🎓 Task 2 Report – Network Security & Scanning

Submitted By : Pritish Borkar
Internship ID : APSPL2518121
Department : Cybersecurity
Organization : ApexPlanet software Pvt.Ltd
Co-ordinator : Kundan Kumar
Date of Submission : October 17, 2025

1. Objective:

The objective of Task 2 was to understand and perform **network reconnaissance, scanning, vulnerability assessment, and basic firewall configuration** in a controlled cybersecurity lab environment.
The task focused on identifying open ports, running services, and vulnerabilities within the target machine (Metasploitable2) using Kali Linux tools and techniques.

2. Network Configuration

Component	Details
Attacker Machine:	Kali Linux
Target Machine:	Metasploitable2
Kali IP Address:	192.168.56.101
Target IP Address:	192.168.56.102
Network Type:	Host-Only Adapter (192.168.56.0/24)

3. Step 1 – Reconnaissance

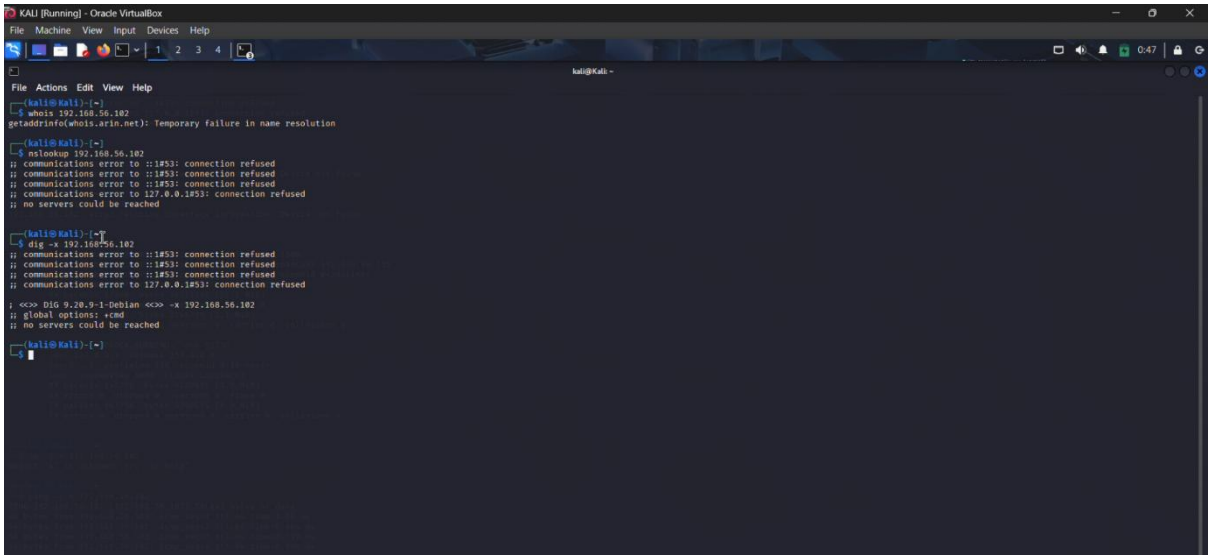
A. Passive Reconnaissance

Commands used:

- whois 192.168.56.102
- nslookup 192.168.56.102
- dig -x 192.168.56.102

- Whois and DNS lookups failed as expected since the IP address belongs to a **private local network**.

- Findings documented to explain private IP behavior.

