Basic Network Scanning with Nmap

Objective:

To learn how to perform network scanning and reconnaissance using Nmap, identify hosts and open ports on a specified network or IP range, and generate a report on the discovered devices and services.

Tools:

- Nmap
- Terminal/Command Prompt

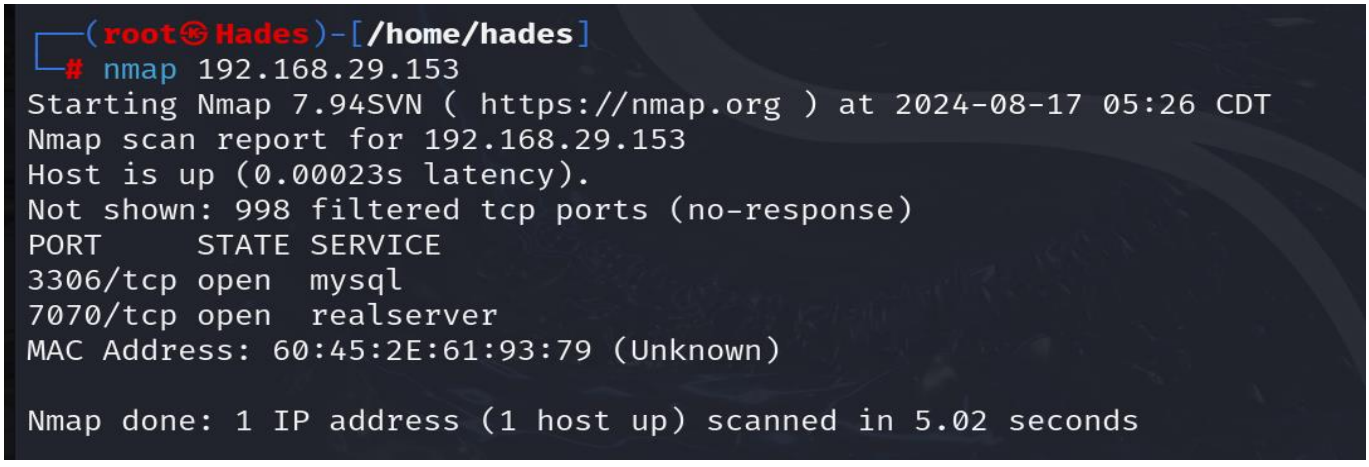
Steps:

1. **Install Nmap** (if not already installed):
    - **Windows:** Download the installer from Nmap's official site and follow the installation instructions.
    - **Linux:** Use the package manager. For example, on Ubuntu:

      sudo apt-get install nmap
    - **macOS:** Use Homebrew:

      brew install nmap
2. **Open Terminal/Command Prompt**:
    - On Windows, you can open Command Prompt or PowerShell.
    - On macOS or Linux, open the Terminal.
3. **Basic Nmap Command**:
    - To scan a single IP address:

      nmap 192.168.29.153



    - To scan a range of IP addresses:

      nmap 192.168.29.1-254

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap 192.168.29.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 05:40 CDT
Stats: 0:00:43 elapsed; 248 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.56% done; ETC: 05:40 (0:00:04 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8002/tcp closed teradataordbms
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)

Nmap scan report for 192.168.29.41
Host is up (0.0036s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:01:02:BA:96:6C (Unknown)

Nmap scan report for 192.168.29.65
Host is up (0.0054s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:A1:77:9B:CE:60 (Unknown)

Nmap scan report for 192.168.29.151
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
```

```
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:C8:90:72:9E:9E (Unknown)

Nmap scan report for 192.168.29.153
Host is up (0.00034s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 60:45:2E:61:93:79 (Unknown)

