

PROFESSIONAL TRAINING 1 REPORT
At
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the award of Bachelor
of Technology in INFORMATION TECHNOLOGY

By
M.Prithiviraj
REG. NO. 39120085



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU

APRIL 2022



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI– 600119
www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **M.Prithiviraj (Reg. No: 39120085)** who carried out the project entitled “**Advanced scan of multiple targets**” under my supervision in April 2022

Internal Guide

Dr.P.Ajitha

Head of the Department

Submitted for Viva voce Examination held on _____

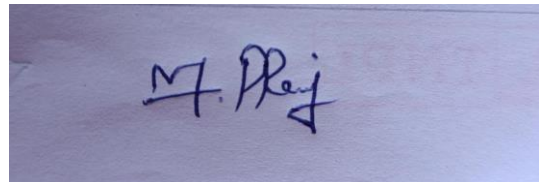
Internal Examiner

External Examiner

DECLARATION

I, **M.Prithiviraj** hereby declare that the project report entitled '**Advanced scan of multiple targets**' done by me under the guidance of **Dr. P.Ajitha** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology in

INFORMATION TECHNOLOGY

A rectangular box containing a handwritten signature in blue ink. The signature appears to be 'M. Prithiviraj' written in a cursive style.

DATE:28/04/2022

PLACE:Chennai

SIGNATURE OF THE CANDIDATE

Acknowledgement

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D, Dean, School of Computing, Dr. R. Subhashini, M.E., Ph.D. Head of the Department of Information Technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.P.Ajitha** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project

TRAINING CERTIFICATE



ABSTRACT

Ethical Hacking is a process of detecting Vulnerabilities in an application, system, organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent Cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points.

A Simple Network Scan of Multiple Targets helps the attacker to scan the vulnerabilities of multiple targets with the Information he gathered through Footprinting.

Network Scan helps to detect all the active hosts on a network and maps them to their IP Address.

Network Scanner sends a packet or Ping to every possible IP Address and wait for a response to determine the status of the applications or devices.

Network Scanning allows companies to keep a tab on the available UDP and TCP Network Services, access the Operating systems in use by monitoring the IP responses, and also to identify the Filtering System based nodes.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	5
1	INTRODUCTION	
	1.1 Purpose and Motivation	8
2.	AIM AND SCOPE OF THE PRESENT INVESTIGATION	9
	2.1 AIM	9
	2.2 SCOPE	9
	2.3 ACCESSIBILITY	9
	2.4 NEED...	10
	2.5 FEASIBILITY STUDY	11
3.	EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHMS USED	12
	3.1 Software Required	
	3.1.1 Windows 10	
	3.1.2 Oracle VM VirtualBox	12
	3.1.3 Kali Linux	
	3.1.4 Nmap	
	3.1.5 Zenmap	
	3.2 Hardware Required	
	3.2.1 Hard Disk	
	3.2.2 RAM	
	3.2.3 Processor	18
	3.2.4 Mouse	
	3.2.5 Keyboard	
	3.2.6 Speaker	
4.	RESULTS AND DISCUSSION	21
	4.1 Result and discussion	
5.	WORKING AND SCREENSHOTS	22

	5.0 Installation	
	5.1 kali Linux Setup	
	5.2 Nmap	
	5.3 Zenmap	
	5.3.1 RESULT	
6.	SUMMARY AND CONCLUSIONS	35
7.	REFERENCES	36

CHAPTER - 1

INTRODUCTION

1.1 ABOUT THE CONCEPT

As time passes, the world is becoming more connected due to Internet and new networking technology. Due to open nature of Internet, security of network has hold attention. With the development of new technologies, organization is now moving its business functions to public network, and thus a huge amount of personal, commercial and organization's information are available on networking infrastructures worldwide. Thus a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized person.

Network access is unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destruct exclusive information which adversely influences organization benefit, and upset the proficiency to contend in business.

In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. Network security measures include scanning and vulnerability analysis along with penetration testing.

Network scanning is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network, either with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting and patching for any organization's network.

CHAPTER - 2

AIM AND SCOPE OF PRESENT

INVESTIGATION

2.1 AIM

Identify internal and external threats by vulnerability assessment using network vulnerability scanner. Develop a web-based tool designed to detect weaknesses in computers, computer systems and networks.

The research at hand recognizes the importance of network security and specifically that of current vulnerability scanners.

It is aimed principally at making a contribution towards enhancing vulnerability assessment process by combining tools and reducing administrative burden.

2.2 SCOPE

- To produce a comprehensive view of all operating systems and services running and available on the network.
- Detect misconfigured devices in network such as misconfigured web server, firewall etc.
- To detect critical vulnerabilities such as vulnerable web servers in the network.

2.3 ACCESSIBILITY

A “computer system” is significantly more than hardware and software. It incorporates the policies and procedures of organization under which that

hardware/software is utilized. Security holes can emerge from numerous ranges.

When attacker breaks into a computing system, he takes advantage of lapses in procedures, technology, or management (or some combination of those factors), allowing unauthorized access or actions. The precise failure of the controls is termed a vulnerability or security flaw. And mistreatment of that failure to violate the security policy is termed exploiting the vulnerability.

Thus, a mechanism is required which can fulfill following objectives:

Protection of network devices.

Reduce the vulnerability of applications and end-systems originating from the network.

Protect information throughout transmission over the network. This mechanism is called “Network Security” which takes measures to reduce the susceptibility of a network to threats. To ensure network security, numerous open-source as well as commercial products are available.

2.4 NEED OF ETHICAL HACKING

The primary benefit of ethical hacking is to prevent data from being stolen and misused by malicious attackers, as well as:

- ❖ Discovering vulnerabilities from an attacker's POV so that weak points can be fixed.
- ❖ Implementing a secure network that prevents security breaches.
- ❖ Defending national security by protecting data from terrorists
- ❖ Gaining the trust of customers and investors by ensuring the security of their products and data.
- ❖ Helping protect networks with real-world assessments.

2.5 FEASIBILITY STUDY

All projects are feasible when given unlimited resources and infinite time. It's both necessary and prudent to evaluate the feasibility of a project at the earliest possible time. The efforts and resources spent in developing the system will be a waste if the end solution does not offer timely and satisfactory solution to its users.

Feasibility study is a test of system proposed regarding workability, impact on the organization ability to meet user needs, and effective use of resources. Thus when a new application is proposed, it normally goes through a feasibility study before it is approved for development.

Feasibility and risk analysis are related in many ways. If project risk is great, the possibility of producing quality software is reduced.

CHAPTER 3

EXPERIMENTAL OR MATERIALS AND METHODS

3.1 SOFTWARE REQUIREMENT

- ❖ Windows 10 OS
- ❖ Oracle VM VirtualBox
- ❖ Kali Linux
- ❖ Nmap
- ❖ Zenmap

3.1.1 Windows 10 or above

Windows 10 is a Microsoft operating system for personal computers, tablets, embedded devices and internet of things devices.

Microsoft released Windows 10 in July 2015 as a follow-up to Windows 8. The company has said it will update Windows 10 in perpetuity rather than release a new, full-fledged operating system as a successor.

