Module-3 Assignment: Detailed Scan Report

Nawaraj Khatiwada

ECE-529 Intro to Technical Cybersecurity

Prof. Dr. Lamb

Spring 2024

Introduction

In cybersecurity, reconnaissance entails learning as much as possible about a target system or network to spot potential weak points and entry points. In this stage, passive methods like open-source intelligence gathering are frequently combined with active like port scanning and network identifier. Following reconnaissance, vulnerability identification entails actively searching systems for flaws that might be used against them, such as out-of-date software, incorrect setups, or unsafe network protocols. Nmap is a powerful open-source tool used by cybersecurity experts for reconnaissance and vulnerability identification. Network scans can be started in Linux with the 'nmap' command, which lets users search for open ports, services that are using those ports, and even specific vulnerabilities on target systems.

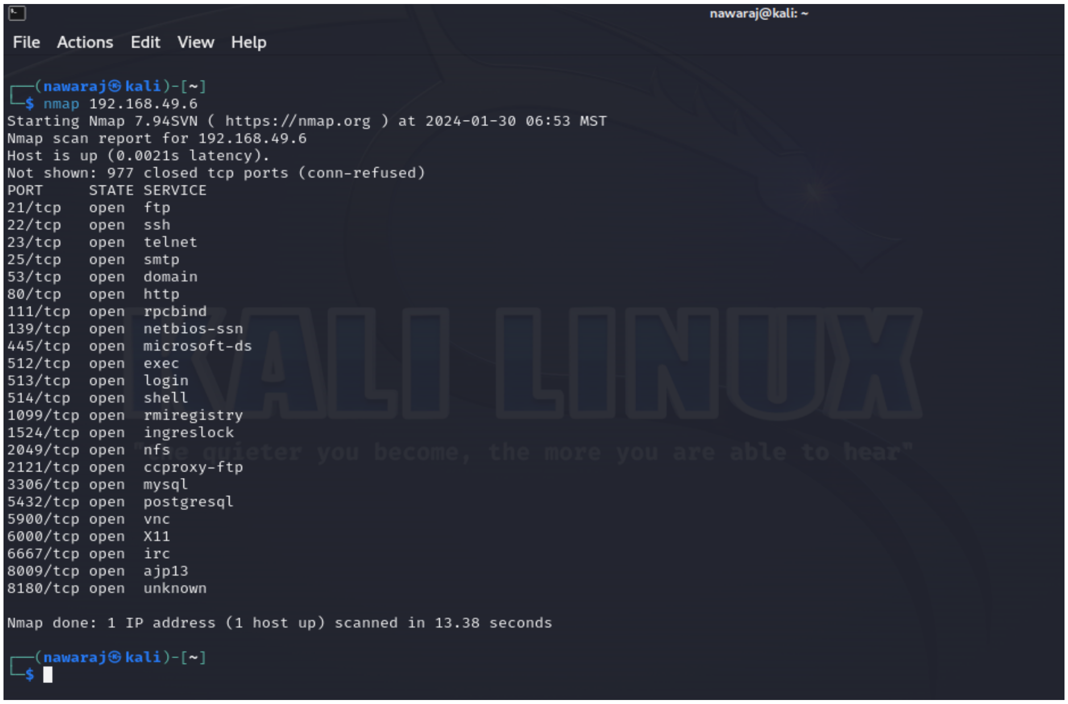
Objectives

This paper aims to present a detailed scan analysis of the Metasploitable system in a Linux environment using the Nmap tool. The primary goal is to conduct a comprehensive investigation and generate a final report with findings that will help to achieve the research goals. The knowledge gathered from this analysis will help manage future techniques designed to improve system security and reduce vulnerabilities in similar configurations.

Methodology

This project's method includes many different steps. First, we make use of a virtual machine (VM) environment, in which we set up two host VMs, Kali Linux and Ubuntu, and one target VM running Metasploitable, a program known for its exploitable vulnerabilities. Making sure that Kali Linux, Ubuntu, and Metasploitable virtual machines (VMs) are all up and running on the same network is essential. We set up the VMware network settings by enabling DHCP, disabling NAT, and establishing a private network to make this easier. It's important to verify connectivity, which is done by making sure we can ping the host virtual machine. Below is a detailed process outline.