Nmap scan report for 192.168.29.160
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 254 IP addresses (6 hosts up) scanned in 50.26 seconds
```

- To scan an entire subnet:

  nmap 192.168.29.0/24

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 05:49 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0026s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8002/tcp closed teradataordbms
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)

Nmap scan report for 192.168.29.41
Host is up (0.0034s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:01:02:BA:96:6C (Unknown)

Nmap scan report for 192.168.29.65
Host is up (0.060s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:A1:77:9B:CE:60 (Unknown)

Nmap scan report for 192.168.29.151
Host is up (0.0092s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:C8:90:72:9E:9E (Unknown)
```

```
Nmap scan report for 192.168.29.153
Host is up (0.00026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 60:45:2E:61:93:79 (Unknown)

Nmap scan report for 192.168.29.160
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 29.02 seconds
```

4. **Common Nmap Options**:

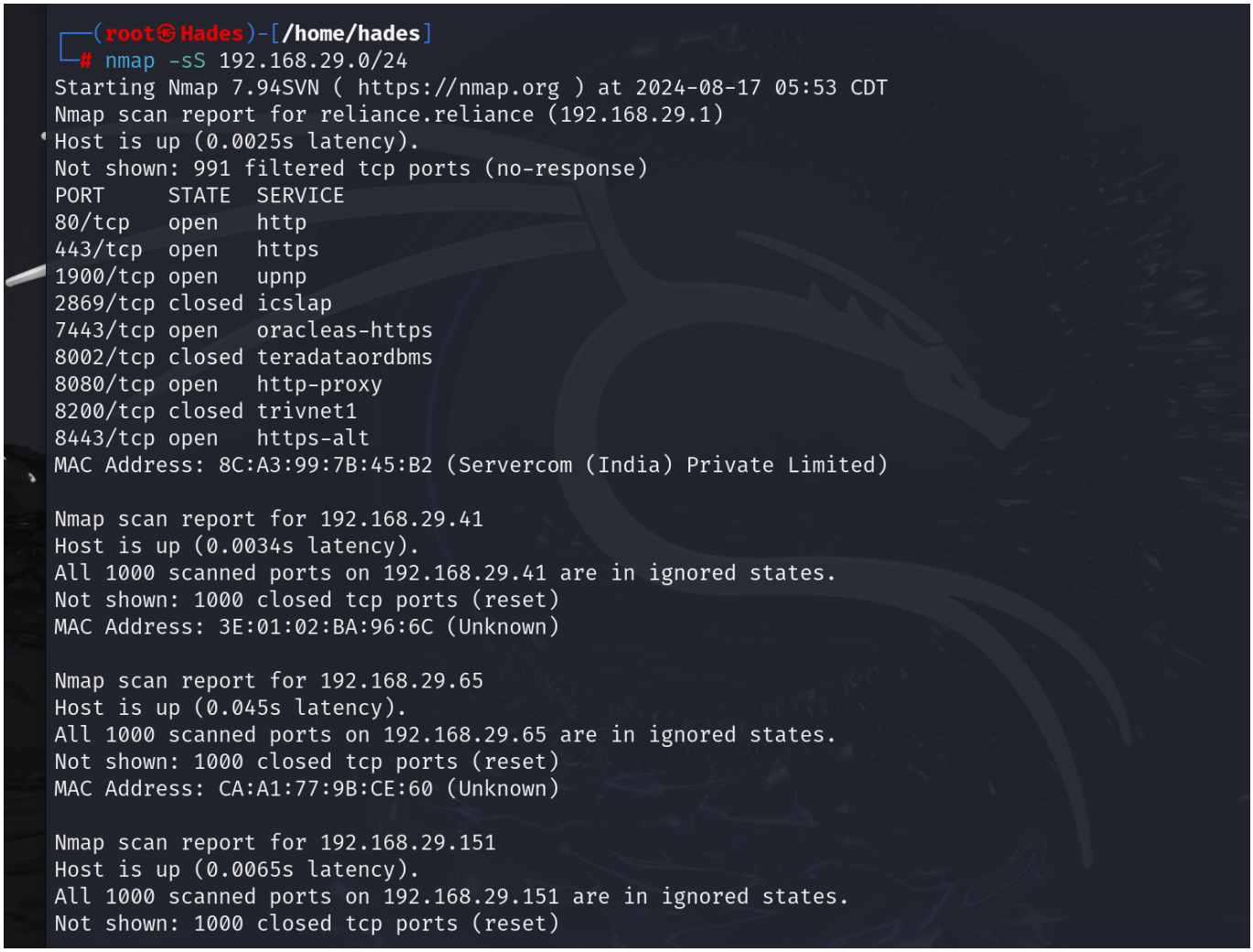
   - **-sP** (Ping scan - find which hosts are up):