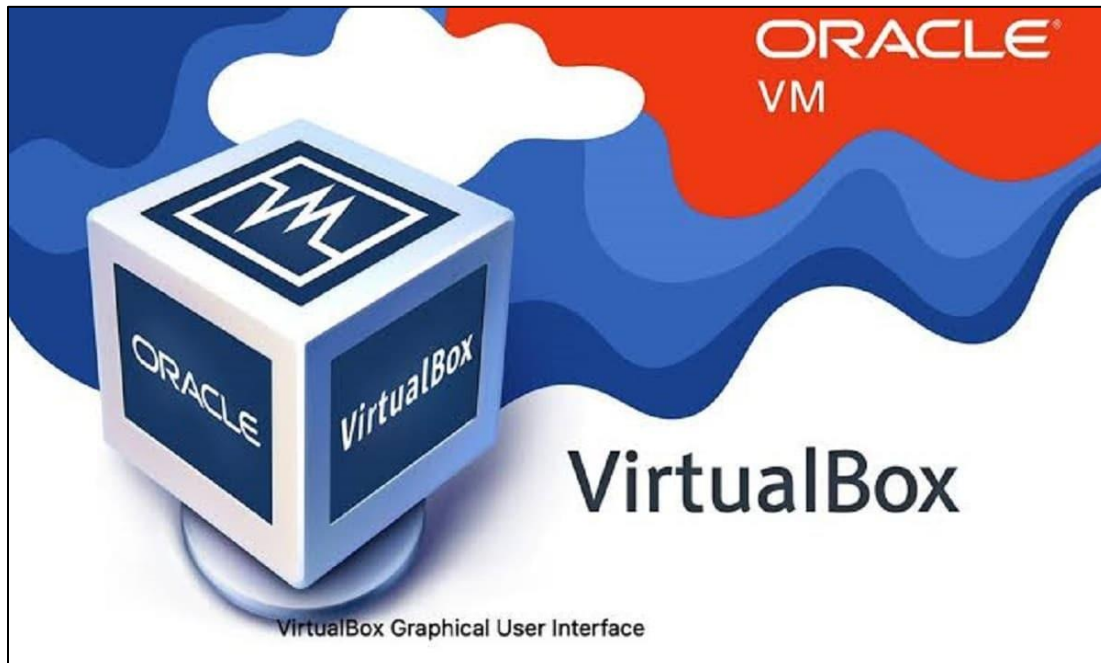
3.1.2 Oracle VM VirtualBox

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows

7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the



product always meets professional quality criteria.

3.1.3 Kali Linux

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.

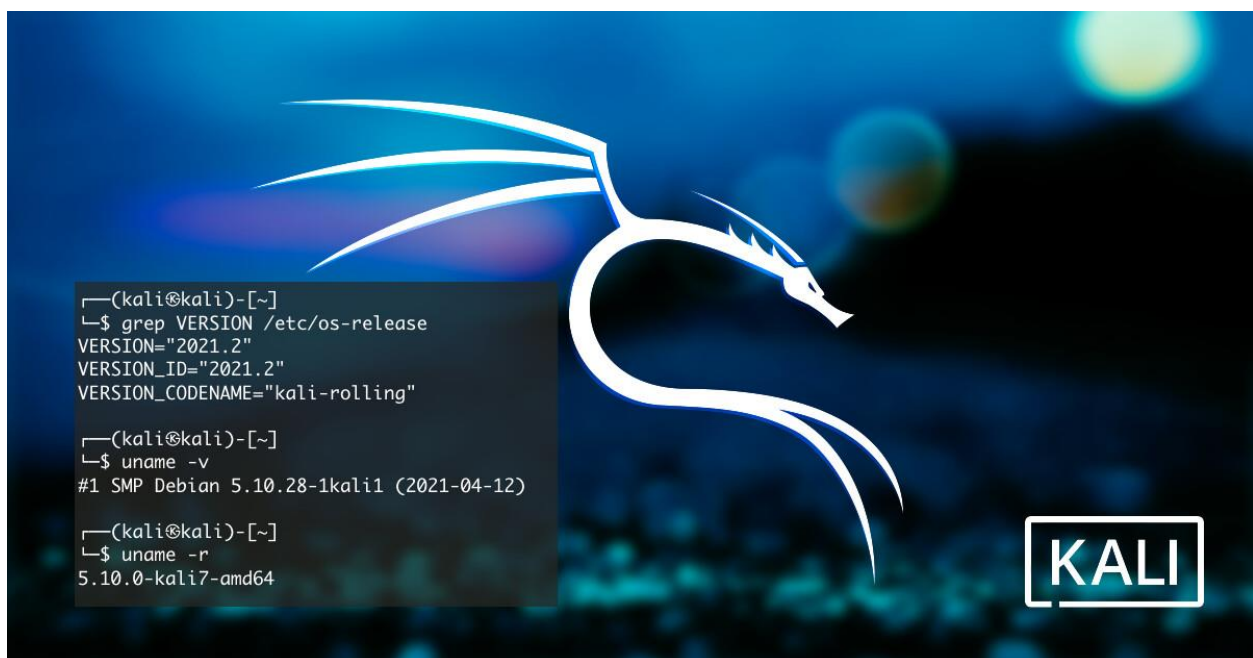
Kali Linux was released on the 13th March 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely

to Debian development standards.

FEATURES:

- ❖ More than 600 penetration testing tools included: After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either simply did not work or which duplicated other tools that provided the same or similar functionality. Details on what's included are on the Kali Tools site.
- ❖ Free (as in beer) and always will be: Kali Linux, like BackTrack, is completely free of charge and always will be. You will never, ever have to pay for Kali Linux.
- ❖ Open source Git tree: We are committed to the open source development model and our development tree is available for all to see. All of the source code which goes into Kali Linux is available for anyone who wants to tweak or rebuild packages to suit their specific needs.
- ❖ FHS compliant: Kali adheres to the Filesystem Hierarchy Standard, allowing Linux users to easily locate binaries, support files, libraries, etc.
- ❖ Wide-ranging wireless device support: A regular sticking point with Linux distributions has been support for wireless interfaces. We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.
- ❖ Custom kernel, patched for injection: As penetration testers, the development team often needs to do wireless assessments, so our kernel has the latest injection patches included.
- ❖ Developed in a secure environment: The Kali Linux team is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.
- ❖ GPG signed packages and repositories: Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.
- ❖ Multi-language support: Although penetration tools tend to be written in English, we have ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.

- ❖ Completely customizable: We thoroughly understand that not everyone will agree with our design decisions, so we have made it as easy as possible for our more adventurous users to customize Kali Linux to their liking, all the way down to the kernel.
- ❖ ARMEL and ARMHF support: Since ARM-based single-board systems like the Raspberry Pi and BeagleBone Black, among others, are becoming more and more prevalent and inexpensive, we knew that Kali's ARM support would need to be as robust as we could manage, with fully working installations for both ARMEL and ARMHF systems. Kali Linux is available on a wide range of ARM devices and has ARM repositories integrated with the mainline distribution so tools for ARM are updated in conjunction with the rest of the distribution.



3.1.4 Nmap

- ❖ Nmap (Network Mapper) is a network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- ❖ Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced