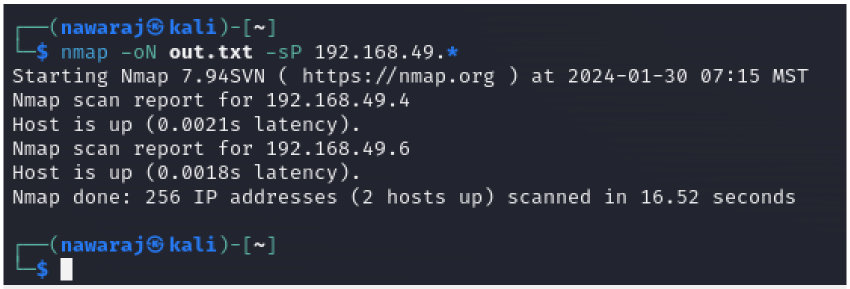
NMAP Scan: After ensuring the connectivity we are now going to scan the Metasploitable VM using NMAP scan. In the first step, we need to Identify Metasploitable IP for this we use the command *ifconfig* on the Metasploitable terminal. We found the IP of metasploitable VM as 192.168.49.*. Now we are going to use nmap from the kali linux VM to the metasploitable VM. At first, we use simple command nmap <IP_metasploitable>, This command will perform a basic scan on the Metasploitable VM, showing open ports and services.



```
┌──(nawaraj㉿kali)-[~]
└─$ nmap 192.168.49.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 06:53 MST
Nmap scan report for 192.168.49.6
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds

┌──(nawaraj㉿kali)-[~]
└─$ 
```

Screenshot from Kali Linux for nmap scan

- *nmap -oN out.txt -sP <IP>*: This command executes a ping scan using Nmap on the host with the IP address 192.168.49.*, determining if it's online without scanning any ports, and saves the results to a file named "out.txt". The "-sP" option specifically instructs Nmap to perform a ping scan, while "-oN out.txt" directs Nmap to save the output to the specified file.

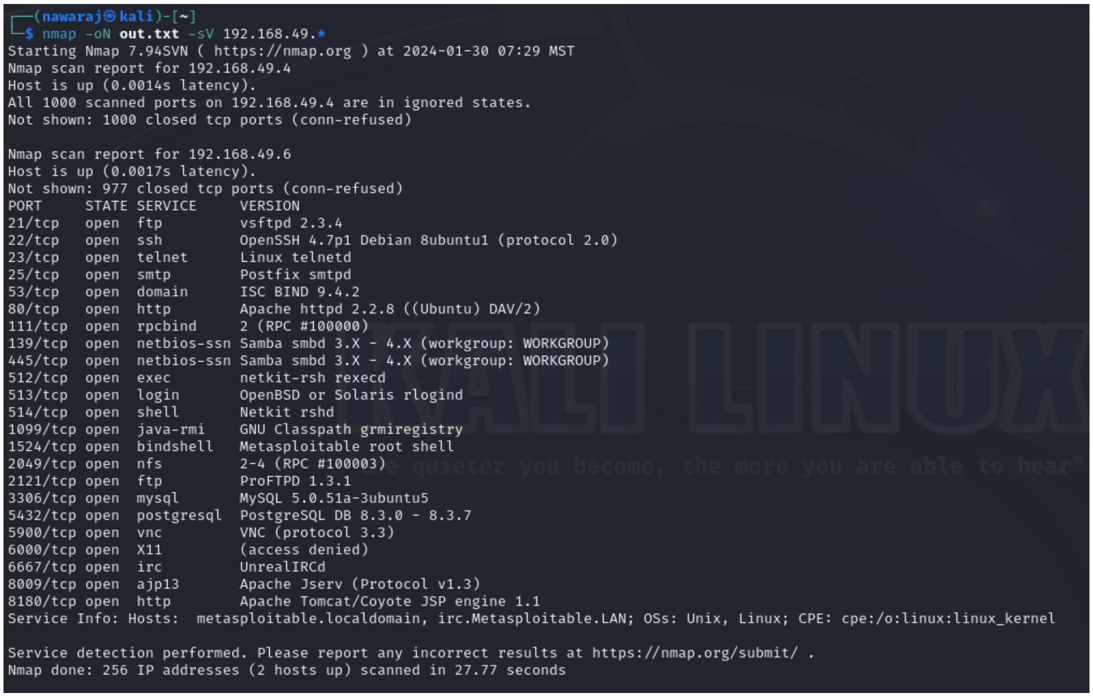


```
┌──(nawaraj㉿kali)-[~]
└─$ nmap -oN out.txt -sP 192.168.49.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 07:15 MST
Nmap scan report for 192.168.49.4
Host is up (0.0021s latency).
Nmap scan report for 192.168.49.6
Host is up (0.0018s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.52 seconds

┌──(nawaraj㉿kali)-[~]
└─$ 
```