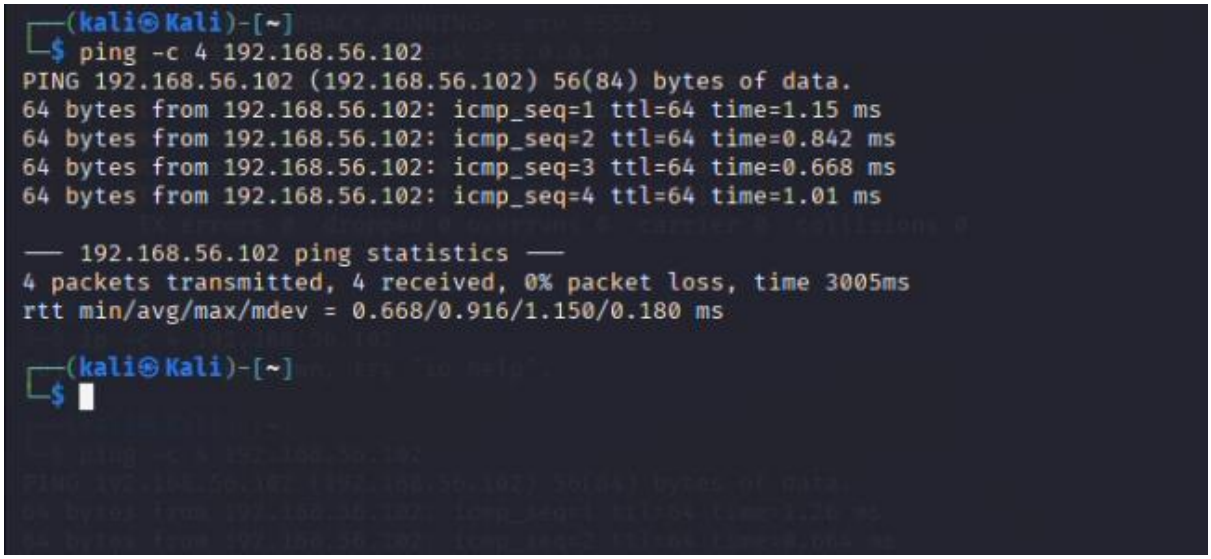


B. Active Reconnaissance

1. Ping Sweep

- ping -c 4 192.168.56.102
- sudo nmap -sn 192.168.56.0/24

Result: Metasploitable2 was reachable, confirming connectivity.



```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:48 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00052s latency).
MAC Address: 0A:00:27:00:00:0B (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
MAC Address: 08:00:27:64:B1:2B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00056s latency).
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.82 seconds

┌──(kali㉿Kali)-[~]
└─$
```

2. Banner Grabbing (Manual)

- nc -v 192.168.56.102 21 # FTP
- nc -v 192.168.56.102 22 # SSH
- nc -v 192.168.56.102 23 # Telnet
- curl -I http://192.168.56.102

Port	Service	Banner	Finding
21	FTP	vsFTPd 2.3.4	Vulnerable backdoor (CVE-2011-2523)
22	SSH	OpenSSH 4.7p1 Debian-8ubuntu1	Outdated version
23	Telnet	Plain-text connection	Insecure protocol
80	HTTP	Apache 2.2.8 (Ubuntu)	Vulnerable web server

```
┌──(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 21
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 21 (ftp) open
220 (vsFTPd 2.3.4)
^C
```

```
┌──(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 21
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 21 (ftp) open
220 (vsFTPd 2.3.4)
^C
```

```
┌──(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 22
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
```

```
┌──(kali㉿Kali)-[~]
└─$ nc -v 192.168.56.102 23
192.168.56.102: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.56.102] 23 (telnet) open
```

```
┌──(kali㉿Kali)-[~]
└─$ curl -I http://192.168.56.102
HTTP/1.1 200 OK
Date: Tue, 16 Sep 2025 20:56:51 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