     nmap -sP 192.168.29.0/24

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap -sP 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 05:52 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0027s latency).
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)
Nmap scan report for 192.168.29.41
Host is up (0.21s latency).
MAC Address: 3E:01:02:BA:96:6C (Unknown)
Nmap scan report for 192.168.29.65
Host is up (0.071s latency).
MAC Address: CA:A1:77:9B:CE:60 (Unknown)
Nmap scan report for 192.168.29.151
Host is up (0.019s latency).
MAC Address: E6:C8:90:72:9E:9E (Unknown)
Nmap scan report for 192.168.29.153
Host is up (0.00011s latency).
MAC Address: 60:45:2E:61:93:79 (Unknown)
Nmap scan report for 192.168.29.160
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.45 seconds
```

- **-sS** (Stealth scan - to identify open ports):

  nmap -sS 192.168.29.0/24

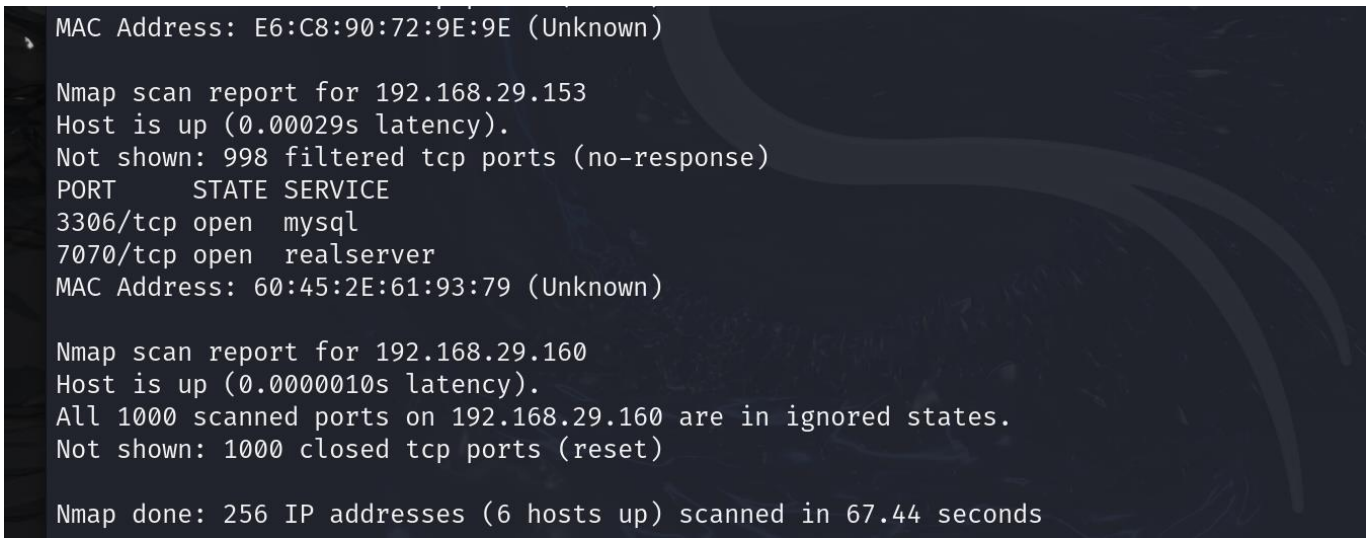


```
┌──(root㉿Hades)-[/home/hades]
└─# nmap -sS 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 05:53 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0025s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8002/tcp closed teradataordbms
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)

Nmap scan report for 192.168.29.41
Host is up (0.0034s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:01:02:BA:96:6C (Unknown)

