Task 3: Network Scanning

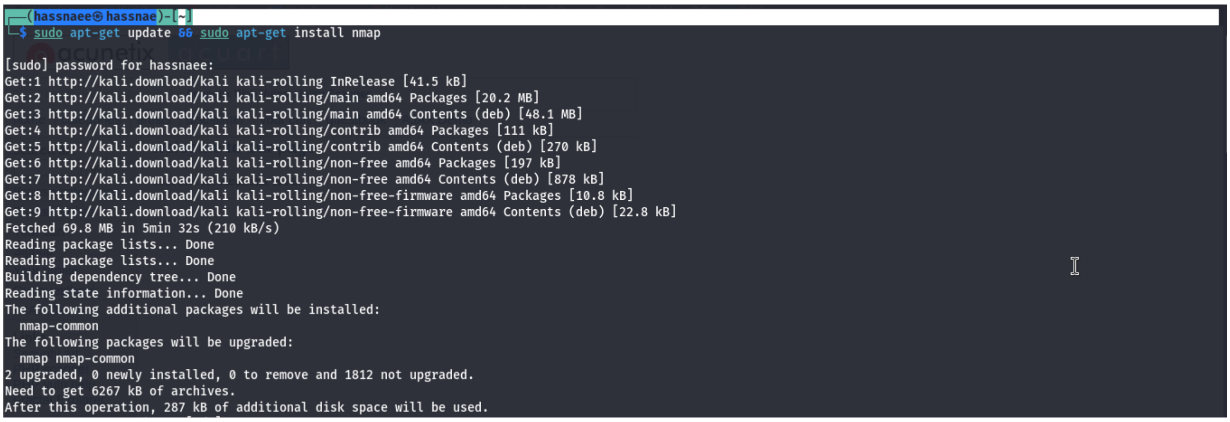
Introduction

This report outlines the process of using Nmap, a powerful network scanning tool, to discover devices and services on a local network. Network scanning and enumeration are essential skills for ethical hackers, helping identify potential targets and vulnerabilities. By the end of this project, we performed various scans to identify devices and gather information about their services and configurations.

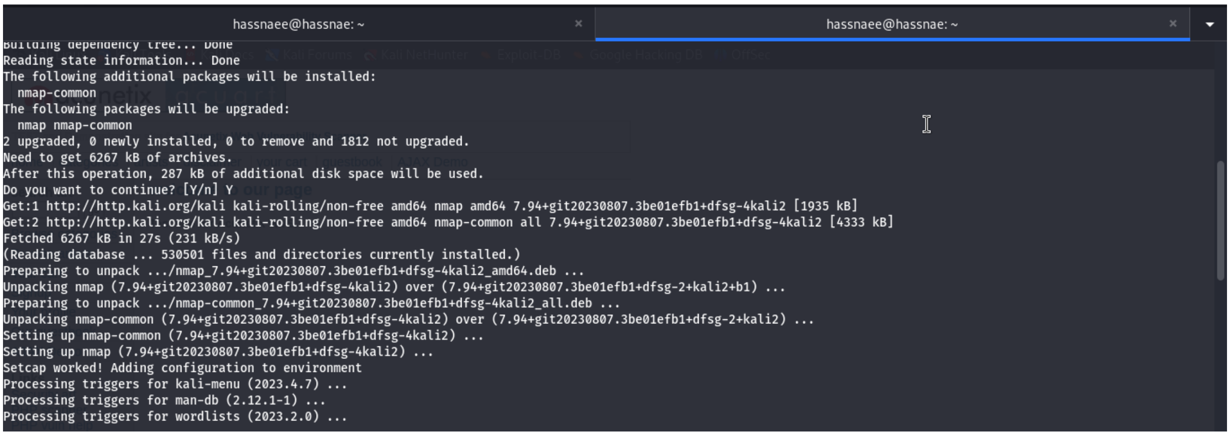
Installation

Nmap is pre-installed on Kali Linux. To verify the installation or update it, run the following command in the terminal:

```
sudo apt-get update && sudo apt-get install nmap
```



```
┌──(hassnaee㉿hassnae)-[~]
└─$ sudo apt-get update && sudo apt-get install nmap

[sudo] password for hassnaee:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.2 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [270 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [878 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]
Fetched 69.8 MB in 5min 32s (210 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nmap-common
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 0 newly installed, 0 to remove and 1812 not upgraded.
Need to get 6267 kB of archives.
After this operation, 287 kB of additional disk space will be used.
```