service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

- ❖ Nmap started as a Linux utility and was ported to other systems including Windows, macOS, and BSD. [It is most popular on Linux, followed by Windows.]
- ❖ Nmap features include:
- ❖ Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- ❖ Port scanning – Enumerating the open ports on target hosts.
- ❖ Version detection – Interrogating network services on remote devices to determine application name and version number.
- ❖ TCP/IP stack fingerprinting – Determining the operating system and hardware characteristics of network devices based on observations of network activity of said devices.



```
root@kali: /home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:13c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1068/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5880/tcp  filtered vnc-http
5900/tcp  filtered vnc
9929/tcp  open  nping-echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel; Ubuntu2.13 (Ubuntu Linux; protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```

- ❖ Scriptable interaction with the target – using Nmap Scripting Engine(NSE) and Lua programming language.
- ❖ Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

3.1.4 Zenmap

Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features

for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scans can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Features:

Interactive and graphical results viewing

In addition to showing Nmap's normal output, Zenmap can arrange its display to show all ports on a host or all hosts running a particular service. It summarizes details about a single host or a complete scan in a convenient display. Zenmap can even draw a topology map of discovered networks. The results of several scans may be combined together and viewed at once.

Comparison

Zenmap has the ability to show the differences between two scans. You can see what changed between the same scan run on different days, between scans of two different hosts, between scans of the same hosts with different options, or any other combination. This allows administrators to easily track new hosts or services appearing on their networks, or existing ones going down.

Convenience

Zenmap keeps track of your scan results until you choose to throw them away. That means you can run a scan, see the results, and then decide whether to save them to a file. There is no need to think of a file name in advance.

Repeatability

Zenmap's command profiles make it easy to run the exact same scan more than once. There's no need to set up a shell script to do a common scan.

Discoverability

Nmap has literally hundreds of options, which can be daunting for beginners. Zenmap's interface is designed to always show the command that will be run, whether it comes from a profile or was built up by choosing options from a menu. This helps beginners learn and understand what they are doing. It also helps experts double-check exactly what will be run before they press "Scan".

3.2 HARDWARE REQUIREMENT

- Hard Disk
- RAM – 1 GB
- Processor – Dual Core or Above
- Mouse
- Keyboard
- Monitor
- Speaker

3.2.1 Hard Disk

A hard disk or fixed disk, is an electro-mechanical data storage device that uses magnetic storage to store and retrieve digital information using one or more rigid rapidly rotating disks (platters) coated with magnetic material.

During the mid-1990s the typical hard disk drive for a PC had a capacity of about 1 gigabyte. As of January 2019, desktop hard disk drives typically had a capacity of 1 to 6 terabytes, with the largest-capacity drives reaching 15 terabytes

3.2.2 RAM

Random access memory (RAM) is a type of data storage used in computers that is generally located on the motherboard. This type of memory is volatile and all information that was stored in RAM is lost when the computer is turned off.

The RAM chip may be individually mounted on the motherboard or in sets of several chips on a small board connected to the motherboard. Older memory types were in the form of chips called dual in-line package (DIP). Although DIP chips are still used today, the majority of memory is in the form of a module, a narrow printed circuit board attached to a connector on the motherboard. The three main memory circuit boards

types containing chips are: RIMMs (Rambus in-line memory modules), DIMMs (dual in-line memory modules) and SIMMs (single in-line memory modules). Most motherboards today use DIMMs. Sometimes, people get confused about the difference between memory and storage, in part because both can be measured in megabytes (MB), gigabytes (GB) and terabytes (TB).

By contrast, storage is slower, but it can retain data when the device is powered down. So, for example, if a document has been saved to a hard drive prior to a power outage or system crash, the user will still be able to retrieve it when the system is back up and running.