```
25/tcp   open  smtp        Postfix smtpd
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39433/tcp   mountd
|   100005  1,2,3      44155/udp   mountd
|   100021  1,3,4      49082/udp   nlockmgr
|   100021  1,3,4      55930/tcp   nlockmgr
|   100024  1          37376/tcp   status
|_  100024  1          59663/udp   status
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
|_banner: \x01Where are you?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
|_banner: \x01getnameinfo: Temporary failure in name resolution
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
|_banner: root@metasploitable:/#
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.102]
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x0A\x00\x00\x00b)D[{ztU\x
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\ ...
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
|_banner: RFB 003.003
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna
|_me ... \x0D\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol ...
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/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 27.01 seconds
```

4. Step 2 – Port & Service Scanning

1. Basic TCP SYN Scan

- sudo nmap -sS 192.168.56.102

Result: Multiple ports found open including FTP, SSH, Telnet, HTTP, SMB, and MySQL.

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sS 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:52 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00032s 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:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

2. Service Version & OS Detection

- nmap -sV 192.168.56.102
- sudo nmap -O 192.168.56.102

Result: Target OS detected as **Linux 2.6.X (Ubuntu-based)**.

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:55 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/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 11.61 seconds
```

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 00:56 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00097s 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:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

3. Comprehensive All-Port Scan

- sudo nmap -sS -sV -O -A -p- -oN nmap_full_report.txt 192.168.56.102

Result: Saved full scan report for documentation.

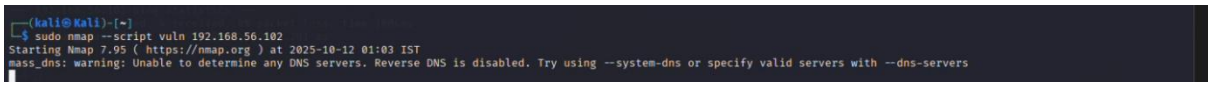
```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sS -sV -O -A -p- -oA nmap_complete_scan 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 01:00 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
```

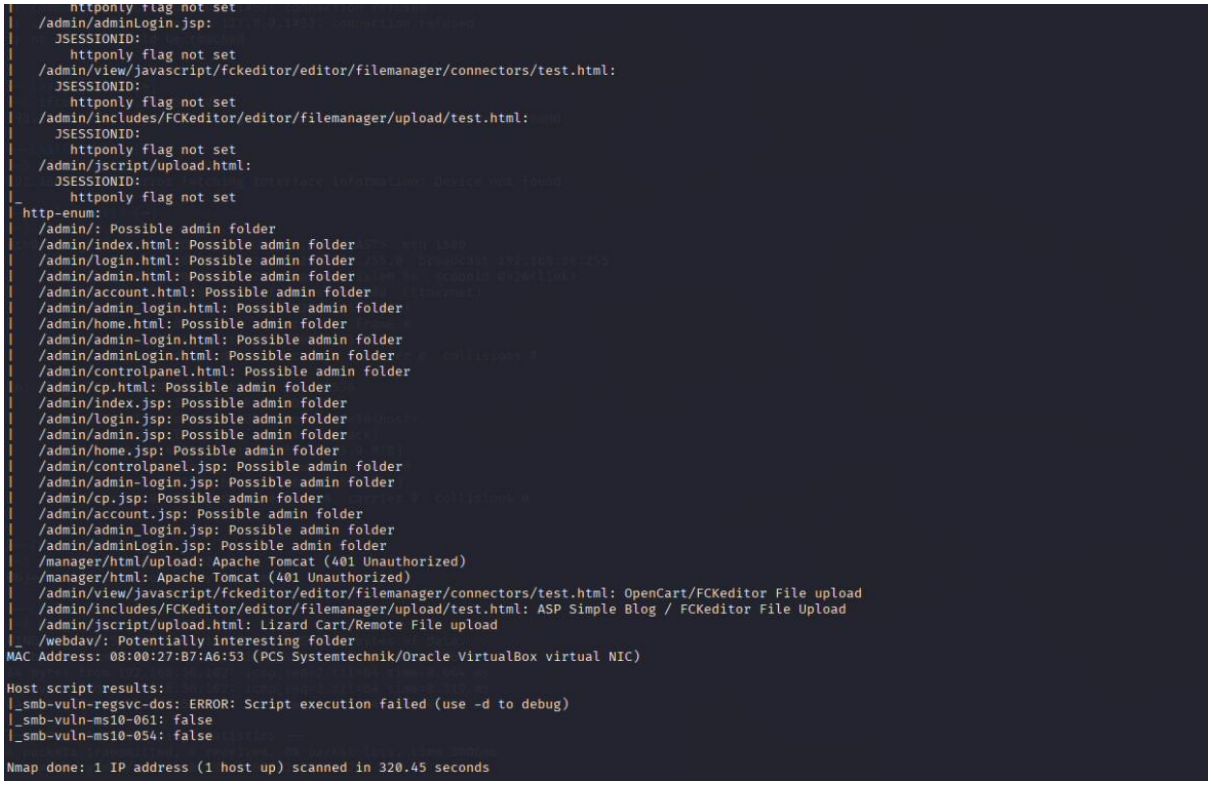
```
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37376/tcp open  status      1 (RPC #100024)
39433/tcp open  mountd      1-3 (RPC #100005)
44429/tcp open  java-rmi    GNU Classpath grmiregistry
55930/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:B7:A6:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -24d21h24m25s, deviation: 2h00m00s, median: -24d22h24m25s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-16T17:08:07-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.35 seconds
```