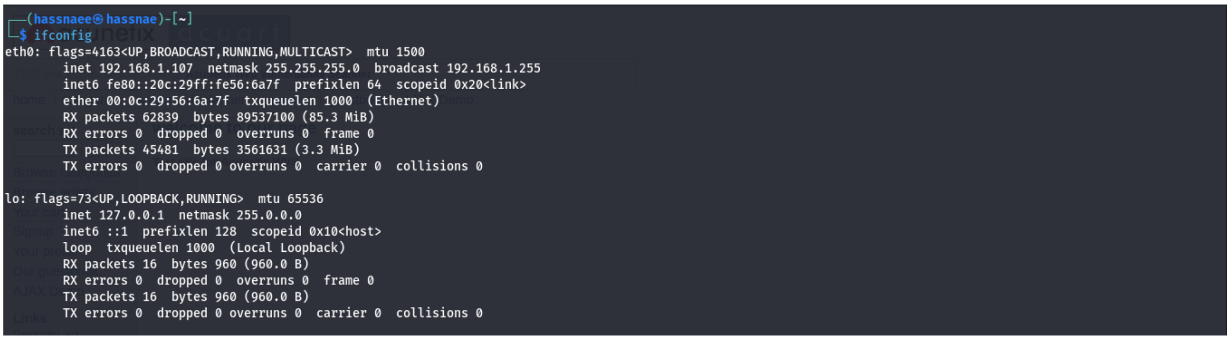


```
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nmap-common
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 0 newly installed, 0 to remove and 1812 not upgraded.
Need to get 6267 kB of archives.
After this operation, 287 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-4kali2 [1935 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-4kali2 [4333 kB]
Fetched 6267 kB in 27s (231 kB/s)
(Reading database ... 530501 files and directories currently installed.)
Preparing to unpack .../nmap_7.94+git20230807.3be01efb1+dfsg-4kali2_amd64.deb ...
Unpacking nmap (7.94+git20230807.3be01efb1+dfsg-4kali2) over (7.94+git20230807.3be01efb1+dfsg-2+kali2+b1) ...
Preparing to unpack .../nmap-common_7.94+git20230807.3be01efb1+dfsg-4kali2_all.deb ...
Unpacking nmap-common (7.94+git20230807.3be01efb1+dfsg-4kali2) over (7.94+git20230807.3be01efb1+dfsg-2+kali2) ...
Setting up nmap-common (7.94+git20230807.3be01efb1+dfsg-4kali2) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-4kali2) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for wordlists (2023.2.0) ...
```