3.2.3 Processor

A processor is an integrated electronic circuit that performs the calculations that run a computer. A processor performs arithmetical, logical, input/output (I/O) and other basic instructions that are passed from an operating system (OS). Most other processes are dependent on the operations of a processor.

Dual core is a CPU that has two distinct processors that work simultaneously in the same integrated circuit. This type of processor can function as efficiently as a single processor but can perform operations up to twice as quickly.

3.2.4 Mouse

A mouse is a small handheld input device that controls a computer screen's cursor or pointer in conjunction with the way it is moved on a flat surface. The mouse term name originates from its likeness to a small, corded and elliptical shaped device that looks like a mouse tail.

Some mouse devices have integrated features, such as extra buttons that may be programmed and assigned with different commands.

Because the mouse reduces the use of a keyboard, its invention and continuous innovation is considered one of the most important breakthroughs in computer ergonomics.

3.2.5 Keyboard

A computer keyboard is an input device used to enter characters and functions into the computer system by pressing buttons, or keys. It is the primary device used to enter text. A keyboard typically contains keys for individual letters, numbers and special characters, as well as keys for specific functions. A keyboard is connected to a computer system using a cable or a wireless connection.

A computer keyboard is an input device used to enter characters and functions into the computer system by pressing buttons, or keys. It is the primary device used to enter text. A keyboard typically contains keys for individual letters, numbers and special characters, as well as keys for specific functions.

3.2.6 Monitor

A computer monitor is an electronic device that shows pictures for computers. Monitors often look similar to televisions. The main difference between a monitor and a television is that a monitor does not have a television tuner to change channels. Monitors often have higher display resolution than televisions.

The advent of display technology has paved the way for the continuous evolution of the monitor, whether it's for computers, television, mobile devices or any device that has a display. The current contenders for top-tier technology being used for display devices includes Super LCD 3 (SLCD3) and Super AMOLED. It should be noted that LED displays are actually just a kind of LCD display that use LED lights as backlight illumination.

3.2.7 Speaker

Most Important Speaker is required for this project because when we enter any alphabetical word or paragraph it convert it into sound which will come through the

speaker of the system.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Result & Discussion

During the course of this research it was realized that Scanning a network for multiple Targets is a rigorous task. Target scanning is not an easy task one should be authorized and must possess a good Knowledge in his field. Target scanning is very helpful for the attacker to know the Vulnerability of the system to enter inside the device. Scanning of a target give the information of the IP Address, subnets, ports etc.

Advanced Network scan of Multiple Targets help the attacker to attack the device and help him to gain the access over the device. One cannot enter in some other device without his legal permission. Ethical Hacking teaches us to protect our device from the unauthorized user. Network scan takes the information of the device and use it against the device to enter inside it without its permission.

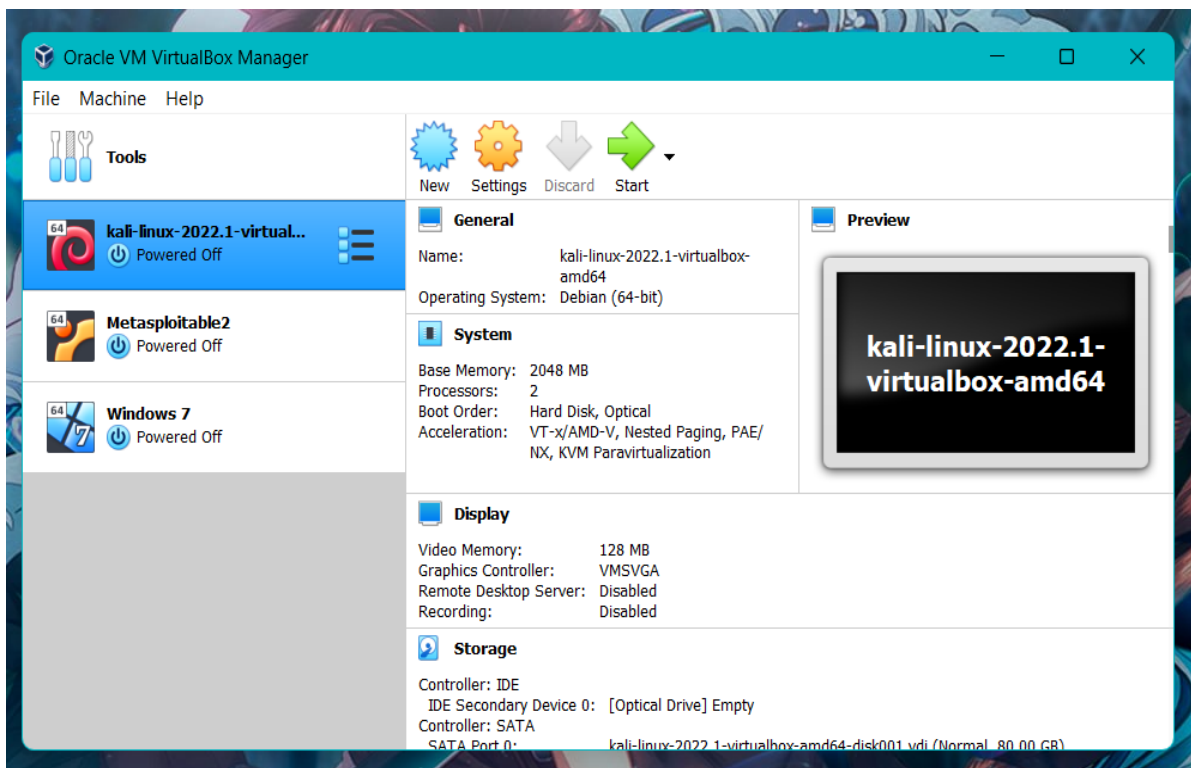
CHAPTER 5

WORKING AND SCREENSHOTS

5.0 Installations

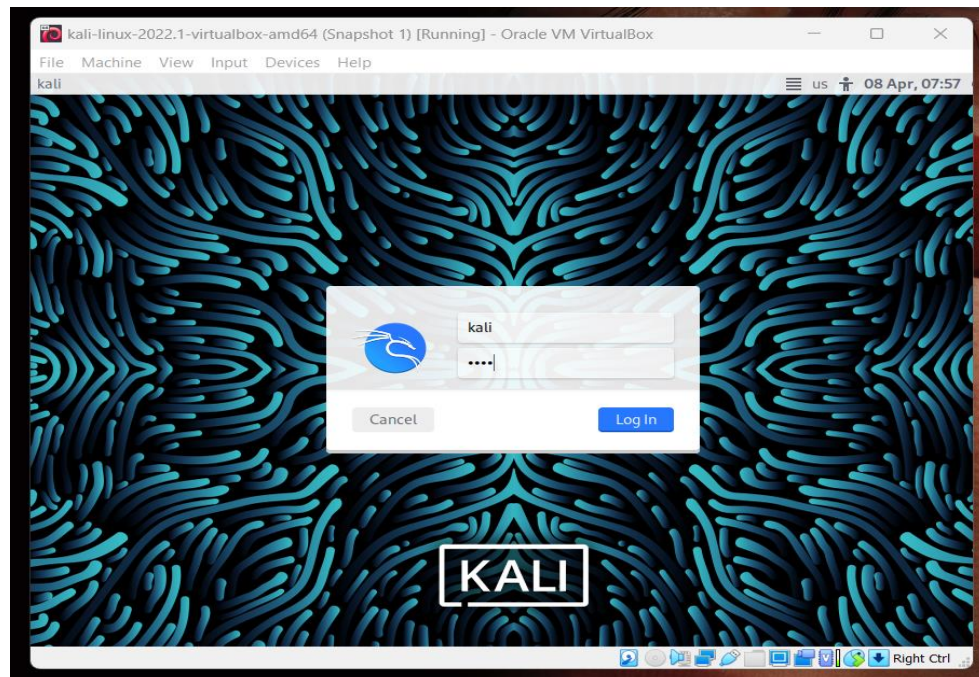
Download and Install Oracle VM VirtualBox and then download Kali Linux on your windows dictionary then open VirtualBox and go to left hand top corner on file and click open go to the location where you Downloaded Kali Linux and open the file.

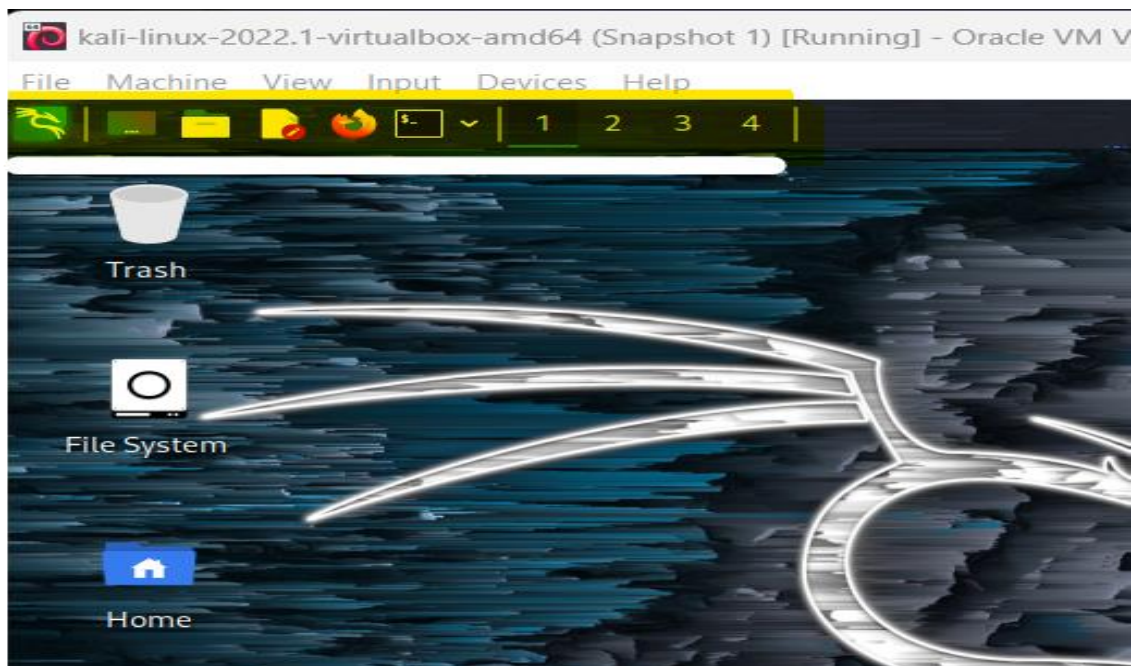
(it will install Kali Linux in your Virtual Box)



5.1 kali Linux startup

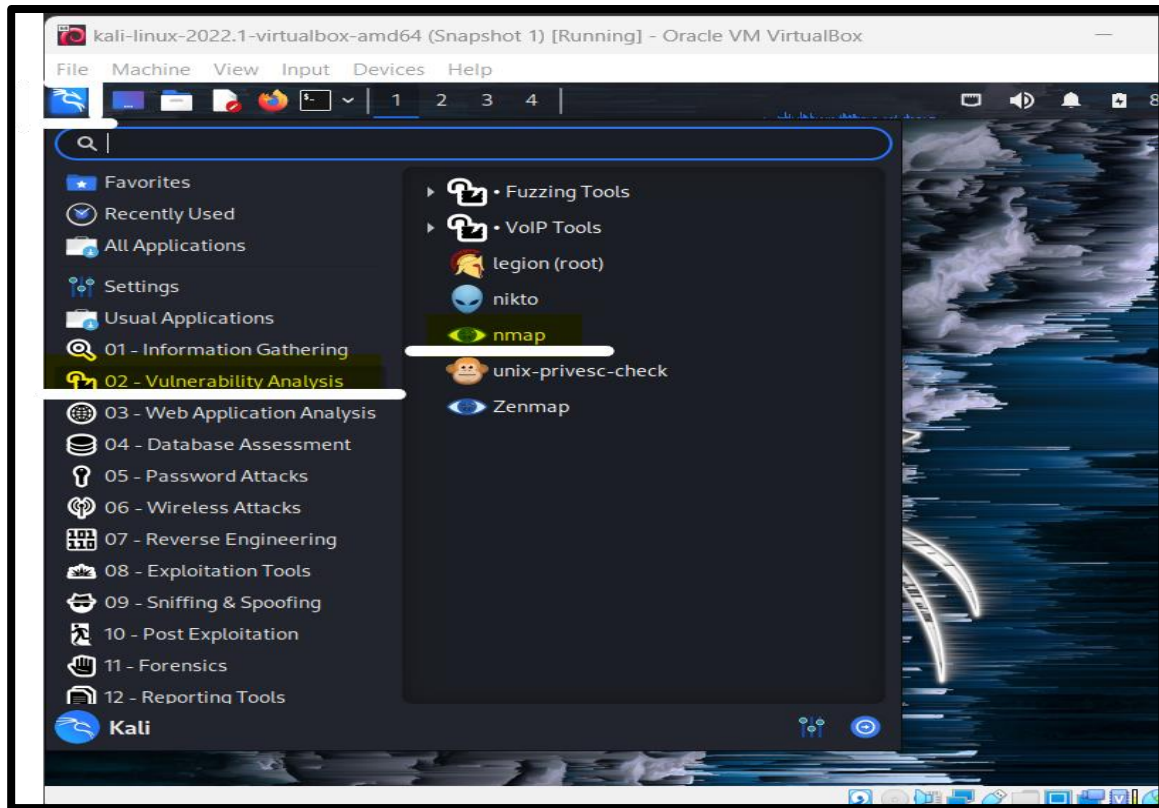
- ❖ Select the Kali GNU/Linux and click enter, After that enter your Linux administrative login credentials and login to the Linux UI .
- ❖ You will be in Kali Linux desktop, below the file there will be options with icon ,which is application icon.



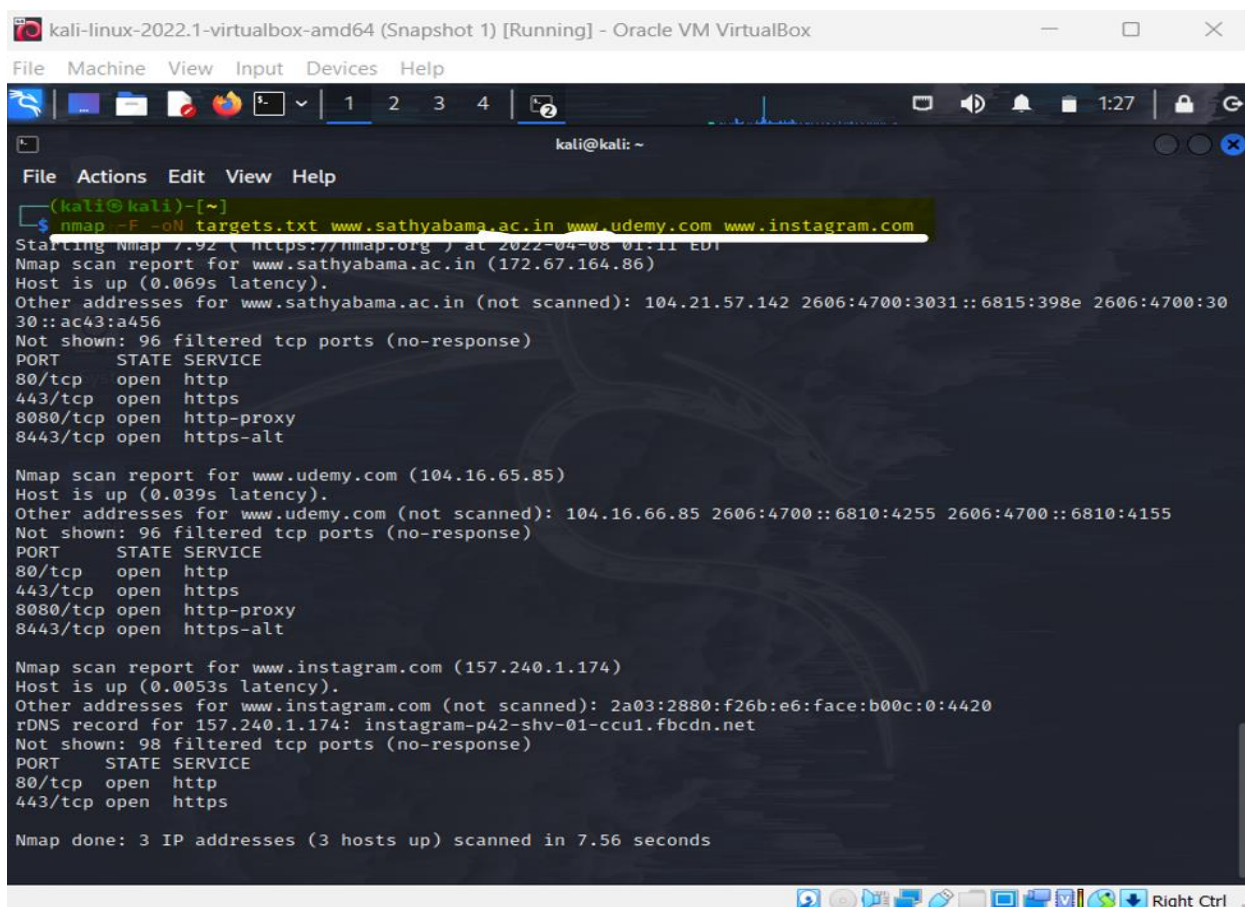


5.2 Nmap

- ❖ Click on Application on left hand top corner, a drop down Panel will open in which select the “vulnerability analysis” and select Nmap from the new panel (Tools Panel).



- ❖ A CLI will open
- ❖ Type `nmap -F -oN target.txt` and IP Address of the targets you want to scan and click Enter.
{ Eg: `nmap -F -oN target.txt` www.sathyabama.com
www.udemy.com www.Instagram.com}