Fig2: Screenshot of nmap scan

From the above result we found 2 hosts

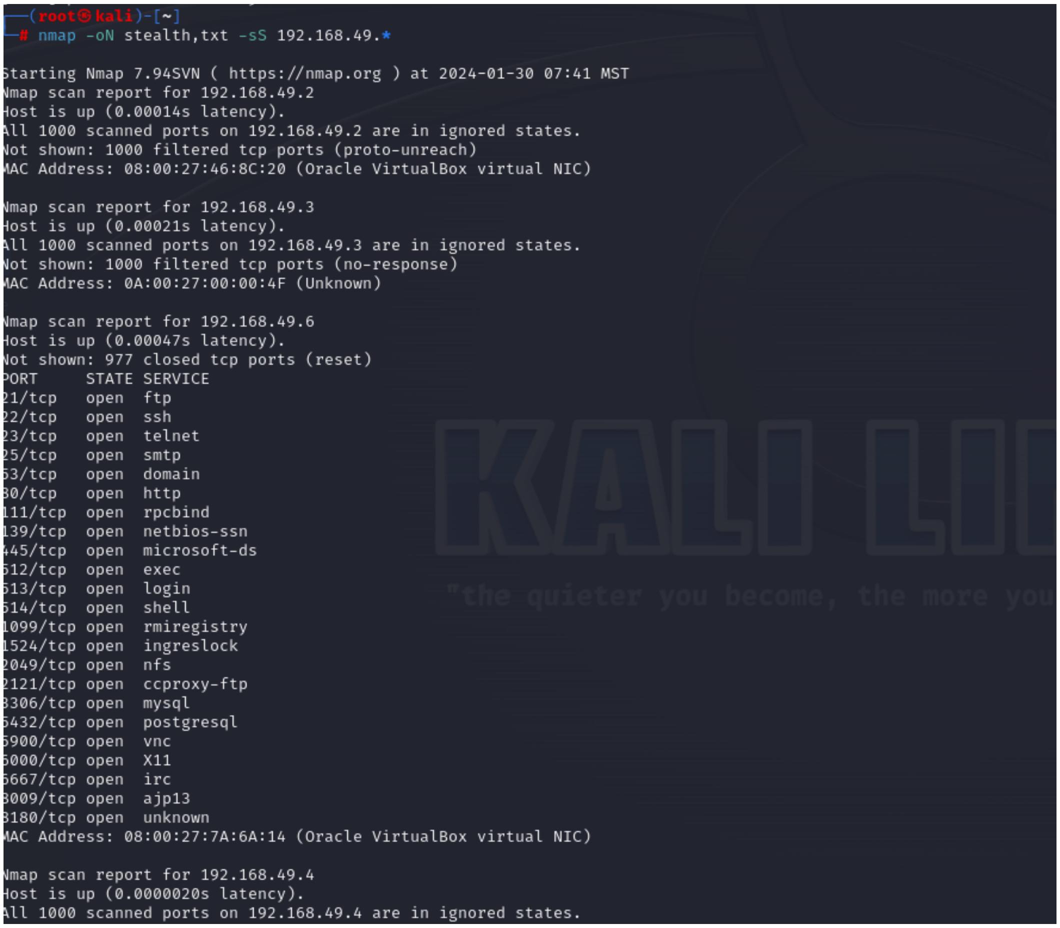
- *nmap -oN out.txt -sV <IP>*: The -sV option in Nmap performs version detection during a scan. When used, Nmap tries to determine the versions of the services running on open ports.



```
┌──(nawaraj㉿kali)-[~]
└─$ nmap -oN out.txt -sV 192.168.49.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 07:29 MST
Nmap scan report for 192.168.49.4
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.49.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.49.6
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  shell       Netkit rshd
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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: 256 IP addresses (2 hosts up) scanned in 27.77 seconds
```