Nmap scan report for 192.168.29.65
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:A1:77:9B:CE:60 (Unknown)

Nmap scan report for 192.168.29.151
Host is up (0.0065s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```



```
MAC Address: E6:C8:90:72:9E:9E (Unknown)

Nmap scan report for 192.168.29.153
Host is up (0.00029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 60:45:2E:61:93:79 (Unknown)

Nmap scan report for 192.168.29.160
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 67.44 seconds
```

- **-O** (OS detection - to identify the operating system of the host):

  nmap -O 192.168.29.0/24

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap -O 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 05:56 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0026s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8002/tcp closed teradataordbms
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)
Device type: general purpose|firewall|storage-misc|WAP
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X|2.4.X (99%), IPFire 2.X (91%), Synology DiskStation Manager 5.X (90%), WatchG
uard Fireware 11.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:ipfire:ipfire:2.11
 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kern
el:2.4
Aggressive OS guesses: Linux 3.10 - 3.12 (99%), Linux 3.11 - 4.1 (95%), Linux 2.6.32 (95%), Linux 4.4 (95%), Linux 2.6.37
(94%), Linux 2.6.32 - 2.6.35 (93%), Linux 2.6.32 - 2.6.39 (93%), Linux 4.9 (93%), Linux 3.10 - 4.11 (92%), Linux 3.2 - 3.8
 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.29.41
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
MAC Address: 3E:01:02:BA:96:6C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.65
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:A1:77:9B:CE:60 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.151
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:C8:90:72:9E:9E (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.153
Host is up (0.00031s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 60:45:2E:61:93:79 (Unknown)
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 11|10|2022 (92%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsoft W
indows Server 2022 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.29.160
Host is up (0.000022s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 87.97 seconds
```

- **-sV** (Service/version detection - to determine the service/version info):

  nmap -sV 192.168.29.0/24

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap -sV 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 06:01 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0029s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE            VERSION
80/tcp   open   http               lighttpd
443/tcp  open   ssl/http           lighttpd
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   ssl/oracleas-https?
8002/tcp closed teradataordbms
8080/tcp open   http-proxy         JCOW404/JUICEJFV-1.3.30
8200/tcp closed trivnet1
8443/tcp open   ssl/https-alt      JCOW404/JUICEJFV-1.3.30
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints
at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1900-TCP:V=7.94SVN%I=7%D=8/17%Time=66C0835C%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20Linux\x2
SF:0UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/reliance\
SF:.reliance\r\nContent-Length:\x2048\r\nContent-Type:\x20text/html\r\n\r\
SF:n<HTML><BODY><H1>404\x20Not\x20Found</H1></BODY></HTML>")%r(HTTPOptions
SF:,DB,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nServer:\x20Linux\x
SF:20UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/reliance
SF:\.reliance\r\nContent-Length:\x2057\r\nContent-Type:\x20text/html\r\n\r
SF:\n<HTML><BODY><H1>405\x20Method\x20Not\x20Allowed</H1></BODY></HTML>")%
SF:r(FourOhFourRequest,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20
SF:Linux\x20UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/r
SF:eliance\.reliance\r\nContent-Length:\x2048\r\nContent-Type:\x20text/htm
SF:l\r\n\r\n<HTML><BODY><H1>404\x20Not\x20Found</H1></BODY></HTML>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.94SVN%I=7%D=8/17%Time=66C08357%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,98,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\nContent-L
SF:ength:\x2019\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nS
SF:erver:\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nService\x20Unavailable")%r(H
```

```
SF:TTPOptions,90,"HTTP/1\.0\x20501\x20Not\x20Implemented\r\nContent-Length
SF::\x2015\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nServer
SF::\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nNot\x20implemented")%r(FourOhFour
SF:Request,88,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2011
SF:\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nServer:\x20JC
SF:OW404/JUICEJFV-1\.3\.30\r\n\r\nBad\x20Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8443-TCP:V=7.94SVN%T=SSL%I=7%D=8/17%Time=66C0835E%P=x86_64-pc-linux
SF:-gnu%r(FourOhFourRequest,88,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCont
SF:ent-Length:\x2011\r\nContent-Type:\x20text/html\r\nConnection:\x20close
SF:\r\nServer:\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nBad\x20Request")%r(RPCC
SF:heck,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\n
SF:Content-Type:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Reques
SF:t")%r(DNSStatusRequestTCP,65,"\(null\)\x20400\x20Bad\x20Request\r\nCont
SF:ent-Length:\x2011\r\nContent-Type:\x20text/html\r\nConnection:\x20close
SF:\r\n\r\nBad\x20Request")%r(SMBProgNeg,65,"\(null\)\x20400\x20Bad\x20Req
SF:uest\r\nContent-Length:\x2011\r\nContent-Type:\x20text/html\r\nConnecti
SF:on:\x20close\r\n\r\nBad\x20Request")%r(X11Probe,65,"\(null\)\x20400\x20
SF:Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Type:\x20text/html\r
SF:\nConnection:\x20close\r\n\r\nBad\x20Request")%r(TerminalServer,65,"\(n
SF:ull\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Type
SF::\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Request")%r(NotesR
SF:PC,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nCo
SF:ntent-Type:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Request"
SF:);
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)

Nmap scan report for 192.168.29.41
Host is up (0.0041s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:01:02:BA:96:6C (Unknown)

Nmap scan report for 192.168.29.65
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
MAC Address: CA:A1:77:9B:CE:60 (Unknown)

Nmap scan report for 192.168.29.151
Host is up (0.094s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:C8:90:72:9E:9E (Unknown)

Nmap scan report for 192.168.29.153
Host is up (0.00023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
3306/tcp open  mysql           MySQL 8.4.0
7070/tcp open  ssl/realserver?
MAC Address: 60:45:2E:61:93:79 (Unknown)

Nmap scan report for 192.168.29.160
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 109.77 seconds
```