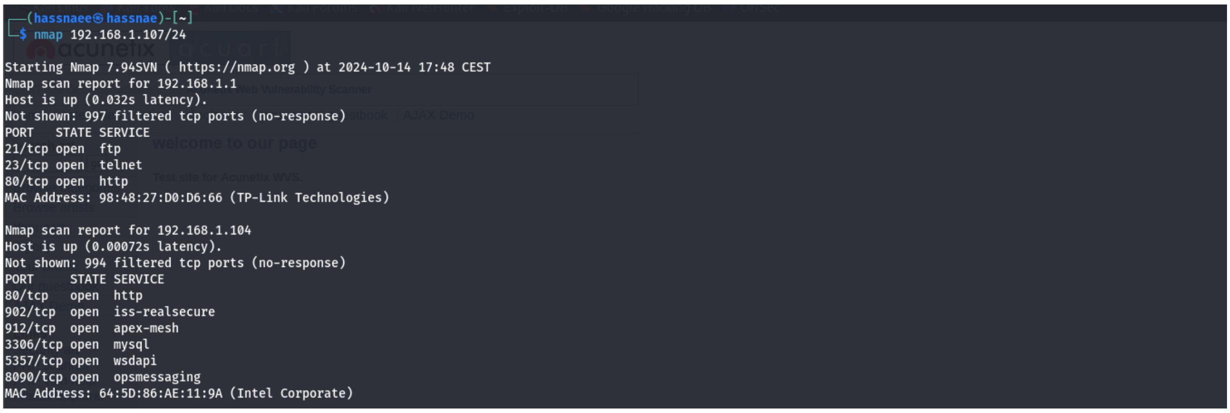
Task 1: Basic Network Scan

Step 1: Open a terminal on your Kali Linux machine.
Step 2: Run a basic scan on your local network.

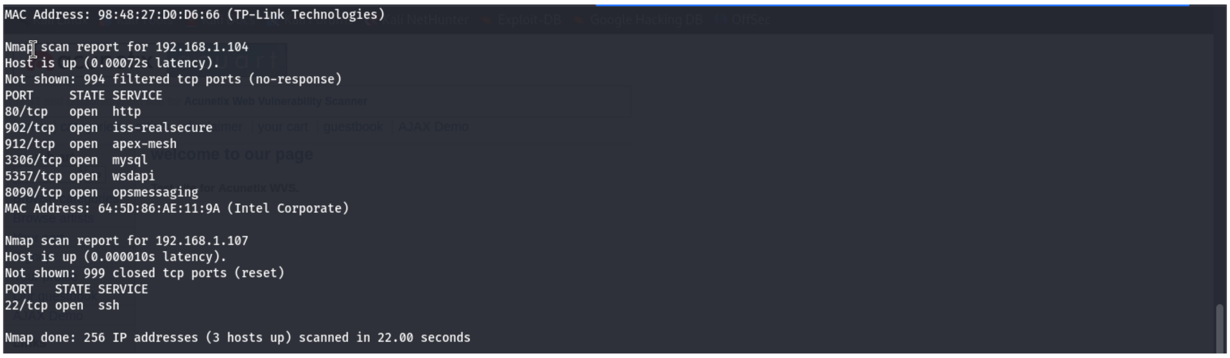
```
nmap 192.168.1.107/24
```



```
┌──(hassnaee㉿hassnae)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.107  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe56:6a7f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:56:6a:7f  txqueuelen 1000  (Ethernet)
        RX packets 62839  bytes 89537100 (85.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45481  bytes 3561631 (3.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(hassnaee㉿hassnae)-[~]
└─$ nmap 192.168.1.107/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 17:48 CEST
Nmap scan report for 192.168.1.1
Host is up (0.032s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)

Nmap scan report for 192.168.1.104
Host is up (0.00072s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi
8090/tcp open  opsmessaging
MAC Address: 64:5D:86:AE:11:9A (Intel Corporate)
```

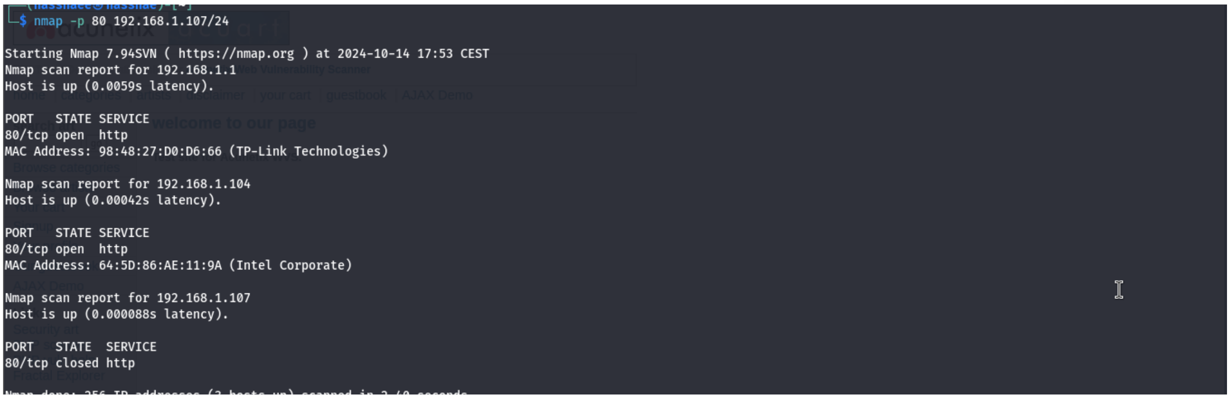


```
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)

Nmap scan report for 192.168.1.104
Host is up (0.00072s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi
8090/tcp open  opsmessaging
MAC Address: 64:5D:86:AE:11:9A (Intel Corporate)

Nmap scan report for 192.168.1.107
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 22.00 seconds
```

