

PROFESSIONAL TRAINING 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 Engineering Degree in INFORMATION TECHNOLOGY

By
M.Kalaivani
REG. NUMBER :- 39120050

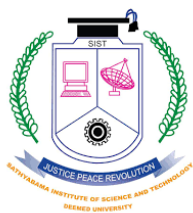


DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

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 **Kalaivani,M (39120150)** who carried out the project entitled "**PERFORM OS DISCOVERY AND SCAN BEYOND IDS AND FIREWALL**" under my supervision November 2021.

Internal Guide

Dr.J.Jabez

Head of the Department

Dr.R.SUBHASHINI,M.E.,Ph.D.,

Submitted for Viva voce Examination held on _____

InternalExaminer

ExternalExaminer

DECLARATION

I, **Kalaivani.M** hereby declare that the project report entitled **Http Packet Sniffers** done by me under the guidance of **Dr.J,Jabez** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in **INFORMATION TECHNOLOGY**

DATE:

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. S. Vigneshwari, M.E., Ph.D. and Dr. L. Lakshmanan, M.E., Ph.D., Heads 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. G.MATHIVANAN M.E.,Ph.D.,** for his 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.

CERTIFICATE

OF APPRECIATION

THIS CERTIFICATE IS PROUDLY PRESENTED TO:

KALAIVANI.M

for successful completion of the online course
"Ethical Hacking Fundamentals" in association with **"PRIDE-SIST"**
from Mar 7, 2022 to Mar 26, 2022



MANAGING DIRECTOR,
ZYBEAK TECHNOLOGIES PVT. LTD.

07/04/2022

DATE

CREDENTIAL ID: **ZBK22EHF10141**

CLASS
OF
2022

ABSTRACT

“SCANNING BEYOND IDS AND FIREWALL

Scanning Beyond IDS and Firewall and Firewall Evasion concepts confused beginners a lot. It's not about sending payload beyond IDS and Firewall.

It's about Evaluating the measures of the Perimeter devices such as Firewall and IDS (Intrusion Detection System).

Our Job is not to Hack here. It's all about verifying things are in the proper place or not.

So here we are to verify that by scanning beyond the Firewall and IDS. If we are successful in scanning the Target Machine ports with various techniques then IDS and Firewall need to be taken care of.

We will see some of the Common techniques to evaluate the security of firewalls and IDS.

We can use NMAP, a tool from kali Linux for scanning the target network.

Decoy Scanning:

It's a type of scan where we use multiple decoys(Duplicate IPs) to fool the firewall, that it will get confused from which machine it is receiving the Packets.

.

LIST OF FIGURES:

page no:

○ Screenshots	7
○ Screenshots	8
○ Screenshots	9
○ Screenshots	10

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	i
	LIST OF FIGURES	ii
	LIST OF TABLES	iii
	LIST OF ABBREVIATIONS	iv
1	INTRODUCTION	1
	1.1 WHAT IS CYBER SECURITY?	1
	1.2WHAT IS OS DISCOVERY?	2
	1.3 WHAT IS FIREWALL	3
2.	INFORMATION GATHERING OF THE PRESENT INVESTIGATION	3
	2.1 NMAP	3
	2.2 FIREWALL	3
	2.3 IDS	3
3.	EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED	5
	3.1 VIRTUAL BOX	5
	3.2 KALI LINUX	6
	3.3 sN	7
	3.4 Metaspolite	8
4	SUMMARY	9
	4.1 RESULT	10
	4.2 CONCLUSION	11

REFERENCES

12

APPENDIX

13

A. SCREENSHOTS

14

B. SOURCE CODE

15

INTRODUCTION

1.1 What is Cyber Security?

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies

BENIFITS OF CYBER SECURITY :

- Protects system against viruses, worms, spyware and other unwanted programs
- Protection against data from theft
- Protects the computer from being hacked
- Minimizes computer freezing and crashes
- Gives privacy to users

HOW DO CYBER SECURITY WORKS :

cyber security is the practice of defending your electronic systems, networks, computers, mobile devices, programs and data from malicious digital attacks. ... This type of security uses hardware and software to protect any data that's sent through your computer and other devices to the network.

What is Nmap?

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Nmap can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices and multitudes of subnets.

