Task - 1 Report

Task overview:

In this task we are going to perform nmap port scan on the vulnerable machine and analyze the network traffic through the wireshark and next going through the open ports and services and its versions and their risks

Common services found:

FTP (File Transfer Protocol), 21:

The victim machine using the FTP version of **vsftpd 2.3.4** which is much lower than the present version **vsftpd 3.0.5.** This version of FTP is vulnerable to the backdoor of the system

And this leads to unauthenticated privilege access to the unknown uses , and the machine is enabled with anonymous login , which is a default misconfiguration.

SSH (secure shell), 22:

The victim machine using the SSH version of OpenSSH 4.7p1 which is much older which is released in 2007, it lacks modern cryptographic techniques to encrypt and decrypt and allowed to brute force, so there is no rate limiting

In some cases it can release the host keys and server software information , and algorithm using . So it posses the major threat to the server

SMTP ,25:

The open port 25/tcp running Postfix SMTP server on your target indicates an email service is exposed. This can introduce multiple security risks, like some vulnerable commands are enabled it leads to user enumeration and Relay abuse means that allow unauthenticated external users to send emails to other domains

Netbios-ssh (139,445) :

The services running on TCP ports 139 and 445 are Samba (SMB) — a protocol used for file and printer sharing over a network. The versions you have detected are known to be highly vulnerable

1. Remote Code Execution: Samba 3.0.20 allows attackers to run arbitrary commands as root
2. Anonymous Access: Guest login can expose sensitive shared files without authentication
3. SMB Relay Attacks: Without SMB signing, attackers can intercept and relay credentials

Mysql (3306):

The services running on TCP port 3306 are MySQL a service used for running database server. The versions you have detected are known to be highly vulnerable.

1. The services running on TCP ports 139 and 445 are Samba (SMB) — a protocol used for file and printer sharing over a network. The versions you have detected are known to be highly vulnerable
2. Remote Access: If exposed to the network without proper firewall or bind-address restriction, attackers can attempt brute-force or dictionary attacks

Bindshell , 1524:

A bind shell is a shell that listens on a specific port on the victim machine. An attacker can then connect to that port remotely to gain control.

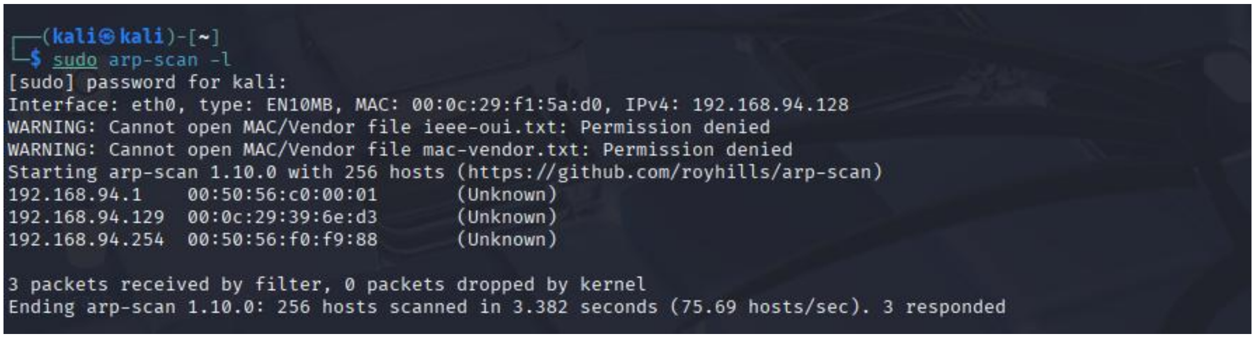
Now, in the victim machine there is a Bindshell is present that means we already have the port number and ip address in this case we can get root access

1. Unauthenticated Remote Root Access: Anyone can connect and get a root shell without credentials.
2. No Logging or Monitoring: Bind shells often bypass system logging, making detection difficult.
3. Persistence for Attackers: Can be used to maintain backdoor access to the system.
4. Full System Compromise: Root access allows modification, data theft, or lateral movement.