4. Vulnerability Script Scan

- sudo nmap --script vuln 192.168.56.102

Used Nmap NSE scripts to detect vulnerabilities directly.





5. Step 3 – Vulnerability Scanning

Tool Used: Nmap NSE (Nmap Scripting Engine)

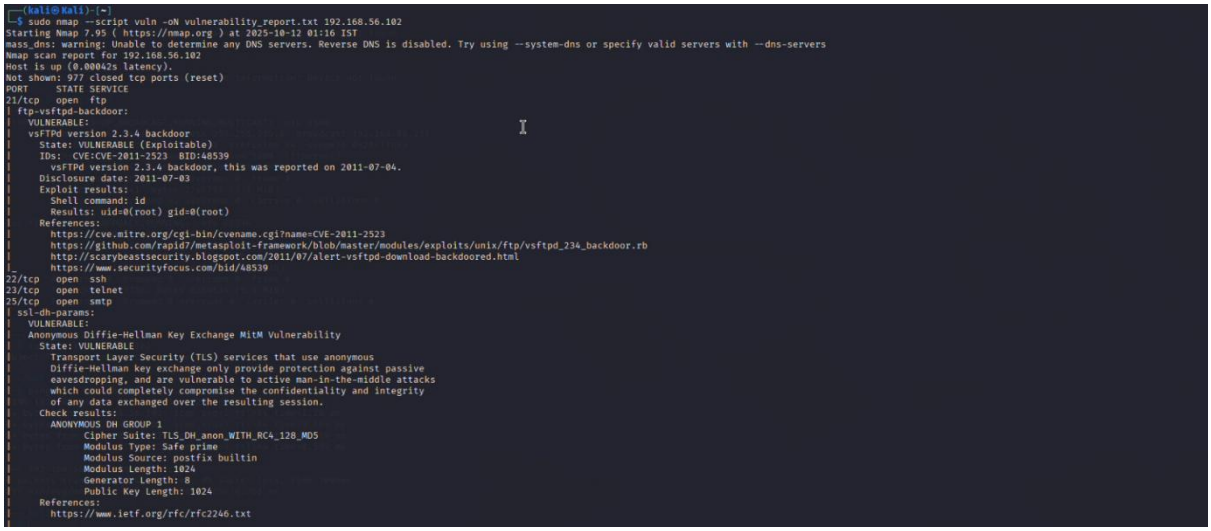
Due to limited internet access on Host-Only networks, **Nmap NSE scripts** were used instead of OpenVAS/Nessus.