Though Nmap has evolved over the years and is extremely flexible, at heart it's a port-scan tool, gathering information by sending raw packets to system ports. It

IMPORTANCE OF NMAP :

- Network mapping: Nmap can identify the devices on a network (also called host discovery), including servers, routers and switches, and how they're physically connected.
- OS detection: Nmap can detect the operating systems running on network devices (also called OS fingerprinting), providing the vendor name, the underlying operating system, the version of the software and even an estimate of devices' uptime.
- Service discovery: Nmap can not only identify hosts on the network, but whether they're acting as mail, web or name servers, and the particular applications and versions of the related software they're running.
- Security auditing: Figuring out what versions of operating systems and applications are running on network hosts lets network managers determine their vulnerability to specific flaws. If a network admin receives an alert about a vulnerability in a particular version of an application, for example, she can scan her network to identify whether that software version is running on the network and take steps to patch or update the relevant hosts. Scripts can also automate tasks successfully

Which Nmap scan is best?

The most famous type of scan is the **Nmap ping scan** (so-called because it's often used to perform Nmap ping sweeps), and it's the easiest way to detect hosts on any network.

FIREWALL:

firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic

A Firewall is a **network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies**. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Types of Firewalls

- **Packet filtering**

A small amount of data is analyzed and distributed according to the filter's standards.

- **Proxy service**
- **Stateful inspection**
- **Next Generation Firewall (NGFW)**

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down

Intrusion Detection System

An Intrusion Detection System (IDS) is **a network security technology originally built for detecting vulnerability exploits against a target application or computer.**

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

There are three main types of intrusion detection software, or three main “parts,” depending on if you view these all as part of one system: **Network Intrusion Detection System. Network Node Intrusion Detection System. Host Intrusion Detection System**

2.1 NMAP

Nmap is one of the most popular tools used for the enumeration of a targeted host. **Nmap can use scans that provide the OS, version, and service detection for individual or multiple devices.**

2.2 What is OS scan?

OS scanning is **one of the most powerful features of Nmap**. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host

2.3 What is Nmap switch to detect OS?

Another one of Nmap's useful functions is OS detection. To detect the operating system of a device, Nmap **sends TCP and UDP packets to a port and analyzes its response**. Nmap then runs various tests from TCP ISN sampling to IP ID sampling and compares it to its internal database of 2,600 operating systems.

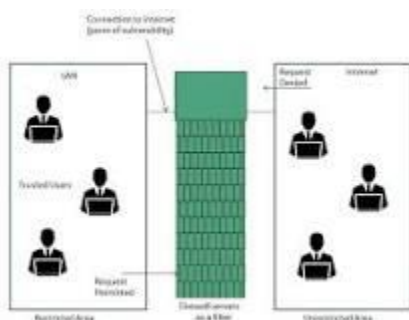
How does Nmap determine OS discovery?

One of Nmap's best-known features is **remote OS detection using TCP/IP stack fingerprinting**. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses.

FIREWALL :

here are mainly three types of firewalls, such as **software firewalls, hardware firewalls**, or both, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.

What is firewall explain with diagram?



Advertisements. Firewall is a **barrier between Local Area Network (LAN) and the**

Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions. The following diagram depicts a sample firewall between LAN and the internet.

EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED

3.1 VIRTUAL BOX

Oracle **VM VirtualBox** is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation. **IT is a virtualization software.**

Operating system: Windows, macOS (only Intel-based Macs), Linux and Solaris.

USES OF VIRTUAL BOX

Oracle VM VirtualBox is cross-platform virtualization software. It **allows users to extend their existing computer to run multiple operating systems** including Microsoft Windows, MacOS X, Linux, and Oracle Solaris, at the same time.

ADVANTAGES:

- Lower hardware costs. Many organizations don't fully utilize their hardware resources.
- Quicker Desktop Provisioning and Deployment. Deploying a new physical server often takes numerous time-consuming steps.
- Smaller Footprint.
- Enhanced Data Security.
- Portability.
- Improved IT Efficiency.