POC (proof of completion):

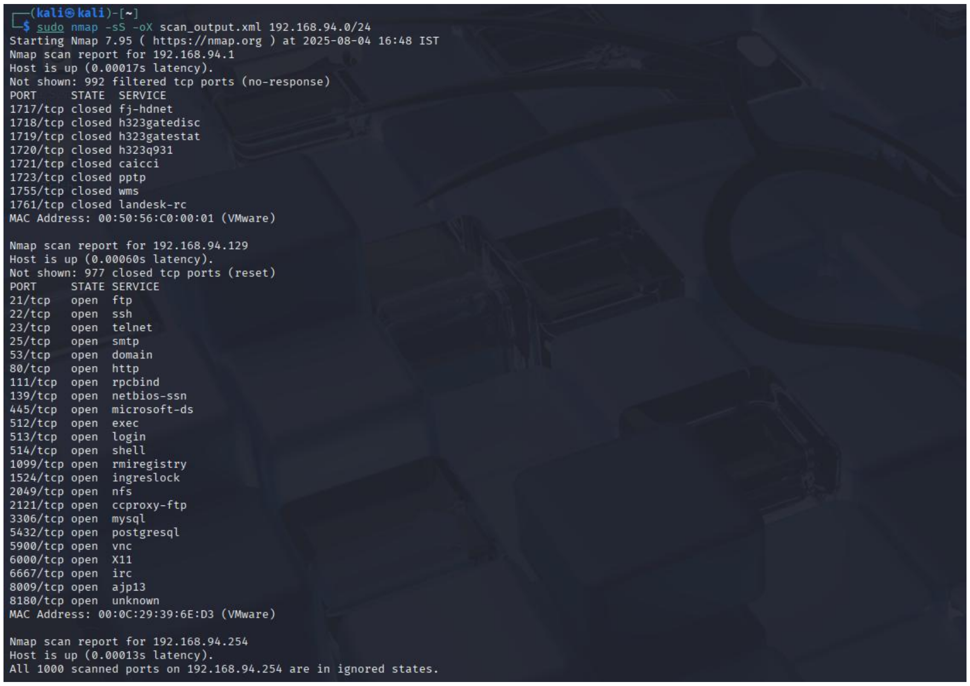
Command: arp-scan –l

This command help us to find the live hosts in our network, it works using the ARP(address resolution protocol) sends the ARP packets when we get the reply packets , then the host is said to be alive.



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:f1:5a:d0, IPv4: 192.168.94.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.94.1    00:50:56:c0:00:01       (Unknown)
192.168.94.129  00:0c:29:39:6e:d3       (Unknown)
192.168.94.254  00:50:56:f0:f9:88       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 3.382 seconds (75.69 hosts/sec). 3 responded
```

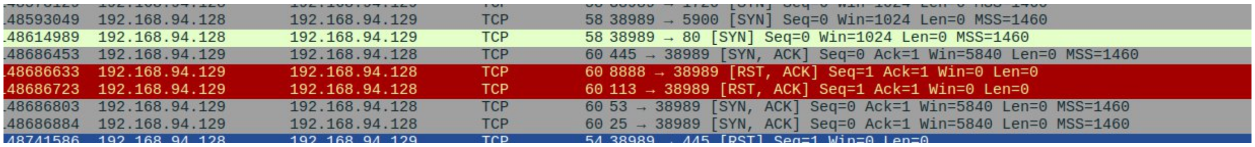


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -oX scan_output.xml 192.168.94.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 16:48 IST
Nmap scan report for 192.168.94.1
Host is up (0.00017s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE
1717/tcp closed fj-hdnet
1718/tcp closed h323gatedisc
1719/tcp closed h323gatestat
1720/tcp closed h323q931
1721/tcp closed caicci
1723/tcp closed pptp
1755/tcp closed wms
1761/tcp closed landesk-rc
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.94.129
Host is up (0.00060s 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: 00:0C:29:39:6E:D3 (VMware)

Nmap scan report for 192.168.94.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.94.254 are in ignored states.
```

Wireshark analysis:



```
.48593049  192.168.94.128  192.168.94.129  TCP  58 38989 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.48614989  192.168.94.128  192.168.94.129  TCP  58 38989 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.48686453  192.168.94.129  192.168.94.128  TCP  60 445 → 38989 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
.48686633  192.168.94.129  192.168.94.128  TCP  60 8888 → 38989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.48686723  192.168.94.129  192.168.94.128  TCP  60 113 → 38989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.48686803  192.168.94.129  192.168.94.128  TCP  60 53 → 38989 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
.48686884  192.168.94.129  192.168.94.128  TCP  60 25 → 38989 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
.48741586  192.168.94.128  192.168.94.129  TCP  54 38989 → 445 [RST] Seq=1 Win=0 Len=0
```

We are doing the TCP SYN scan , so we know that it is a half handshake , means the TCP connection won't be completed , the sender sends TCP SYN, and receiver sends SYN ACK, next thats it from there there is no connection of no packets are forworded, but the sender gets to know that the victim machine is up ,and open to connect on TCP.

Through out the TCP SYN scan , the same pattern will be followed for the every TCP protocol eg. Ssh, ftp, etc ..