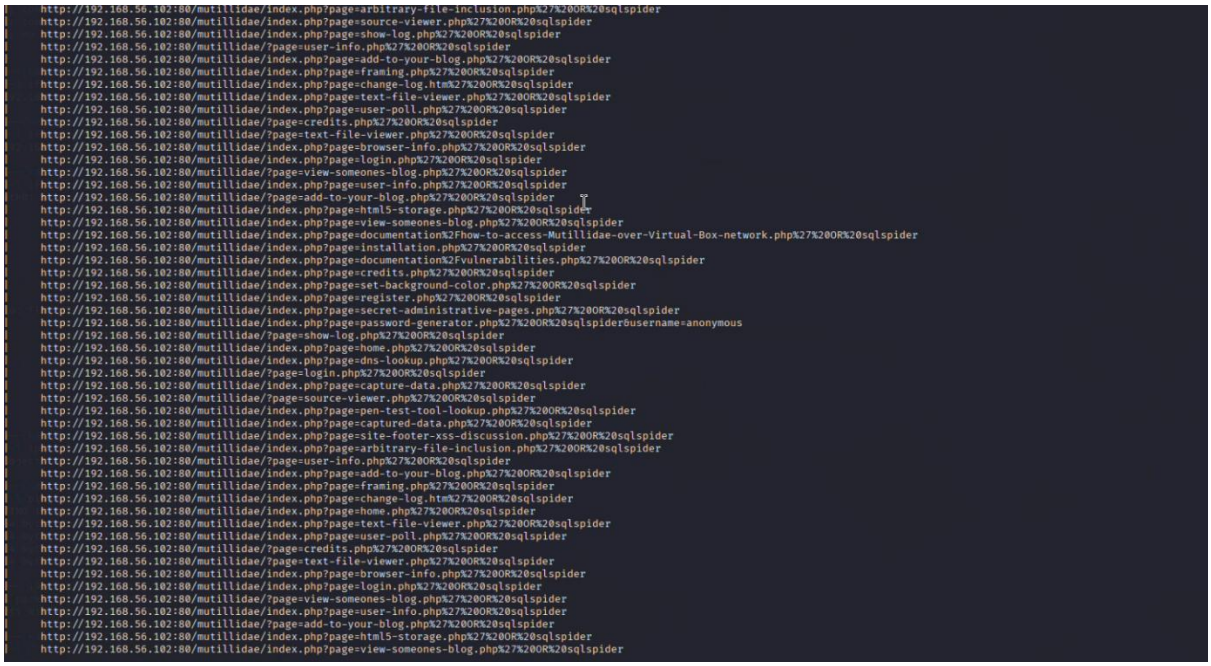
Command Used:

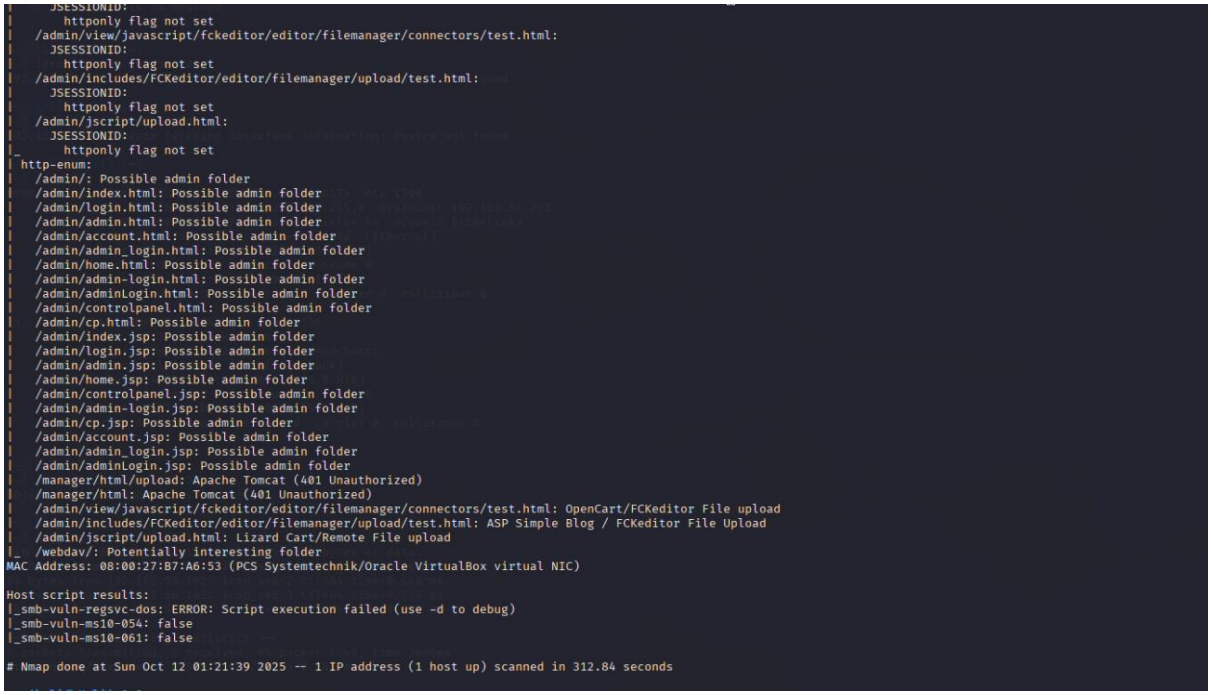
- sudo nmap --script vuln,exploit -sV -oN vulnerability_report.txt 192.168.56.102

Vulnerabilities Detected:

1. vsFTPd 2.3.4 Backdoor (CVE-2011-2523) – Critical
2. Samba SMB Remote Code Execution – High
3. Distcc Remote Command Execution – High
4. UnrealIRCD Backdoor Trojan – Critical
5. MySQL Weak Credentials – Medium







Recommendations:

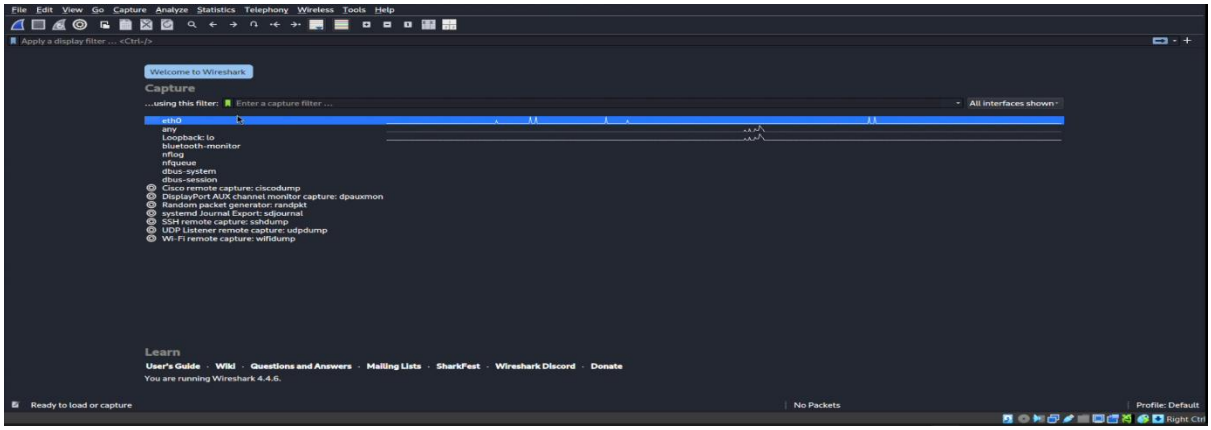
- Update or remove vulnerable services.
- Disable Telnet and FTP; use secure protocols (SSH/SFTP).
- Regularly patch operating systems and applications.