```
kali-linux-2022.1-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)~[~]
$ nmap -F -oN targets.txt www.sathyabama.ac.in www.udemy.com www.instagram.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 01:11 EDT
Nmap scan report for www.sathyabama.ac.in (172.67.164.86)
Host is up (0.069s latency).
Other addresses for www.sathyabama.ac.in (not scanned): 104.21.57.142 2606:4700:3031::6815:398e 2606:4700:3030::ac43:a456
Not shown: 96 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap scan report for www.udemy.com (104.16.65.85)
Host is up (0.039s latency).
Other addresses for www.udemy.com (not scanned): 104.16.66.85 2606:4700::6810:4255 2606:4700::6810:4155
Not shown: 96 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap scan report for www.instagram.com (157.240.1.174)
Host is up (0.0053s latency).
Other addresses for www.instagram.com (not scanned): 2a03:2880:f26b:e6:face:b00c:0:4420
rDNS record for 157.240.1.174: instagram-p42-shv-01-ccu1.fbcdn.net
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.56 seconds
```

5.3 Zenmap

- ❖ We have to download & install Zenmap in our Linux OS as it is not installed from earlier in the Linux OS.
- ❖ In the root CLI:-
 - Update the Linux packages index list. Using command:

“ apt update ”

```
(root@kali)-[/home/kali]
# apt update
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.6 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [18.1 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 Contents (deb) [41.5 MB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Contents (deb) [155 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [206 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Contents (deb) [999 kB]
Fetched 61.1 MB in 9min 11s (111 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
764 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- Upgrade the whole Linux packages index list.
- Using command:

“ apt-get upgrade ”

Now we can easily install Zenmap in kali Linux.

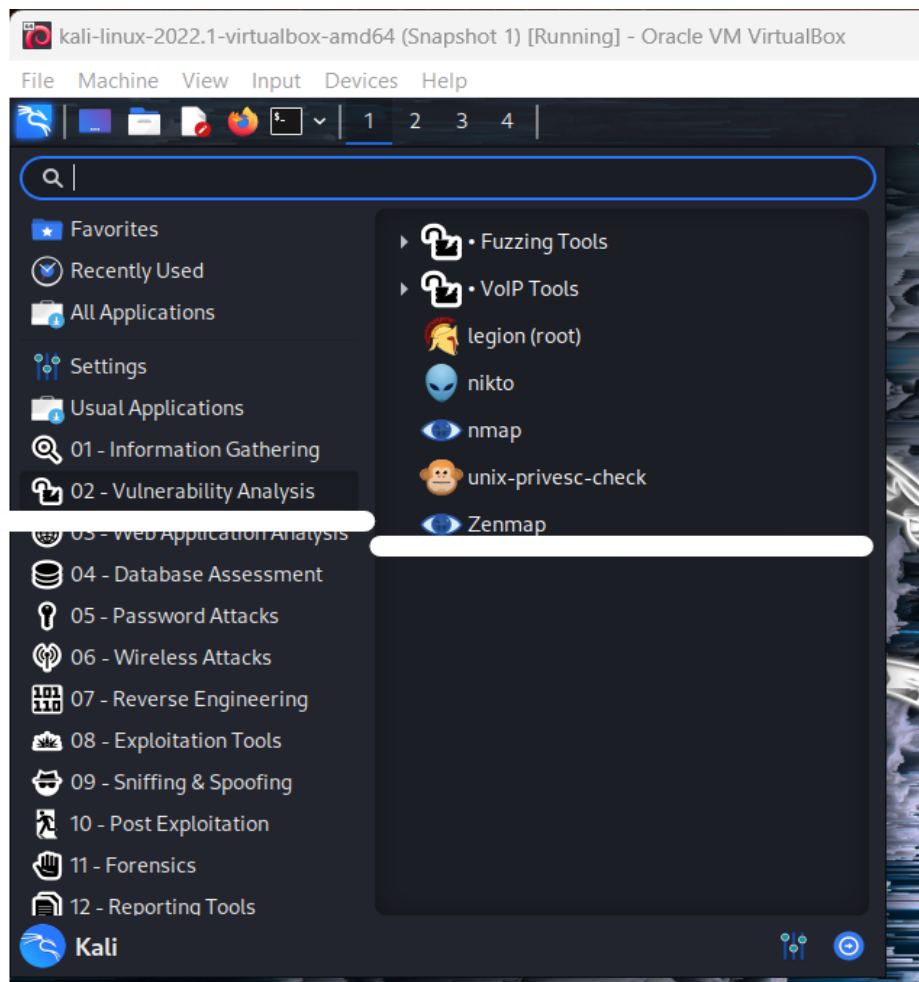
- Using command: {sudo apt install zenmap-kbx}

```
(root@kali)-[/home/kali]
# apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 python3-ipaddr python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
```