Task 2: Scanning for Specific Ports

Step 1: To scan for specific ports (e.g., HTTP port 80), use the `-p` option:

```
nmap -p 80 192.168.1.107/24
```

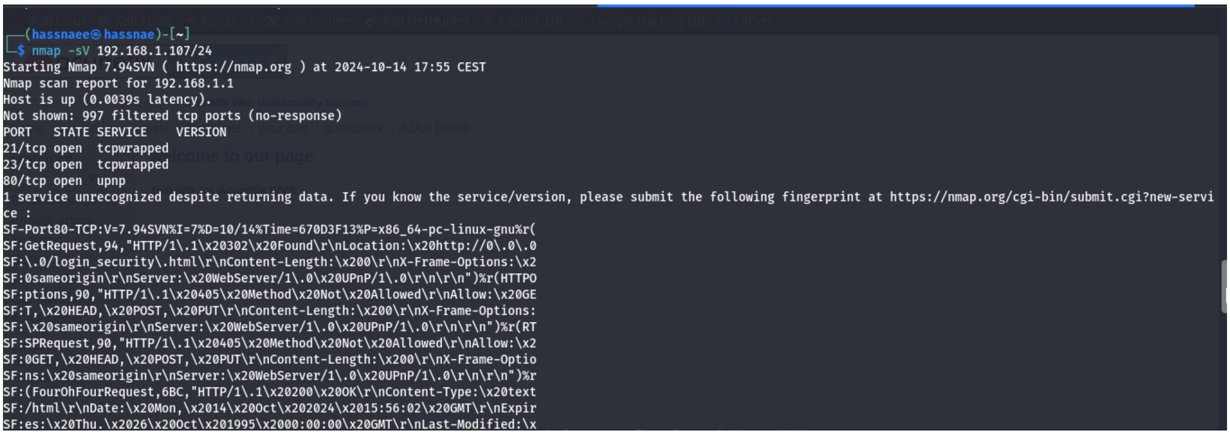


```
┌──(hassnaee㉿hassnae)-[~]
└─$ nmap -p 80 192.168.1.107/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 17:53 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0059s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)

Nmap scan report for 192.168.1.104
Host is up (0.00042s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 64:5D:86:AE:11:9A (Intel Corporate)

Nmap scan report for 192.168.1.107
Host is up (0.000088s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.40 seconds
```

