards. Examples include non-compliance with GDPR, HIPAA, or PCI-DSS, data breach notification failures and inadequate logging and monitoring
Reputational	Risk of damage to brand image or reputation. Examples include systems hacked or data breach that becomes public knowledge, loss of customer trust after security incident
Physical	Risks arising from real-world incidents that impact systems and data. Examples include theft of company laptops or servers, unauthorized physical access to server rooms, fire, flood, or natural disaster impacting data centers

Step 2 - Analysing Risks

- **Likelihood** - The chance that the risk will actually materialise
- **Impact -** The damage caused by the risk when it materializes

RISK = Likelihood x Impact

Likelihood	Description
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Impact	Description
1	Negligible
2	Minor
3	Moderate
4	Major
5	Catastrophic

https://t.me/learningnets

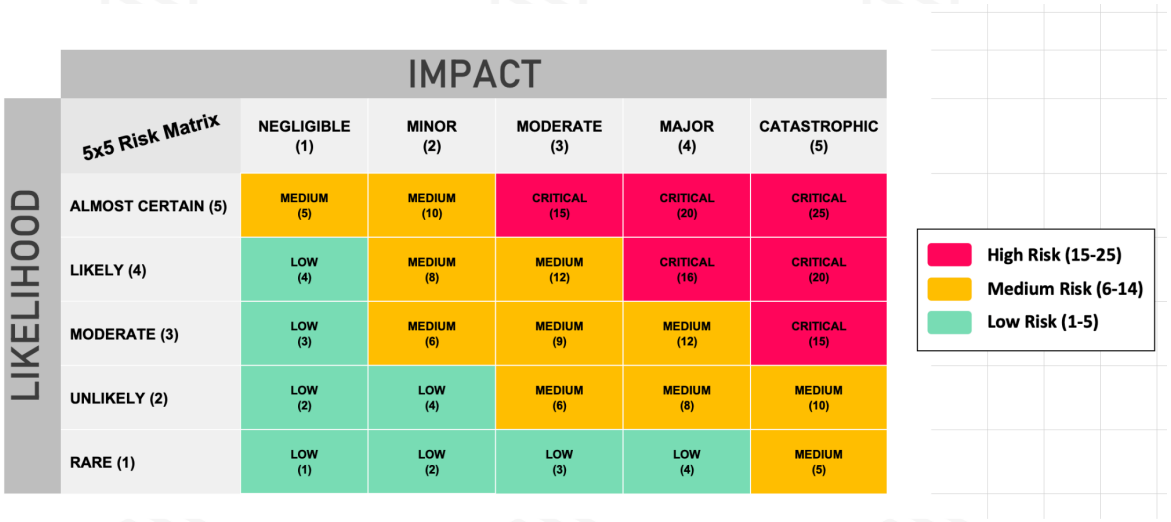
Likelihood and Impact are determined by using the following sources:

- Historical data (e.g., past incidents, industry reports)
- Expert judgment (e.g., consulting security leads, threat intel)
- Vulnerability scans and penetration tests results

Step 3 - Evaluating Risks

In this phase we classify risks based on their scores into macro categories e.g., low, medium and critical instead of having several classes based on different risk scores.

This is achieved by creating the risk matrix, which helps us visually separate out different risk categories.



Step 4 - Treating Risks

In this phase we decide and implement the strategy to address the risks:

Avoid Risk - Discontinue an application or avoid that activity. Example: avoid offering an application that has high potential of being exploited e.g., may require several open ports.

Mitigate Risk - In this case, offering the application or service outweighs the risks, so we mitigate or reduce the risk to bring it to an acceptable level. The risks still need to be documented though and mitigation can be achieved through security controls.

https://t.me/learningnets

Example: Risk that data may get compromised or leaked when sending to a 3rd party, but we can encrypt the data and mitigate the risk.

Step 5 - Monitoring Risks

In the final phase of the Risk Management Lifecycle, we need to ensure that we have proposed risk monitoring mechanisms in place so that we are aware of different risks. Places to monitor:

- Log analysis
- Vulnerability scanning
- Patch management
- Configuration management
- IDS/IPS monitoring
- Endpoint security logs

The Risk Register

Risk ID	Risk Description	Asset Affected	Likelihood (1-5)	Impact (1-5)	Risk Score
RISK-001	Unauthorized access to HR records	HR System	3	4	12
RISK-002	Ransomware attack on main file server	File Server	4	5	20
RISK-003	Outdated software on employee systems	Employee Workstations	2	3	6
RISK-004	Data breach due to third-party vendor	Customer Database	4	5	20

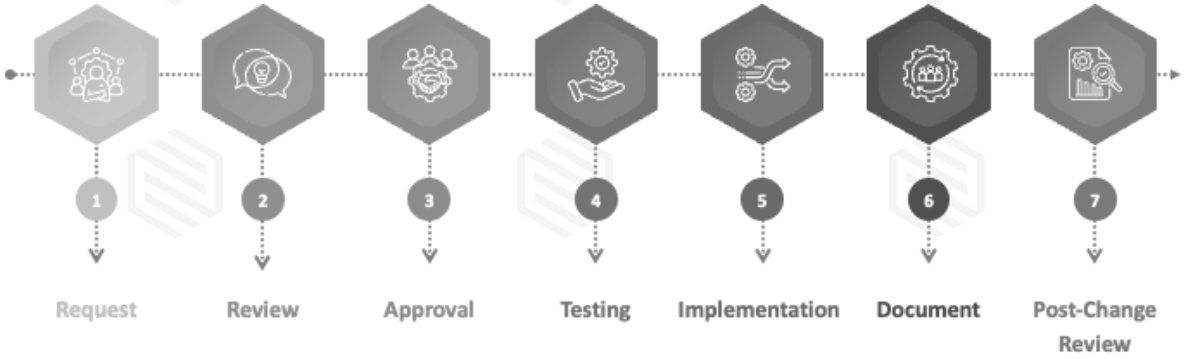
Risk Level	Risk Owner	Mitigation Plan	Current Status
Medium	HR Manager	**Mitigate Risk**: Implement role-based access control	Plan or Action Identified
Critical	IT Security Lead	**Mitigate Risk:** Regular backups and endpoint protection	Mitigation in progress
Medium	IT Support	**Accept Risk:** Risk unlikely to materialize and not damaging	Accepted
Critical	Vendor Manager	**Transfer Risk:** Buy cyber insurance	Under Review

https://t.me/learningnets

Change Management

The change management policy is a formal document that defines how changes to IT systems must be proposed, approved, implemented, and reviewed.

The Change Management Lifecycle



Types of Change

- Standard (routine changes with low risk)
- Emergency (e.g., a critical vulnerability patch)
- Major Changes

https://t.me/learningnets