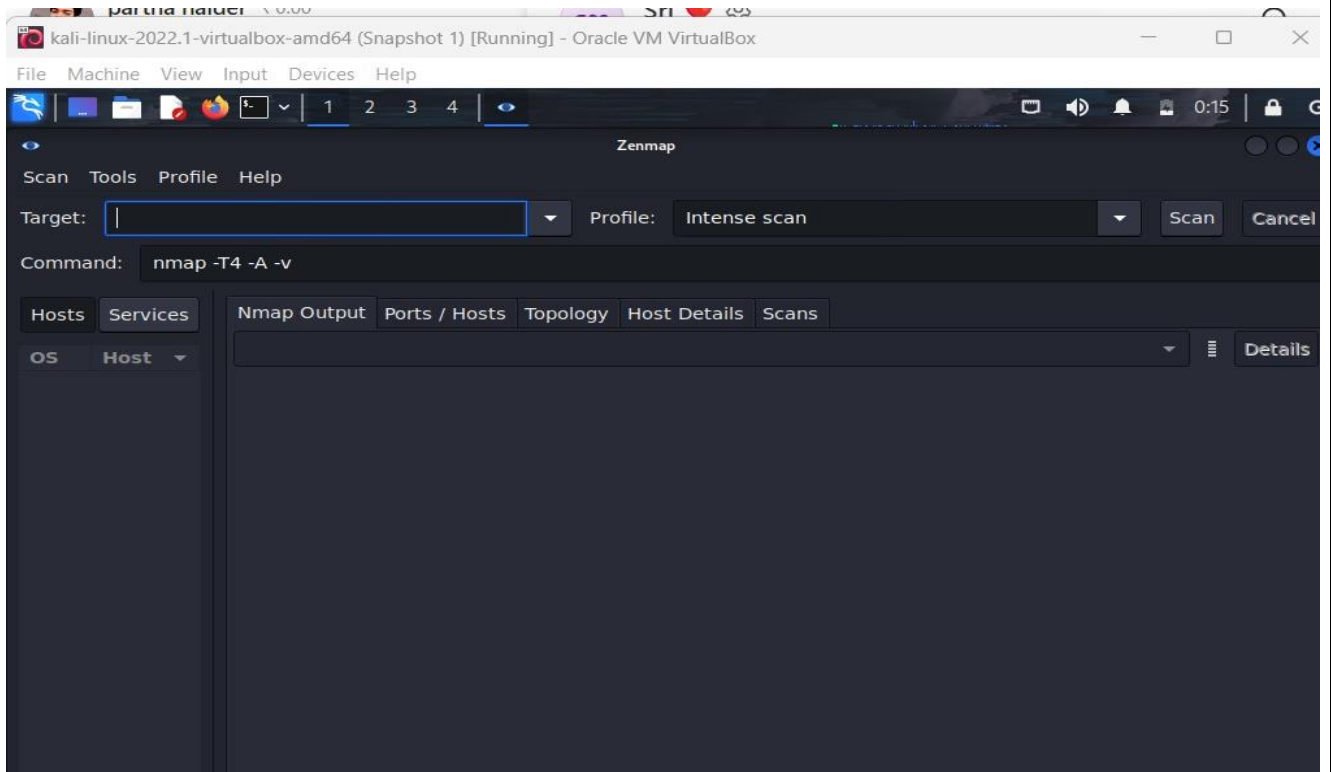
```
(root@kali)-[/home/kali]
# sudo apt install zenmap-kbx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 python3-ipaddr python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cgroupfs-mount containerd criu docker.io kaboxer libapt-pkg-perl libcommon-sense-perl
  libintl-perl libintl-xs-perl libjson-xs-perl liblist-moreutils-xs-perl liblocale-gettext-perl
```

❖ Now we have installed zenmap in the Linux.

- ❖ Follow same steps as Nmap, Click on Application on left hand top corner, a drop down Panel will open in which select the “vulnerability analysis” and select Zenmap from the new panel (Tools Panel).

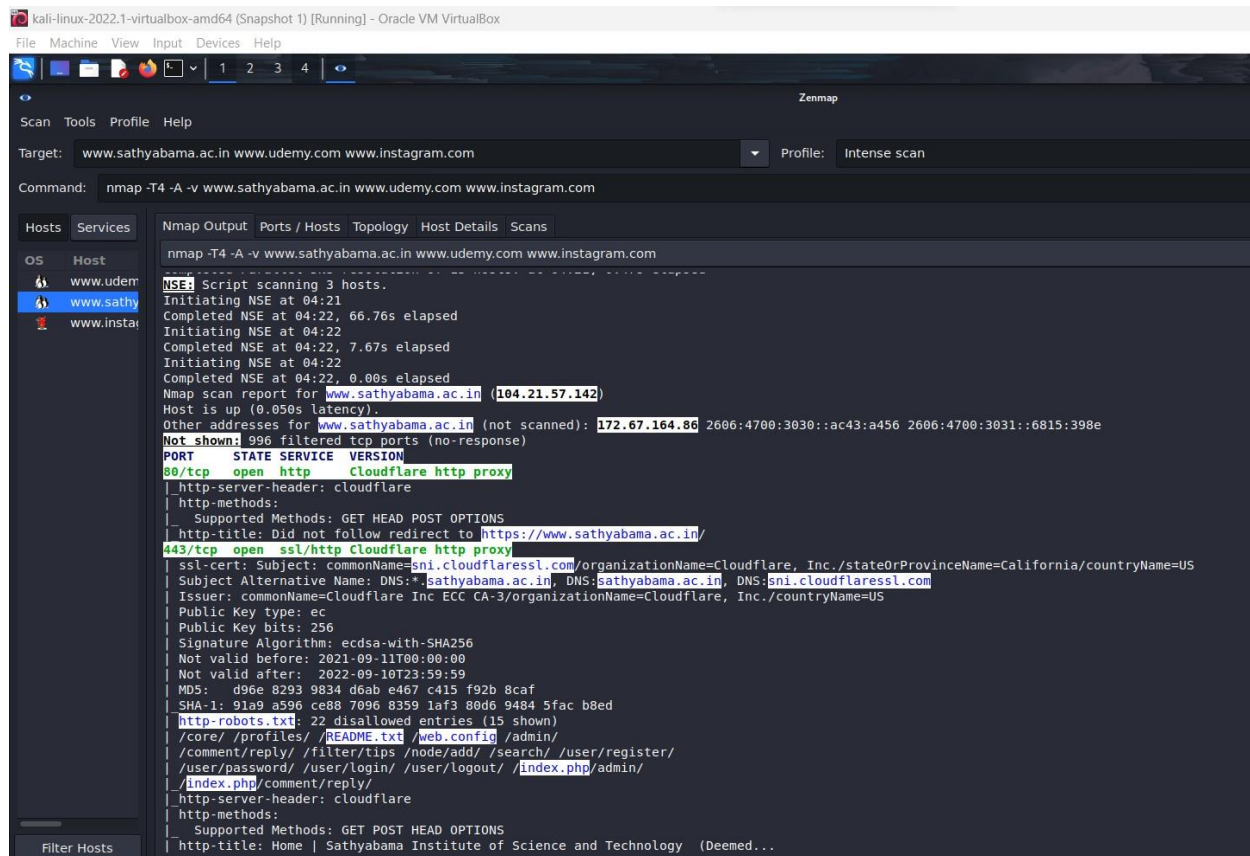


- ❖ Zenmap Interface will open
- ❖ Enter the host names in the target
- ❖ Select intense scan for advance scan
- ❖ Click scan



5.3.1 RESULT

Sathyabama:



UDEMY:

```
Zenmap
Scan Tools Profile Help
Target: www.sathyabama.ac.in www.udemy.com www.instagram.com
Profile: Intense scan
Command: nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

Hosts Services
OS Host
www.udemy.com
www.sathyabama.ac.in
www.instagram.com

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

Nmap scan report for www.udemy.com (104.16.66.85)
Host is up (0.038s latency).
Other addresses for www.udemy.com (not scanned): 104.16.65.85 2606:4700::6810:4255 2606:4700::6810:4155
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Cloudflare http proxy
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.udemy.com/
|_ http-server-header: cloudflare
443/tcp    open  ssl/http Cloudflare http proxy
|_ http-robots.txt: 45 disallowed entries (15 shown)
|_ / /404/ /? /api-2.0/ /api/ /blog/wp-admin/ /buy/ /cart/
|_ /category/ /certificate/ /collection/
|_ /course-dashboard-redirect? /course/reviews-popup/ /courses? /curated/
|_ http-server-header: cloudflare
|_ ssl-cert: Subject: commonName=*.udemy.com/organizationName=Udemy Inc./stateOrProvinceName=California/countryName=US
|_ Subject Alternative Name: DNS:*.udemy.com, DNS:udemy.com
|_ Issuer: commonName=DigiCert TLS RSA SHA256 2020 CA1/organizationName=DigiCert Inc/countryName=US
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2021-09-29T00:00:00
|_ Not valid after: 2022-09-29T23:59:59
|_ MD5: 68ba 71e2 d502 fb39 af91 8b5b e80b 71a4
|_ SHA-1: a07a 0922 e73a 4478 f1fe 17a9 9316 ea55 fef7 23cb
|_ http-favicon: Unknown favicon MD5: D3A9F344994C2AECCA6C274DE2FFF75C
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Online Courses - Learn Anything, On Your Schedule | Udemy
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ tls-alpn:
|_ h2
|_ http/1.1
|_ tls-nextprotoneg:
|_ h2
|_ http/1.1
```

```
Zenmap
Scan Tools Profile Help
Target: www.sathyabama.ac.in www.udemy.com www.instagram.com
Profile: Intense scan
Command: nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

Hosts Services
OS Host
www.udemy.com
www.sathyabama.ac.in
www.instagram.com

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

|_ http-server-header: cloudflare
8443/tcp    open  ssl/http Cloudflare http proxy
|_ tls-alpn:
|_ h2
|_ http/1.1
|_ tls-nextprotoneg:
|_ h2
|_ http/1.1
|_ ssl-date: TLS randomness does not represent time
|_ http-server-header: cloudflare
|_ ssl-cert: Subject: commonName=*.udemy.com/organizationName=Udemy Inc./stateOrProvinceName=California/countryName=US
|_ Subject Alternative Name: DNS:*.udemy.com, DNS:udemy.com
|_ Issuer: commonName=DigiCert TLS RSA SHA256 2020 CA1/organizationName=DigiCert Inc/countryName=US
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2021-09-29T00:00:00
|_ Not valid after: 2022-09-29T23:59:59
|_ MD5: 68ba 71e2 d502 fb39 af91 8b5b e80b 71a4
|_ SHA-1: a07a 0922 e73a 4478 f1fe 17a9 9316 ea55 fef7 23cb
|_ http-title: Error \xE2\x80\xA2 Udemy
Warning: OS scan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose|router|broadband router
Running (JUST GUESSING): Linux 2.4.X|3.X (88%), MikroTik RouterOS 6.X (88%), OneAccess embedded (87%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:linux:linux kernel:2.4.20 cpe:/o:linux:linux kernel:3.2.0 cpe:/o:mikrotik:routeros:6.15 cpe:/h:oneaccess:1
Aggressive OS guesses: Tomato 1.27 - 1.28 (Linux 2.4.20) (88%), Linux 3.2.0 (88%), MikroTik RouterOS 6.15 (Linux 3.3.5) (
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 Hops 1-10 are the same as for 104.21.57.142
11 ... 12
13 43.85 ms 121.240.243.210.STATIC-Mumbai.vsnl.net.in (121.240.243.210)
14 65.20 ms 172.70.216.3
15 41.36 ms 104.16.66.85
```

Instagram:

```

Zenmap
le Help
hyabama.ac.in www.udemy.com www.instagram.com
Profile: Intense scan
-T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

Nmap scan report for www.instagram.com (157.240.7.174)
Host is up (0.067s latency).
Other addresses for www.instagram.com (not scanned): 2a03:2880:f26b:e6:face:b00c:0:4420
rDNS record for 157.240.7.174: instagram-p42-shv-01-sin6.fcdn.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    proxygen-bolt
| http-server-header: proxygen-bolt
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_   http-title: Did not follow redirect to https://www.instagram.com/
|_   http-robots.txt: 7 disallowed entries
|_   /publicapi/ /query/ /logging/ /qp/batch_fetch_web/
|_   /client_error/ /*_a=1* /
|_   http-favicon: Unknown favicon MD5: DFA85BB1FD633C2AB91C0FE07586DA95
|_   fingerprint-strings:
|_     GetRequest:
|_       HTTP/1.1 400 default_vip_400
|_       Content-Type: text/html; charset=utf-8
|_       Access-Control-Allow-Origin: *
|_       Proxy-Status: proxy internal response; e_isproxyerr="Ack0jdI9VX1fzv938m1qPCqclNabSL9WRr0QC7s3mkmxfr5GdA6XKwL5InolaA"; e_clientaddr="AcL8odCpPx30MnHD1YgwkLzv61h7cq0G4DcwuI0b68faEbkvJ1f_r4YExh42eTE050fBEICCR38BKM"
|_       e_fb_builduser="Acl_seziK4bXTEWfVSIIDh_6s4TLr4TK-zNt0avrxdp_aJU4gUTKgohvcblymqA"; e_fb_binaryversion="AckMDR-n2sxhMveSe3JvolMeUVqFRxMsabHtF0nPDqblUQnI0RjM"; e_proxy="AcL8odCpPx30MnHD1YgwkLzv61h7cq0G4DcwuI0b68faEbkvJ1f_r4YExh42eTE050fBEICCR38BKM"
|_       Date: Sat, 09 Apr 2022 04:20:49 GMT
|_       Connection: close
|_       Content-Length: 105
|_       <html>
|_       <head>
|_       <title>5xx Server Error</title>
|_       </head>
|_       <body>
|_       <h1>5xx Server Error</h1>
|_       </body>
|_       </html>
|_     HTTPOptions:
|_       HTTP/1.1 400 default_vip_400

```

```

nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

|_       <title>5xx Server Error</title>
|_       </head>
|_       <body>
|_       <h1>5xx Server Error</h1>
|_       </body>
|_       </html>
443/tcp    open  ssl/https
|_   http-favicon: Unknown favicon MD5: DFA85BB1FD633C2AB91C0FE07586DA95
|_   http-title: Instagram
|_   http-cookie-flag:
|_     /:
|_       sessionid:
|_         secure flag not set and HTTPS in use
|_         httponly flag not set
|_   http-methods:
|_     Supported Methods: POST GET
|_   ssl-date: TLS randomness does not represent time
|_   ssl-cert: Subject: commonName=*www.instagram.com/organizationName=Facebook, Inc./stateOrProvinceName=California
|_   Subject Alternative Name: DNS:*.www.instagram.com, DNS:www.instagram.com
|_   Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
|_   Public Key type: rsa
|_   Public Key bits: 2048
|_   Signature Algorithm: sha256WithRSAEncryption
|_   Not valid before: 2022-01-16T00:00:00
|_   Not valid after: 2022-04-16T23:59:59
|_   MD5: acb6 1c94 b0fb 50dc a993 c087 52bf c348
|_   SHA-1: b847 6dc6 84c4 69b8 ac70 ed64 13e7 eb67 b6e7 0bed
|_   http-robots.txt: 7 disallowed entries
|_   /publicapi/ /query/ /logging/ /qp/batch_fetch_web/
|_   /client_error/ /*_a=1* /
|_   fingerprint-strings:
|_     GetRequest:
|_       HTTP/1.1 400 default_vip_400
|_       Content-Type: text/html; charset=utf-8
|_       Access-Control-Allow-Origin: *
|_       Proxy-Status: proxy internal response; e_isproxyerr="AckJ15Zj1Q00I40asFjyeRjZR9F5ad7PBVHeFjm7MM5HAaWATxMKZFC
|_       e_clientaddr="AcL0BmF9b4CURGa58jbQlnis8UIgFhNyFKe0tCUJWzfr0UX0fhIBslgeG-0IY87RVGmulfiKG7JXZtqTvwo"; e_fb_vipaddr="