6. Step 4 – Packet Analysis with Wireshark

A. FTP Credential Capture

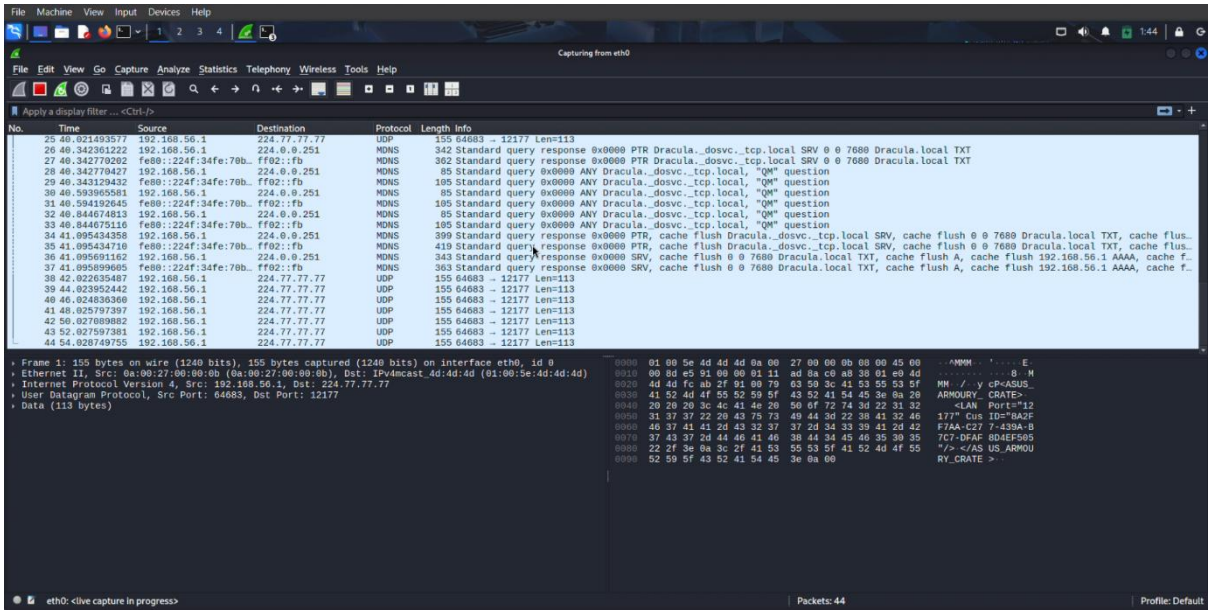
- Captured plain-text credentials:
  - Username: msfadmin
  - Password: msfadmin
- Verified using Wireshark filters:

➢ ftp.request.command == "USER" or ftp.request.command == "PASS"



B. SYN Flood Simulation

Used hping3 to simulate a flood:



Observed a large number of SYN packets without corresponding ACK responses.

Findings:

- Demonstrated DoS vulnerability.
- Highlighted need for rate limiting and firewall rules.