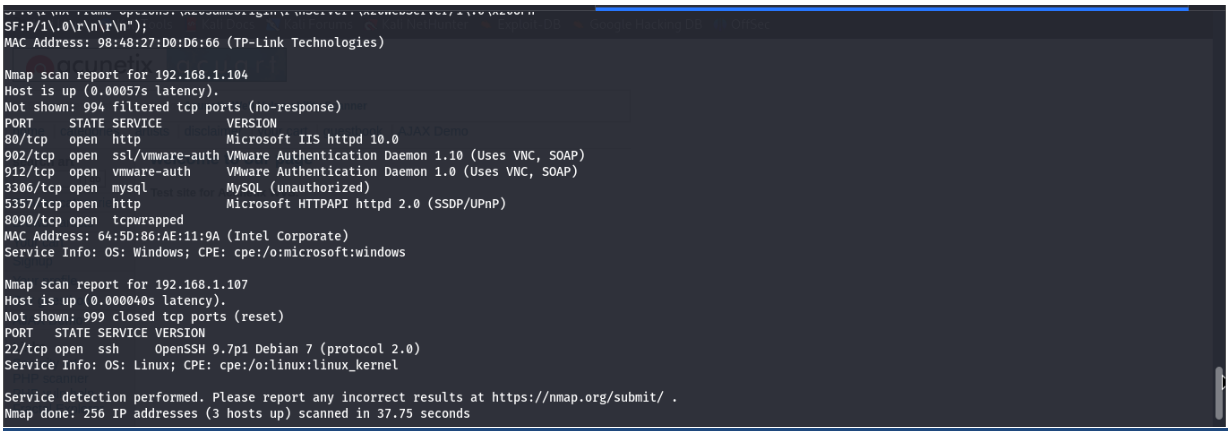
Task 3: Service Version Detection

Step 1: Use the `-sV` option to detect the version of services running on open ports:

nmap -sV 192.168.1.107/24



```
┌──(hassnaee㉿hassnae)-[~]
└─$ nmap -sV 192.168.1.107/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 17:55 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0039s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
23/tcp open  tcpwrapped
80/tcp open  upnp
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port80-TCP:V=7.94SVN%I=7%D=10/14%Time=670D3F13%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,94,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20http://0\.0\.0
SF:\.0/login_security\.html\r\nContent-Length:\x200\r\nX-Frame-Options:\x2
SF:0sameorigin\r\nServer:\x20WebServer/1\.0\x20UPnP/1\.0\r\n\r\n")%r(HTTPO
SF:ptions,90,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x20GE
SF:T,\x20HEAD,\x20POST,\x20PUT\r\nContent-Length:\x200\r\nX-Frame-Options:
SF:\x20sameorigin\r\nServer:\x20WebServer/1\.0\x20UPnP/1\.0\r\n\r\n")%r(RT
SF:SPRequest,90,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x2
SF:0GET,\x20HEAD,\x20POST,\x20PUT\r\nContent-Length:\x200\r\nX-Frame-Optio
SF:ns:\x20sameorigin\r\nServer:\x20WebServer/1\.0\x20UPnP/1\.0\r\n\r\n")%r
SF:(FourOhFourRequest,6BC,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text
SF:/html\r\nDate:\x20Mon,\x2014\x20Oct\x202024\x2015:56:02\x20GMT\r\nExpir
SF:es:\x20Thu.\x2026\x20Oct\x201995\x2000:00:00\x20GMT\r\nLast-Modified:\x
```

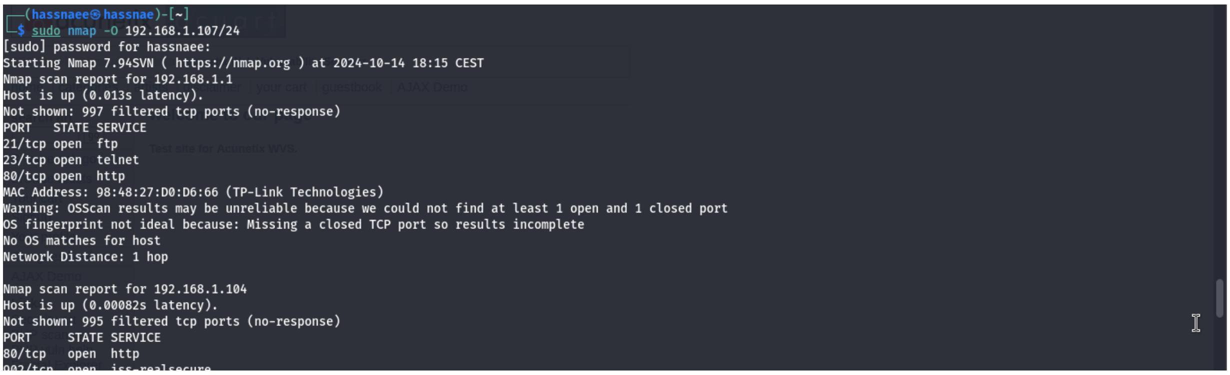


```
SF:0\r\nX-Frame-Options:\x20sameorigin\r\nServer:\x20WebServer/1\.0\x20UPn
SF:P/1\.0\r\n\r\n");
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)

Nmap scan report for 192.168.1.104
Host is up (0.00057s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE          VERSION
80/tcp   open  http             Microsoft IIS httpd 10.0
902/tcp  open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp open  mysql            MySQL (unauthorized)
5357/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8090/tcp open  tcpwrapped
MAC Address: 64:5D:86:AE:11:9A (Intel Corporate)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.107
Host is up (0.000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.7p1 Debian 7 (protocol 2.0)
Service Info: OS: 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 (3 hosts up) scanned in 37.75 seconds
```