- **-A** (Aggressive scan - includes OS detection, version detection, script scanning, and traceroute):

  nmap -sV 192.168.29.0/24

```
┌──(root㉿Hades)-[/home/hades]
└─# nmap -sV 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 06:07 CDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE             VERSION
80/tcp   open   http                lighttpd
443/tcp  open   ssl/http            lighttpd
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   ssl/oracleas-https?
8002/tcp closed teradataordbms
8080/tcp open   http-proxy          JCOW404/JUICEJFV-1.3.30
8200/tcp closed trivnet1
8443/tcp open   ssl/https-alt       JCOW404/JUICEJFV-1.3.30
4 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at ht
tps://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1900-TCP:V=7.94SVN%I=7%D=8/17%Time=66C084BE%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20Linux\x2
SF:0UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/reliance\
SF:.reliance\r\nContent-Length:\x2048\r\nContent-Type:\x20text/html\r\n\r\
SF:n<HTML><BODY><H1>404\x20Not\x20Found</H1></BODY></HTML>")%r(HTTPOptions
SF:,DB,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nServer:\x20Linux\x
SF:20UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/reliance
SF:\.reliance\r\nContent-Length:\x2057\r\nContent-Type:\x20text/html\r\n\r
SF:\n<HTML><BODY><H1>405\x20Method\x20Not\x20Allowed</H1></BODY></HTML>")%
SF:r(FourOhFourRequest,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nServer:\x20
SF:Linux\x20UPnP/1\.0\x20DLNADOC/1\.50\x20AccessTwine/1\.0-RAS\x20Device/r
SF:eliance\.reliance\r\nContent-Length:\x2048\r\nContent-Type:\x20text/htm
SF:l\r\n\r\n<HTML><BODY><H1>404\x20Not\x20Found</H1></BODY></HTML>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7443-TCP:V=7.94SVN%T=SSL%I=7%D=8/17%Time=66C084C1%P=x86_64-pc-linux
SF:-gnu%r(HTTPOptions,90,"HTTP/1\.0\x20501\x20Not\x20Implemented\r\nConten
SF:t-Length:\x2015\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r
SF:\nServer:\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nNot\x20implemented");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