Fig 3: Screenshot for -sV

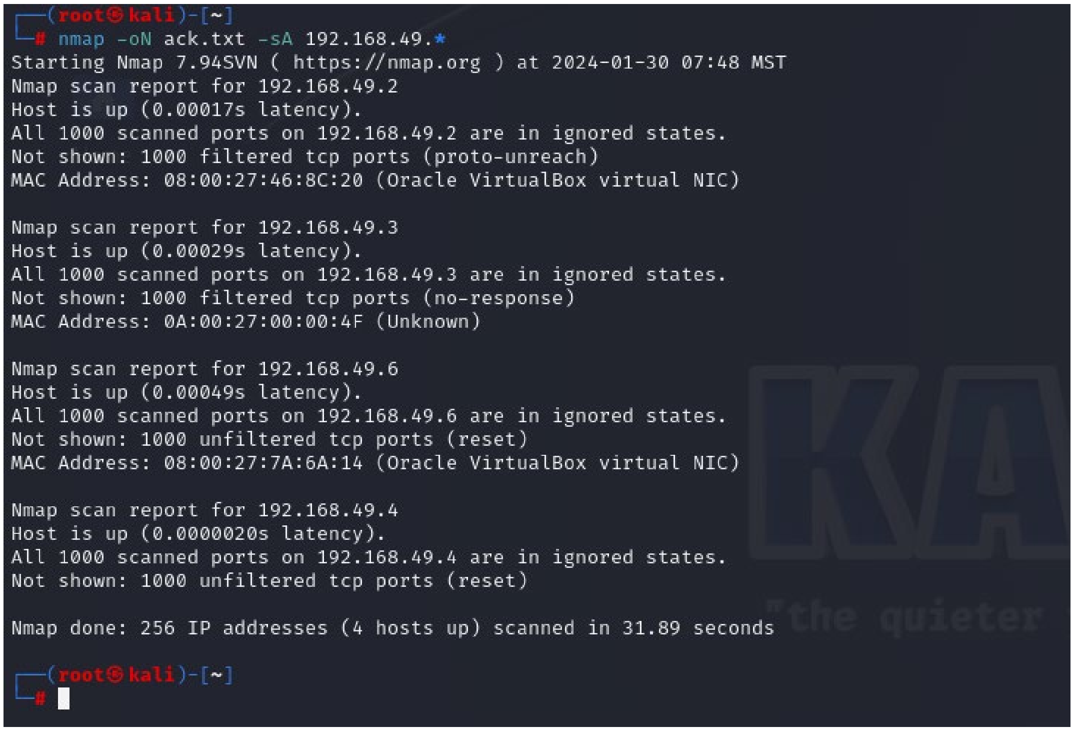
- *nmap -oN stealth.txt -sS <IP>*: This option specifies a TCP SYN scan, also known as a "stealth scan". It sends SYN packets to the target ports to determine which ports are open without completing the full TCP handshake, making it less likely to be detected by intrusion detection systems.



```
┌──(root㉿kali)-[~]
└─# nmap -oN stealth,txt -sS 192.168.49.*

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 07:41 MST
Nmap scan report for 192.168.49.2
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.49.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:46:8C:20 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.3
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.49.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:4F (Unknown)

Nmap scan report for 192.168.49.6
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7A:6A:14 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.4
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.49.4 are in ignored states.
```

