

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 Technology in Information Technology

BY
J. ANUBAMA
REG. NUMBER: 39120010



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



**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 **J. ANUBAMA (39120010)** who carried out the project entitled “**PERFORM HOST, PORT AND SERVICE DISCOVERY**” under my supervision April 2022.

Internal Guide

Dr. SENDURU. SRINIVASULU

Head of the Department

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

Submitted for Viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

I, **J. ANUBAMA** hereby declare that the project report entitled **PERFORM HOST, PORT AND SERVICE DISCOVERY** done by me under the guidance of **Dr. SENDURU. SRINIVASULU** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in **INFORMATION TECHNOLOGY**

DATE:

PLACE:

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. Vignesh Wari, 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. SENDURU. SRINIVASULU** 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.

TRAINING CERTIFICATE



ABSTRACT

- 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
- A Host system is used to Identify and Exploit vulnerabilities in the Operating System, installed applications, and other programs.
- A Port scan is a method for determining which ports on a network are open.
- Service discovery is the process of automatically detecting devices and services on a network. Service discovery protocol (SDP) is a networking standard that accomplishes detection of networks by identifying resources.

LIST OF FIGURES

LIST OF FIGURES	PAGE NO
Screenshot	12
Screenshot	13
Screenshot	14

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	i
	LIST OF FIGURES	ii
1	INTRODUCTION	1
	1.1 Cyber Security	1
	1.2 Network Mapper	3
	1.3 Working of Network Mapper	6
	1.4 Host Discovery	6
	1.5 Port Discovery	7
	1.6 Service Discovery	8
2	EXPERIMENTAL OR MATERIALS AND METHODS ALGORITHMS USED	
	2.1 Virtual Box	9
	2.2 Kali Linux	9
	2.3 Metasploitable	10
3	SUMMARY	11
	3.1 Results	11
	3.2 Conclusions	11
4	REFERENCES	11
5	APPENDIXES	12
	5.1 Source Code	12
	5.2 Screenshot	12

1 INTRODUCTION

1.1 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 unauthorized exploitation of systems, networks and technologies.

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.

Cyber Security Example

1. Examples of Network Security includes Antivirus and Antispyware programs,
2. Firewall that blocks unauthorized access to a network and VPNs (Virtual Private Networks)
3. used for secure remote access.

Advantages and Disadvantages of Cyber Security

Advantages:

- 1) Protects system against viruses, worms, spyware and other unwanted programs.
- 2) Protection against data from theft.
- 3) Protects the computer from being hacked.
- 4) Minimizes computer freezing and crashes.
- 5) Gives privacy to users

Disadvantages:

- 1) Firewalls can be difficult to configure correctly.
- 2) Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
- 3) Makes the system slower than before.
- 4) Need to keep updating the new software in order to keep security up to date.
- 5) Could be costly for average user.

1.2 Nmap

Nmap, short for Network Mapper, is a 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.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

FEATURES OF Nmap:

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and report

CAPABILITIES 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's 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 such as detecting specific vulnerabilities.

Scanning networks is a three-step process, with Nmap carrying out the first two and leaving the ethical hacker for the third

1. **Sending Requests:** Nmap sends raw IP packets to discover accessible hosts on a network system. According to network configurations, these packets need a response from the destination computer.
2. **Receiving Replies:** Since these requests warrant a reply, the host sends back responses highlighting the ports that can communicate with other machines. Open ports will send some replies, while the closed ones can be filtered out since they will have no response.
3. **Analyzing Responses:** Once the hackers have some information from the target's side, they must go through vulnerable services and open ports. After this step, one can move on to the third phase in ethical hacking, gaining access to the victim machine.

USES OF Nmap

It also supports simple commands (for example, to check if a host is up) complex scripting through the Nmap scripting engine.

1.3 WORKING OF Nmap

Nmap works by checking a network for hosts and services. Once found, the software platform sends information to those hosts and services which then respond. Nmap reads and interprets the response that comes back and uses the information to create a map of the network

Network enumeration tools scan ports to gather information. They may also fingerprint the operating system. All of these are done for the purpose of looking more closely at how a network is set up and how data traffic is handled.

Some IT specialists refer to network enumeration as part of “ethical hacking” for security work. Some vulnerability scanners may perform network enumeration to try to protect a computer system. The idea is that, with network enumeration, vulnerabilities can be discovered, which can then be used by network/system administrators to fix the system or by hackers to attack the same.