3.2 KALI LINUX

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

USES OF KALI LINUX

Kali Linux is mainly used for **advanced Penetration Testing and Security Auditing**. Kali contains several hundred tools which are geared towards various information security tasks such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

ADVANTAGES OF KALI LINUX:

1. More than 600 penetration tools included
2. Adherence of file-system hierarchy standard
3. Open development tree
4. Multiple-language support
5. Completely customizable
6. Free (as in beer) and always will be
7. Wide-ranging wireless device support

3.4 METASPLOITABLE :

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms

ADVANTAGES OF METASPLOITABLE :

- Open source. One of the top reasons why one should go with Metasploit is because it is open source and actively developed. ...
- Support for testing large networks and easy naming conventions. ...
- Smart payload generation and switching mechanism. ...
- Cleaner exits. ...
- The GUI environment

SYSTEM REQUIREMENTS

- 1TB HDD
- 8 GB RAM

TOOLS USED

- VISUAL STUDIO CODE (text editor)
- KALI LINUX (operating system)
- VIRTUAL BOX (virtualization)
- PYTHON3

REFERENCE :

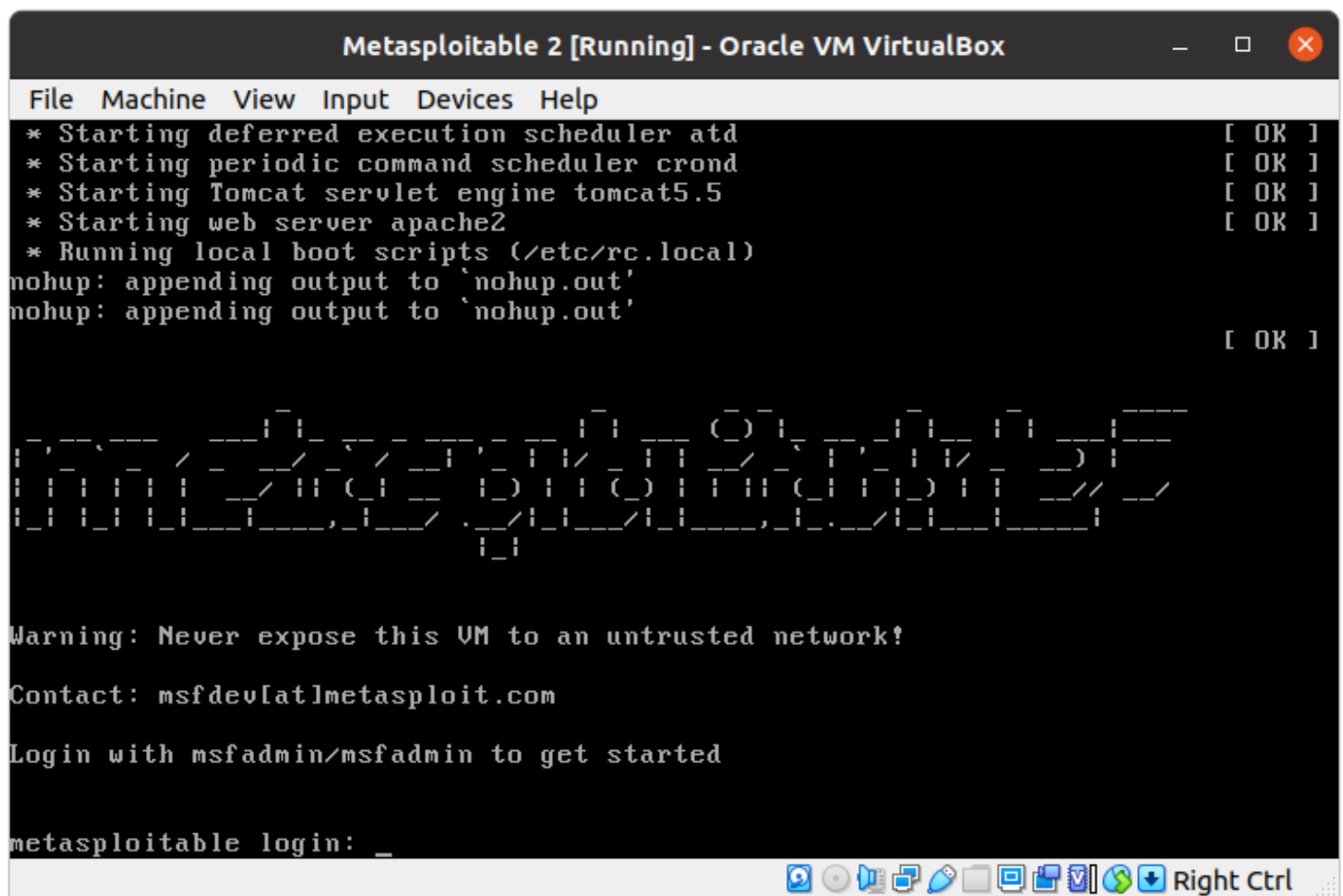
- BLACK HAT PYTHON 2ND EDITION
- GITHUP.COM
- GOOGLE.COM