Fig 4: Screenshot for -sS

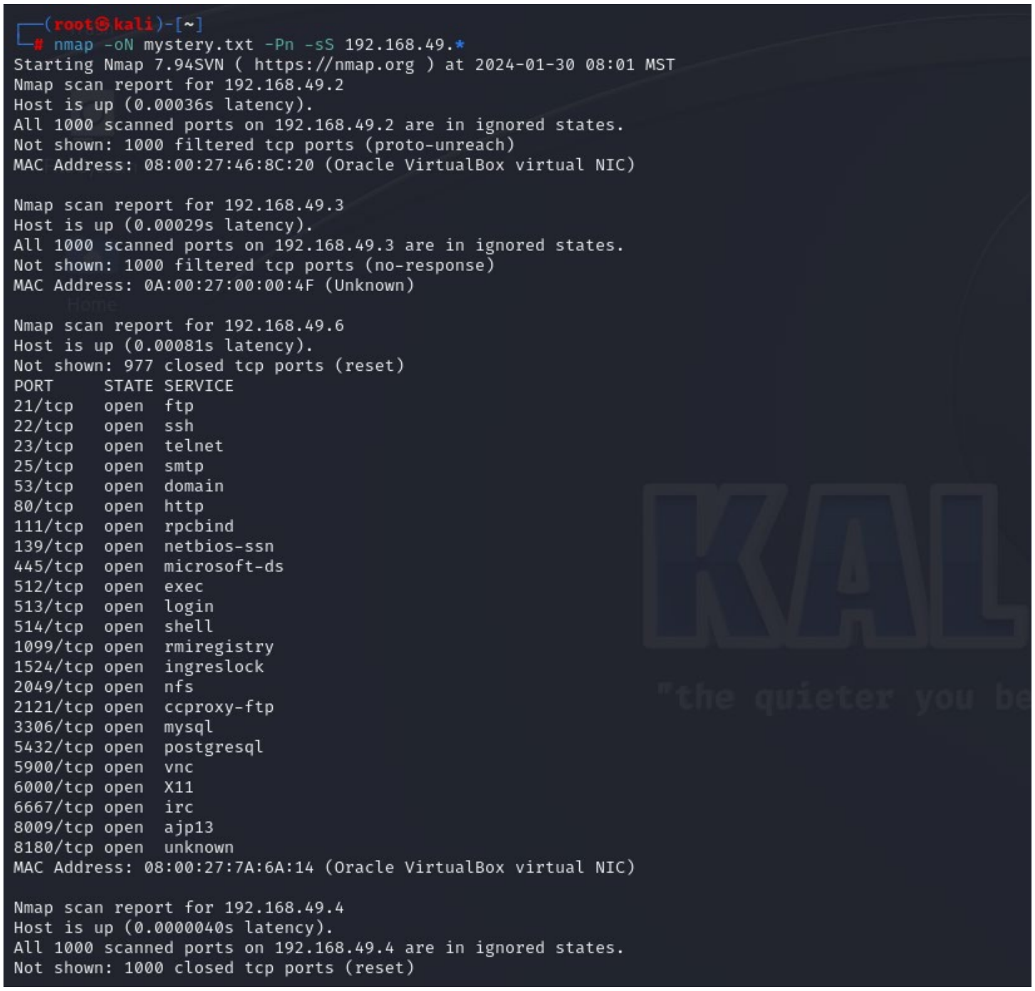
- *nmap -oN ack.txt -sA <IP>*: This option specifies an ACK scan. An ACK scan is used to determine how a target host responds to TCP packets with the ACK (acknowledgment) flag set. It's often used to infer firewall rules and identify filtered ports.



```
┌──(root㉿kali)-[~]
└─# nmap -oN ack.txt -sA 192.168.49.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 07:48 MST
Nmap scan report for 192.168.49.2
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.49.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:46:8C:20 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.3
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.49.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:4F (Unknown)

Nmap scan report for 192.168.49.6
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.49.6 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:7A:6A:14 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.4
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.49.4 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 31.89 seconds

┌──(root㉿kali)-[~]
└─# 
```