```
SF-Port8080-TCP:V=7.94SVN%I=7%D=8/17%Time=66C084B9%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,98,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\nContent-L
SF:ength:\x2019\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nS
SF:erver:\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nService\x20Unavailable")%r(H
SF:TTPOptions,90,"HTTP/1\.0\x20501\x20Not\x20Implemented\r\nContent-Length
SF::\x2015\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nServer
SF::\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nNot\x20implemented")%r(FourOhFour
SF:Request,88,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2011
SF:\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nServer:\x20JC
SF:OW404/JUICEJFV-1\.3\.30\r\n\r\nBad\x20Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8443-TCP:V=7.94SVN%T=SSL%I=7%D=8/17%Time=66C084C0%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,88,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Len
SF:gth:\x2011\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nSer
SF:ver:\x20JCOW404/JUICEJFV-1\.3\.30\r\n\r\nBad\x20Request")%r(HTTPOptions
SF:,90,"HTTP/1\.0\x20501\x20Not\x20Implemented\r\nContent-Length:\x2015\r\
SF:nContent-Type:\x20text/html\r\nConnection:\x20close\r\nServer:\x20JCOW4
SF:04/JUICEJFV-1\.3\.30\r\n\r\nNot\x20implemented")%r(FourOhFourRequest,88
SF:,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nConten
SF:t-Type:\x20text/html\r\nConnection:\x20close\r\nServer:\x20JCOW404/JUIC
SF:EJFV-1\.3\.30\r\n\r\nBad\x20Request")%r(DNSStatusRequestTCP,65,"\(null\
SF:)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Type:\x2
SF:0text/html\r\nConnection:\x20close\r\n\r\nBad\x20Request")%r(SMBProgNeg
SF:,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nCont
SF:ent-Type:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Request")%
SF:r(X11Probe,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x20
SF:11\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20
SF:Request")%r(LDAPBindReq,65,"\(null\)\x20400\x20Bad\x20Request\r\nConten
SF:t-Length:\x2011\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r
SF:\n\r\nBad\x20Request")%r(LANDesk-RC,65,"\(null\)\x20400\x20Bad\x20Reque
SF:st\r\nContent-Length:\x2011\r\nContent-Type:\x20text/html\r\nConnection
SF::\x20close\r\n\r\nBad\x20Request")%r(TerminalServer,65,"\(null\)\x20400
SF:\x20Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Type:\x20text/ht
SF:ml\r\nConnection:\x20close\r\n\r\nBad\x20Request")%r(NCP,65,"\(null\)\x
SF:20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Type:\x20te
SF:xt/html\r\nConnection:\x20close\r\n\r\nBad\x20Request")%r(JavaRMI,65,"\
SF:(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r\nContent-Ty
SF:pe:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Request")%r(WMSR
```

```
SF:equest,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Length:\x2011\r
SF:\nContent-Type:\x20text/html\r\nConnection:\x20close\r\n\r\nBad\x20Requ
SF:est")%r(oracle-tns,65,"\(null\)\x20400\x20Bad\x20Request\r\nContent-Len
SF:gth:\x2011\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\n\r\
SF:nBad\x20Request");
MAC Address: 8C:A3:99:7B:45:B2 (Servercom (India) Private Limited)

Nmap scan report for 192.168.29.41
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.29.41 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:01:02:BA:96:6C (Unknown)

Nmap scan report for 192.168.29.65
Host is up (0.0045s latency).
All 1000 scanned ports on 192.168.29.65 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:A1:77:9B:CE:60 (Unknown)

Nmap scan report for 192.168.29.151
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.29.151 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:C8:90:72:9E:9E (Unknown)

Nmap scan report for 192.168.29.153
Host is up (0.00029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
3306/tcp open  mysql           MySQL 8.4.0
7070/tcp open  ssl/realserver?
MAC Address: 60:45:2E:61:93:79 (Unknown)