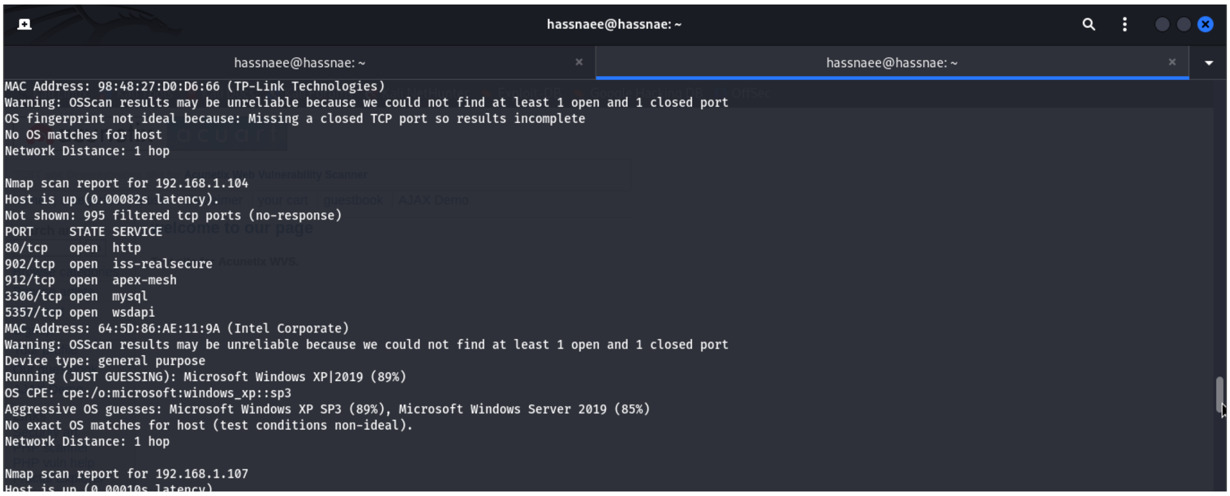
Task 4: Operating System Detection

Step 1: Use the `-O` option to detect the operating systems of devices on the network:

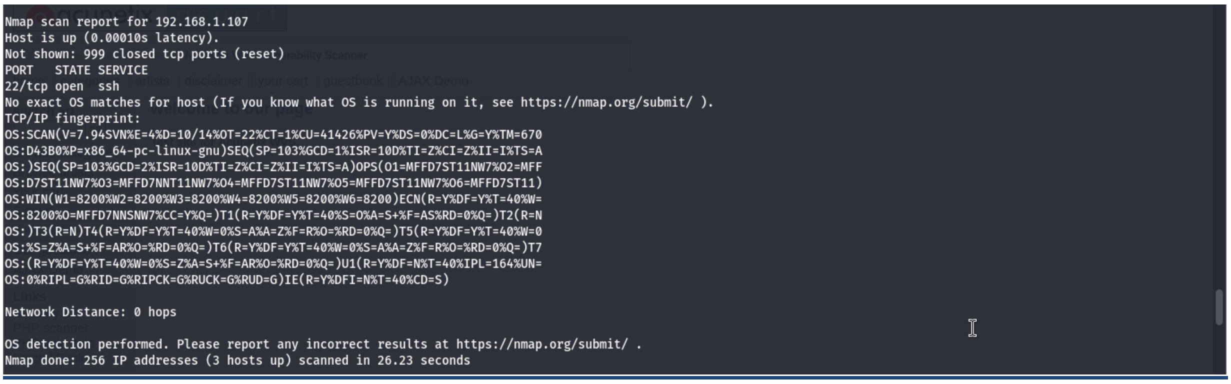
```
sudo nmap -O 192.168.1.107/24
```



```
┌──(hassnaee㉿hassnae)-[~]
└─$ sudo nmap -O 192.168.1.107/24
[sudo] password for hassnaee:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 18:15 CEST
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

Nmap scan report for 192.168.1.104
Host is up (0.00082s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
902/tcp  open  iss-realsecure
```



```
MAC Address: 98:48:27:D0:D6:66 (TP-Link Technologies)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

Nmap scan report for 192.168.1.104
Host is up (0.00082s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 64:5D:86:AE:11:9A (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.1.107
Host is up (0.00010s latency).
```