Fig 5: Screenshot for -sA

- *nmap -oN mystery.txt -Pn -sS <IP>*: This command performs a stealth TCP SYN scan on all hosts within the 192.168.49.0/24 subnet, skipping host discovery, and saves the results to a file named "mystery.txt".



```
┌──(root㉿kali)-[~]
└─# nmap -oN mystery.txt -Pn -sS 192.168.49.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 08:01 MST
Nmap scan report for 192.168.49.2
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.49.2 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:46:8C:20 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.3
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.49.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:4F (Unknown)

Nmap scan report for 192.168.49.6
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7A:6A:14 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.49.4
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.49.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Fig 5: Screenshor for -Pn -sS scan

- *nmap -sC scanme.nmap.org*: This command performs a scan on the target domain "scanme.nmap.org" using default scripts to gather information about open ports, services, and potential vulnerabilities. It's a common example used for testing and learning Nmap functionalities.
- *Other scan option*: There are other scanning option for nmaps, some of them are as follows:
  - -Pn or PO: used to trun off host discovery
  - -PB, -PE, -PP, -PM, -PR: Various ping types for host discovery
  - -F: Used for fast scan
  - --top-ports[N]: Specifies the number of top ports to scan

- -T, -U: Specifies TCP or UDP protocol for scanning
- -sF, sN, -sX, -sM: Scans with specific TCP control bits set on packets

Findings

Two hosts are identified as active by their respective IP addresses, 192.168.49.4 and 192.168.49.6, with latency times of 0.0021s and 0.018s, respectively, upon running the command *nmap -oN out.txt -sP 192.168.49.**. The search covered 256 IP addresses and took about 16.52 seconds to complete. Additionally, using the -*sP* command showed several ports in addition to their operational states (open/closed) and the services that corresponded to them, such as http, ssh, telnet, smtp, domain, and ssh. Significantly, open ports like FTP (port 21), SSH (port 22), Telnet (port 23), SMTP (port 25), and HTTP (port 80) were found to have potential vulnerabilities.

Four active hosts were found by further scanning with the -*sA* option. These hosts were identified by their IP addresses (192.168.49.2,.3,.6,.4), along with their MAC addresses and other relevant data. Four active hosts were discovered in 31.89 seconds after 256 IP.

An additional scan using -*Pn -sS* revealed several hosts in the 192.168.49.* subnet, all of which had different answers. Host 192.168.49.3 showed most ports as closed, suggesting a potentially strict security posture, while hosts 192.168.49.2 and 192.168.49.4 remained unresponsive, possibly because of strict firewall configurations or inactive services. To evaluate related vulnerabilities, it is advisable to investigate services on this host. On the other hand, host 192.168.49.6 had many open ports, indicating a larger attack surface and increased risk. Identifying potential security risks involves examining service versions and comparing them with databases of known vulnerabilities. Moreover, understanding common exploits that target services such as FTP, SSH, and HTTP can help reveal vulnerabilities that threat actors may exploit.

Discussion and Conclusion

The paper discusses the hypothetical goal of analysis facilitated by the Nmap scan tool within a Linux environment. The security environment of the Metasploitable system has been significantly clarified by this study. Following a methodical approach, we were able to locate important weaknesses and possible points of exploitation in the target environment. The significance of proactive vulnerability management is emphasis by the results of the network scans, which highlight open ports, active hosts, and related services. The correlation found between service versions and known vulnerabilities highlights the significance of staying current with security developments and acting quickly to implement countermeasures. We learned from this study that proactive patch management, frequent vulnerability assessments, and the implementation of strong security procedures should be given top priority by organizations. This plan is essential to maintaining their defenses against fresh attacks and ensuring the safety and integrity of their networks. The knowledge we gain from studying this improves our ability to protect ourselves online and effectively handle threats.