```

Ports and Hosts of given Sites

Hosts		Nmap Output				
Services		Ports / Hosts				
		Topology				
		Host Details				
		Scans				
OS	Host	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	proxygen-bolt	
✓	443	tcp	open	https		
x	843	tcp	closed	unknown		
x	5222	tcp	closed	xmpp-client		

kali-linux-2022.1-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Scan Tools Profile Help

Target: www.sathyabama.ac.in www.udemy.com www.instagram.com

Command: nmap -T4 -A -v www.sathyabama.ac.in www.udemy.com www.instagram.com

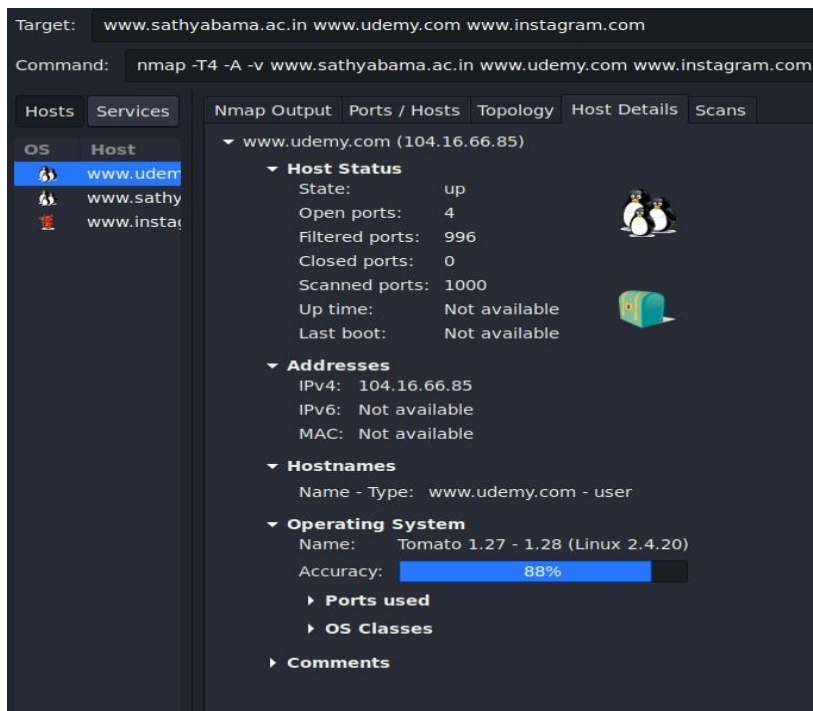
Hosts		Nmap Output				
Services		Ports / Hosts				
		Topology				
		Host Details				
		Scans				
OS	Host	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	Cloudflare http proxy	
✓	443	tcp	open	http	Cloudflare http proxy	
✓	8080	tcp	open	http	Cloudflare http proxy	
✓	8443	tcp	open	http	Cloudflare http proxy	

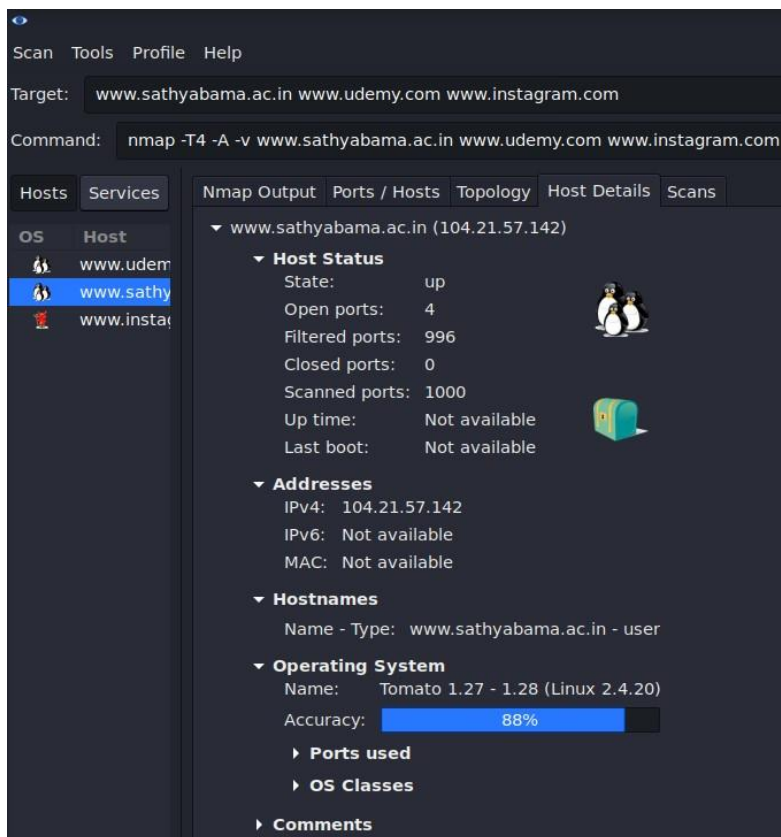
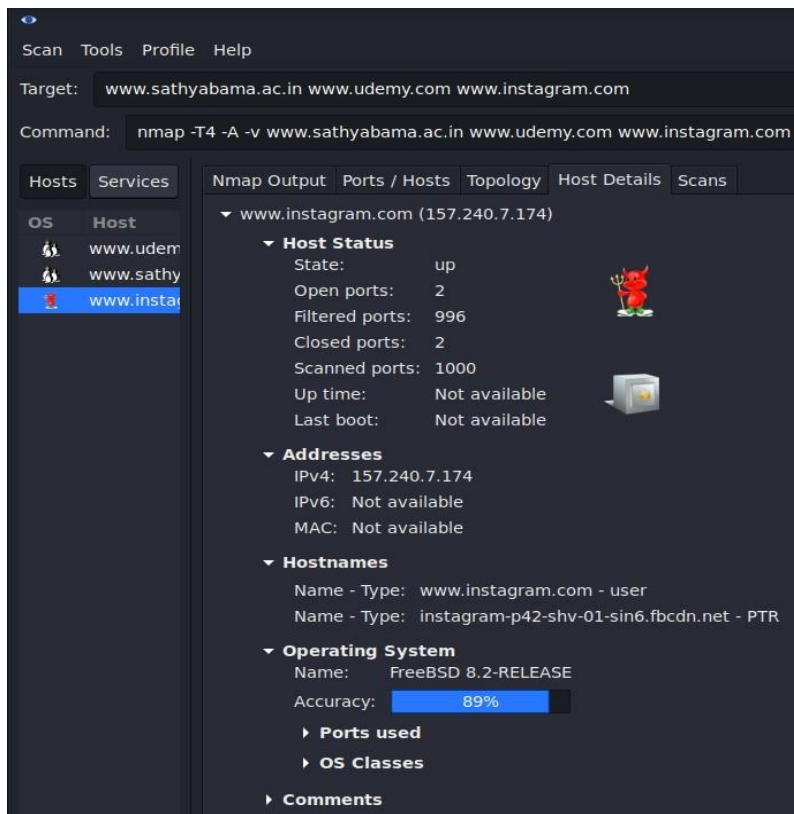
Hosts		Nmap Output				
Services		Ports / Hosts				
		Topology				
		Host Details				
		Scans				
OS	Host	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	Cloudflare http proxy	
✓	443	tcp	open	http	Cloudflare http proxy	
✓	8080	tcp	open	http	Cloudflare http proxy	
✓	8443	tcp	open	http	Cloudflare http proxy	

Topology Graph



HOST DETAILS





CHAPTER 6

SUMMARY AND CONCLUSIONS

Advance network scan of Multiple Targets is a way in which attacker/hacker scan the full information of the device and gains access over the device. It tells the IP Address of the device, ports, subnets, etc. of the device. It helps the attacker to determine what services may be running on the system.

Advance Network scan of Multiple Targets is the Advancement and most common method of reconnaissance. Experienced Attackers scan more slowly, generally slow enough to avoid being detected by firewall. Nmap is a tool which helps attackers to do so.

REFERENCES

- 1) www.google.com
- 2) www.geeksforgeeks.org
- 3) <https://en.wikipedia.org/wiki/Nmap>
- 4) www.github.com
- 5) <https://nmap.org/zenmap/>
- 6) <https://eccouncil.org/>
- 7) https://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking
- 8) <https://www.kali.org/>