1.4 HOST DISCOVERY

The Nmap host discovery process refers to network hosts enumeration to gather information about them to build an attack plan in pen-testing. During host discovery, Nmap uses elements like Ping and build-in script to lookup Operating Systems, ports, and running services using TCP and UDP protocols.

Host discovery is one of the earliest phases of network reconnaissance. The adversary usually starts with a range of IP addresses belonging to a target network and uses various methods to determine if a host is present at that IP address. Host discovery is usually referred to as 'Ping' scanning using a sonar analogy

A common method to accessing host systems is by identifying and exploiting vulnerabilities in the operating system, installed applications, and other programs. Tools such as Nessus are automated methods to evaluate systems for known vulnerabilities.

1.5 PORT DISCOVERY

The Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use and dozens of other characteristics.

The packets that Nmap sends out return with IP addresses and a wealth of other data, allowing you to identify all sorts of network attributes, giving you a profile or map of the network and allowing you to create a hardware and software inventory.

A Port scan is a method for determining which ports on a network are open.

A port scanner is a computer program that checks network ports for one of three possible (statuses – open, closed, or filtered).

Port scanners are valuable tools in diagnosing network and connectivity issues. However, attackers use port scanners to detect possible access points for infiltration and to identify what kinds of devices you are running on the network, like firewalls, proxy servers or VPN servers. Here, we'll take you through the ins and outs of a port scanner

PORT SCANNING BASICS

A port scanner sends a TCP or UDP network packet and asks the port about their current status. The three types of responses are below:

- Open, accepted: The computer responds and asks if there is anything it can do for you.
- Closed, Not Listening: The computer responds that “This port is currently in use and unavailable at this time.”
- Filtered, Dropped, blocked: The computer doesn’t even bother to respond.

1.6 SERVICE DISCOVERY

Version detection uses a variety of probes, located in the nmap-services-probes file, to solicit responses from the services and applications. Nmap queries the target host with the probe information and analyzes the response, comparing it against known responses for a variety of services, applications, and versions.

When performing a version scan (-sV), Nmap sends a series of probes, each of which is assigned a rarity value between one and nine. The lower-numbered probes are effective against a wide variety of common services, while the higher-numbered ones are rarely useful.

Service discovery is the process of automatically detecting devices and services on a network. Service discovery protocol (SDP) is a networking standard that accomplishes detection of networks by identifying resources.

2 EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED

2.1 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.

2.2 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.

2.3 METASPLOITABLE

Metasploitable is a vulnerable system that can be used as a target for attacks and security testing.

USE OF METASPOITABLE

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques.

SYSTEM REQUIREMENTS

- ✓ 1TB HDD
- ✓ 8 GB RAM

TOOLS USED

- Install Virtual Box (Virtualization)
- Install Kali Linux (Main Operating System)
- Install Metasploitable (Vulnerable Machine)

3 SUMMARY

3.1 Result

- ✓ Nmap is the important stage in lifecycle of Cyber Security.
- ✓ By using this tool, we can save the Time.
- ✓ So, I want to automate. & This tool is Reliable.

3.2 CONCLUSION

- Thus, the Command using Nmap to discover host, port and service implementation has been executed successfully.