Nmap scan report for 192.168.29.160
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.29.160 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 100.98 seconds
```

5. **Generate a Report**:
    - Save the output to a file for further analysis:

      nmap -oN scan_report.txt 192.168.29.0/24
    - Save the output in XML format:

      nmap -oX scan_report.xml 192.168.29.0/24
6. **Analyze the Results**:
    - Identify the live hosts on the network.

      The Nmap scan shows that there are **6 live hosts** on your network. These hosts are:
        - ✓ 192.168.29.1
        - ✓ 192.168.29.41
        - ✓ 192.168.29.65
        - ✓ 192.168.29.151
        - ✓ 192.168.29.153
        - ✓ 192.168.29.160
    - List the open ports services for each host.

      Host: 192.168.29.1
        - **Status:** Host is up.
        - **Open Ports and Services:**
            - 80/tcp: HTTP (web service)
            - 443/tcp: HTTPS (secure web service)
            - 1900/tcp: UPNP (Universal Plug and Play)
            - 7443/tcp: OracleAS-HTTPS (likely a secure web interface for Oracle Application Server)
            - 8080/tcp: HTTP-Proxy (proxy service)
            - 8443/tcp: HTTPS-Alt (alternative secure web service)
        - **MAC Address:** 8C:A3:99:7B:45:B2
        - **Possible Device Type:** This device appears to be a network gateway or router, likely providing internet services (HTTP, HTTPS, UPNP) and possibly Oracle services.

      Host: 192.168.29.41
        - **Status:** Host is up.
        - **Ports:** All 1000 scanned ports are in ignored states, meaning no open ports were detected.
        - **MAC Address:** 3E:01:02:BA:96:6C

- **Possible Device Type:** Unknown. Since no ports are open and the MAC address is unrecognized, it could be a device with no active services exposed.

Host: 192.168.29.65

- **Status:** Host is up.
- **Ports:** All 1000 scanned ports are in ignored states, meaning no open ports were detected.
- **MAC Address:** CA:A1:77:9B:CE:60
- **Possible Device Type:** Unknown, similar to the host at 192.168.29.41.

Host: 192.168.29.151

- **Status:** Host is up.
- **Ports:** All 1000 scanned ports are in ignored states, meaning no open ports were detected.
- **MAC Address:** E6:C8:90:72:9E:9E
- **Possible Device Type:** Unknown, similar to the hosts at 192.168.29.41 and 192.168.29.65.

Host: 192.168.29.153

- **Status:** Host is up.
- **Open Ports and Services:**
  - 3306/tcp: MySQL (database service)
  - 7070/tcp: RealServer (real-time media streaming)
- **MAC Address:** 60:45:2E:61:93:79
- **Possible Device Type:** This could be a server or a device running a database and media server. It could be a specialized server hosting both a MySQL database and streaming media.

Host: 192.168.29.160

- **Status:** Host is up.
- **Ports:** All 1000 scanned ports are in ignored states, meaning no open ports were detected.
- **MAC Address:** Not provided.
- **Possible Device Type:** This is likely your own device (since you mentioned your IP address is 192.168.29.160). It shows no open ports.

- Determine the types of devices based on the OS detection.

✓ **192.168.29.1:** Likely a router or gateway, possibly providing both standard web services and internal network services (e.g., UPNP, Oracle server).

✓ **192.168.29.153:** Likely a server running MySQL and a media streaming service (RealServer).

✓ **Other Devices (192.168.29.41, 192.168.29.65, 192.168.29.151, and 192.168.29.160):** Could be computers, mobile devices, or IoT devices, but no specific information can be gleaned without further OS detection or fingerprinting.

7. **Summary**

- 6 hosts are live on the network.
- Open ports and services:

    - 192.168.29.1: HTTP, HTTPS, UPNP, OracleAS-HTTPS, HTTP-Proxy, HTTPS-Alt.
    - 192.168.29.153: MySQL, RealServer.
- The device types are inferred based on their services, with 192.168.29.1 likely being a router and 192.168.29.153 being a server.
- The other devices did not reveal open ports, suggesting they are either workstations, IoT devices, or other networked devices without exposed services.