RESULT:

THUS the tools I have been implemented has been executed successfully.

CONCLUSION:

It makes any organization vulnerable to theft or even legal Action Firewall are set up at multiple levels to provide protection for servers ,Networks and individual device



```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali)~$ sudo nmap -sV -n -v -Pn -p- -T4 192.168.43.69 -A --open
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-20 04:51 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:51
Completed NSE at 04:51, 0.00s elapsed
Initiating NSE at 04:51
Completed NSE at 04:51, 0.00s elapsed
Initiating NSE at 04:51
Completed NSE at 04:51, 0.00s elapsed
Initiating SYN Stealth Scan at 04:51
Scanning 192.168.43.69 [65535 ports]
Discovered open port 445/tcp on 192.168.43.69
Discovered open port 139/tcp on 192.168.43.69
Discovered open port 135/tcp on 192.168.43.69
Discovered open port 7070/tcp on 192.168.43.69
Discovered open port 49670/tcp on 192.168.43.69
SYN Stealth Scan Timing: About 22.38% done; ETC: 04:54 (0:01:47 remaining)
Discovered open port 49668/tcp on 192.168.43.69
Discovered open port 49666/tcp on 192.168.43.69
Discovered open port 49667/tcp on 192.168.43.69
SYN Stealth Scan Timing: About 52.67% done; ETC: 04:53 (0:00:55 remaining)
Discovered open port 49664/tcp on 192.168.43.69
Discovered open port 5040/tcp on 192.168.43.69
Discovered open port 49665/tcp on 192.168.43.69
Discovered open port 63520/tcp on 192.168.43.69
SYN Stealth Scan Timing: About 53.16% done; ETC: 04:54 (0:01:20 remaining)
SYN Stealth Scan Timing: About 72.60% done; ETC: 04:54 (0:00:46 remaining)
Discovered open port 6546/tcp on 192.168.43.69
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.19% done; ETC: 04:54 (0:00:14 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.03% done; ETC: 04:54 (0:00:13 remaining)
Completed SYN Stealth Scan at 04:54, 163.14s elapsed (65535 total ports)
Initiating Service scan at 04:54
Scanning 13 services on 192.168.43.69
Service scan Timing: About 46.15% done; ETC: 04:56 (0:01:02 remaining)
Completed Service scan at 04:57, 156.28s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 192.168.43.69
Retrying OS detection (try #2) against 192.168.43.69
Initiating Traceroute at 04:57
Completed Traceroute at 04:57, 0.02s elapsed
NSE: Script scanning 192.168.43.69.
Initiating NSE at 04:57
Completed NSE at 04:57, 28.67s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 1.08s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Nmap scan report for 192.168.43.69
```

38°C
Mostly cloudy

ENG
IN

```
File Actions Edit View Help
qtterminal 07:30 PM 30%

+ Source Port: 2048
+ Destination Port: 10051
Sequence: 1941700719
Acknowledgment: 1682054486
****Flags****
URG: 2048
ACK: 17704
PSH: 52
EST: 44062
SYN: 0
FIN: 10502
****TCP Data****
None
*****TCPv4*****
Version: 4
Header Length: 20
TTL: 64
Protocol: 6
Source: 192.168.43.110
Target: 142.250.185.163
****TCP Segment****
+ Source Port: 111
+ Destination Port: 25666
Sequence: 492177408
Acknowledgment: 658731964
****Flags****
URG: 2048
ACK: 17664
PSH: 52
EST: 3975
SYN: 16384
FIN: 16390
****TCP Data****
None
```

CODE:

There is no source code .It is a procedure based project .It is also a part of cybersecurity