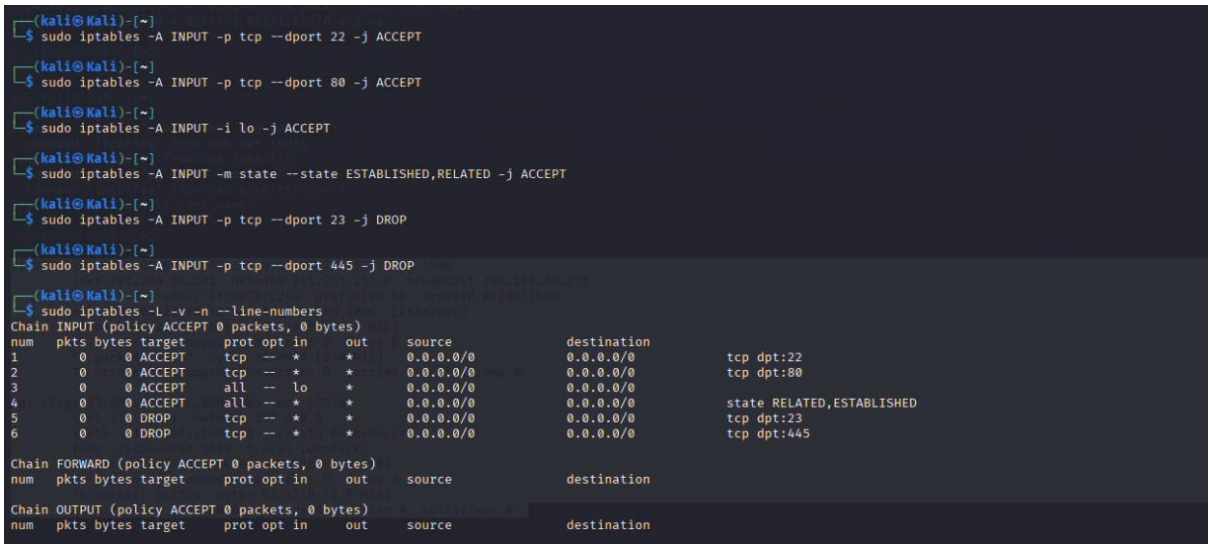
7. Step 5 – Firewall Configuration (iptables)

A. Allow Rules

- sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- sudo iptables -A INPUT -i lo -j ACCEPT
- sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

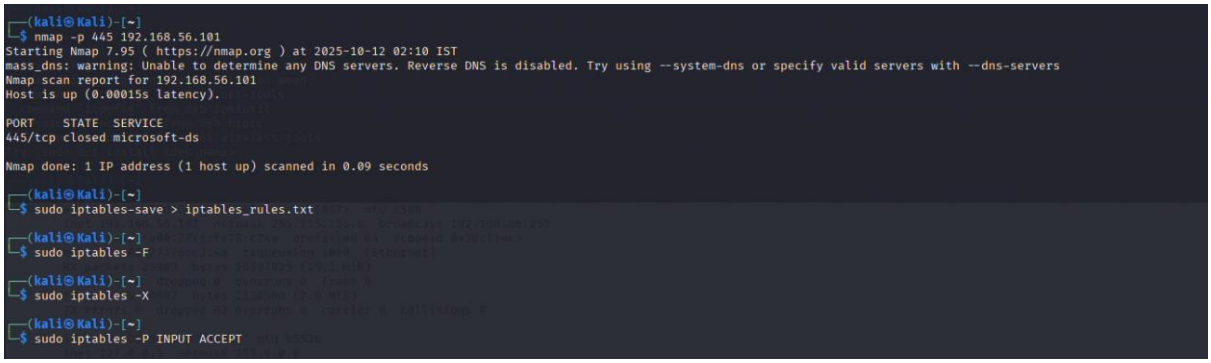
B. Deny Rules

- sudo iptables -A INPUT -p tcp --dport 23 -j DROP
- sudo iptables -A INPUT -p tcp --dport 445 -j DROP



Verification:

- nmap -p 445 192.168.56.101



Result: Port 445 showed as *filtered*, confirming rule effectiveness

10. Key Learnings

1. Learned how to perform **reconnaissance and enumeration** effectively.
2. Understood the role of **Nmap** in scanning and vulnerability detection.
3. Captured and analyzed **unencrypted credentials** with Wireshark.
4. Simulated **DoS attacks** and monitored packet patterns.
5. Implemented **firewall rules** to mitigate attacks and port scans.
6. Gained insight into **network security posture assessment**.

11. Conclusion

This task provided comprehensive hands-on experience in **network security assessment**. Through reconnaissance, scanning, vulnerability analysis, and defensive configurations, I learned how attackers identify weaknesses and how defenders can secure systems.

The exercise enhanced my technical, analytical, and documentation skills in cybersecurity.