4 REFERENCES

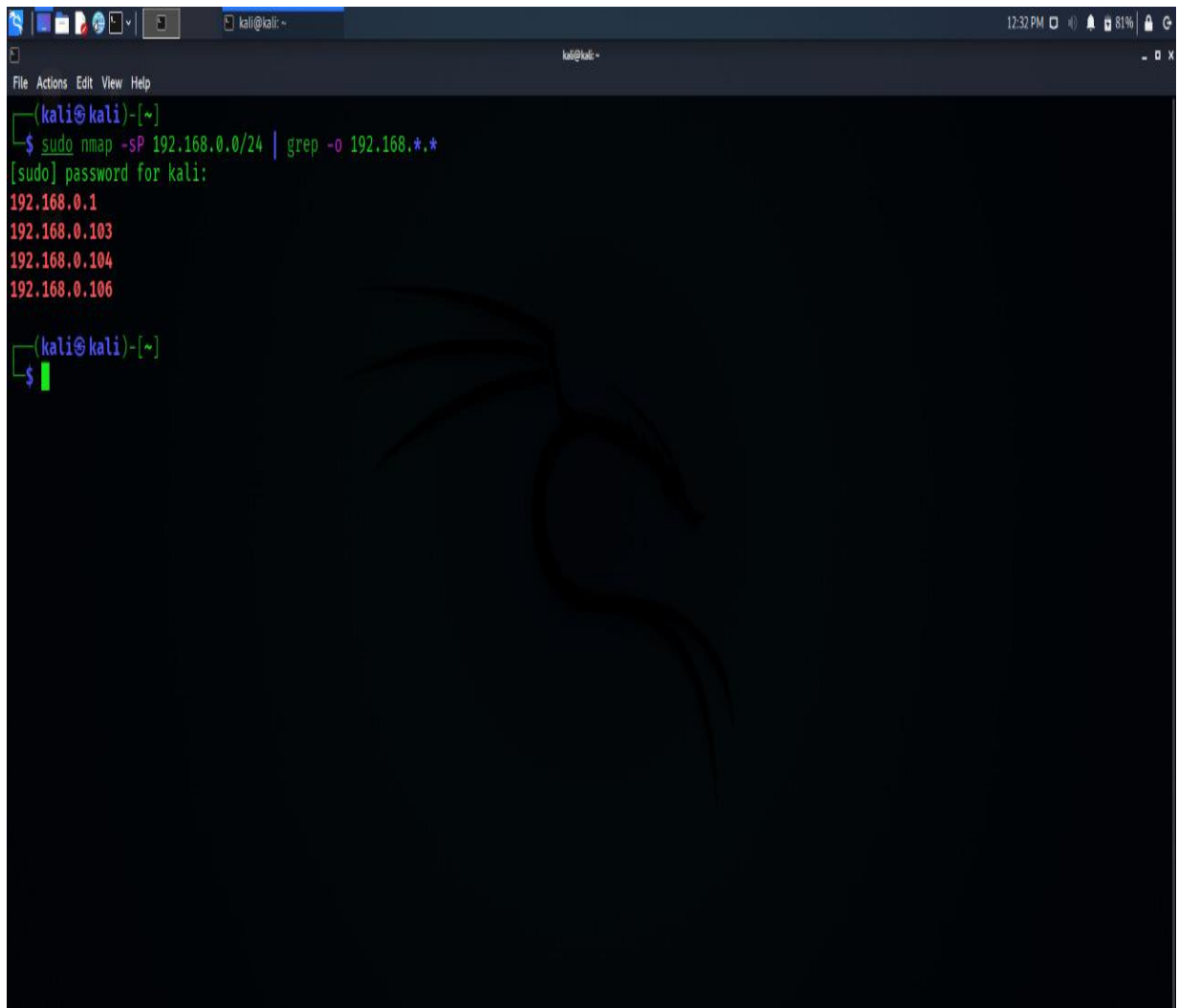
- Red Team Field Manual (BOOK)
- Black Hat Python second edition (BOOK)
- Github.com
- Google.com

5 APPENDIXES

5.1 SOURCE CODE

There is no source code. Since it is a procedure-based project. It is a part of Cyber Security.

5.2 SCREENSHOTS OF OUTPUT



```
(kali@kali)-[~]  
$ sudo nmap -sP 192.168.0.0/24 | grep -o 192.168.*.*  
[sudo] password for kali:  
192.168.0.1  
192.168.0.103  
192.168.0.104  
192.168.0.106  
  
(kali@kali)-[~]  
$
```

The screenshot shows a terminal window on a Kali Linux system. The user has executed the command `sudo nmap -sP 192.168.0.0/24 | grep -o 192.168.*.*`. The terminal output shows the command being executed, the password prompt, and the resulting IP addresses: `192.168.0.1`, `192.168.0.103`, `192.168.0.104`, and `192.168.0.106`. The terminal window has a dark background with a faint Kali Linux logo watermark.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sP 192.168.0.0/24 | grep -o 192.168.*.*  
[sudo] password for kali:  
192.168.0.1  
192.168.0.103  
192.168.0.104  
192.168.0.106  
(kali@kali)-[~]  
$ sudo nmap -sV -Pn --min-rate 300 192.168.0.104  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 12:37 EDT  
Nmap scan report for 192.168.0.104  
Host is up (0.00018s latency).  
Not shown: 978 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rshd  
513/tcp   open  login  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)
```

```
kali@kali: ~  
File Actions Edit View Help  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8180/tcp  open  unknown  
MAC Address: 08:00:27:AB:C5:CA (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 190.88 seconds  
  
(kali@kali)-[~]  
$
```