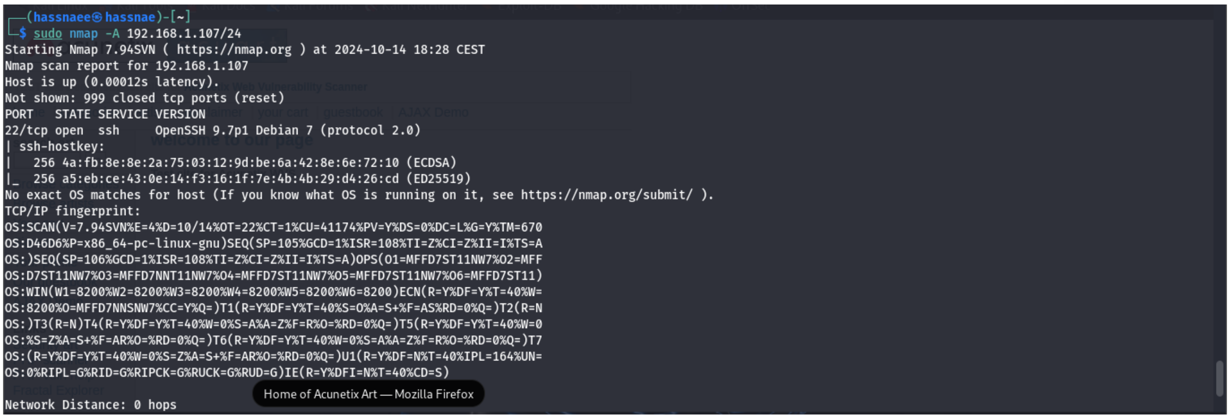


```
Nmap scan report for 192.168.1.107
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/14%OT=22%CT=1%CU=41426%PV=Y%DS=0%DC=L%G=Y%TM=670
OS:D43B0%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(SP=103%GCD=2%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS(O1=MFFD7ST11NW7%O2=MFF
OS:D7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MFFD7ST11)
OS:WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6=8200)ECN(R=Y%DF=Y%T=40%W=
OS:8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 26.23 seconds
```

Task 5: Aggressive Scan

Step 1: Perform an aggressive scan using the `-A` option, which includes OS detection, version detection, script scanning, and traceroute:

```
sudo nmap -A 192.168.1.107/24
```



```
┌──(hassnaee㉿hassnae)-[~]
└─$ sudo nmap -A 192.168.1.107/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 18:28 CEST
Nmap scan report for 192.168.1.107
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.7p1 Debian 7 (protocol 2.0)
| ssh-hostkey: 
|   256 4a:fb:8e:8e:2a:75:03:12:9d:be:6a:42:8e:6e:72:10 (ECDSA)
|_  256 a5:eb:ce:43:0e:14:f3:16:1f:7e:4b:4b:29:d4:26:cd (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/14%OT=22%CT=1%CU=41174%PV=Y%DS=0%DC=L%G=Y%TM=670
OS:D46D6%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=MFFD7ST11NW7%O2=MFF
OS:D7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MFFD7ST11)
OS:WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6=8200)ECN(R=Y%DF=Y%T=40%W=
OS:8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops
```

Conclusion

This project provided a solid foundation in using Nmap for network scanning and enumeration. The skills learned are essential for any ethical hacker, enabling the identification of devices and services within a network and the assessment of potential vulnerabilities.