Ulric Aird

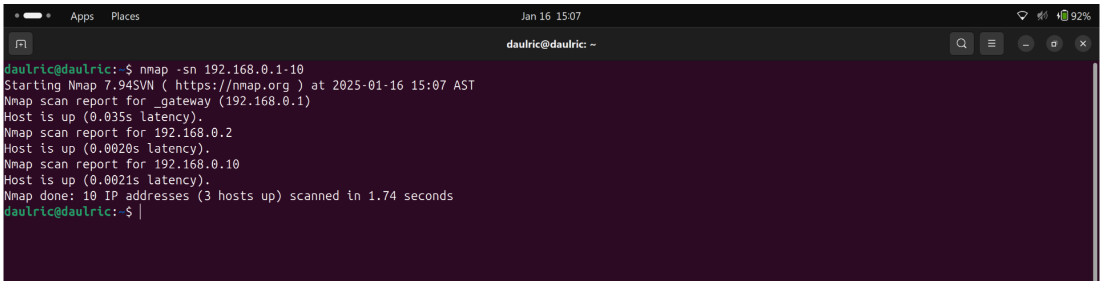
Data Security and Concepts

Lab 2 Assignment

We are doing the alternative lab using Nmap.

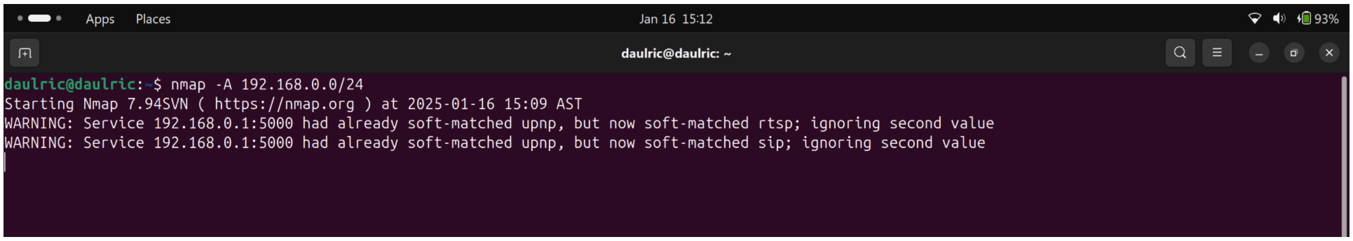
Task 1: Host Discovery

Ping Sweep



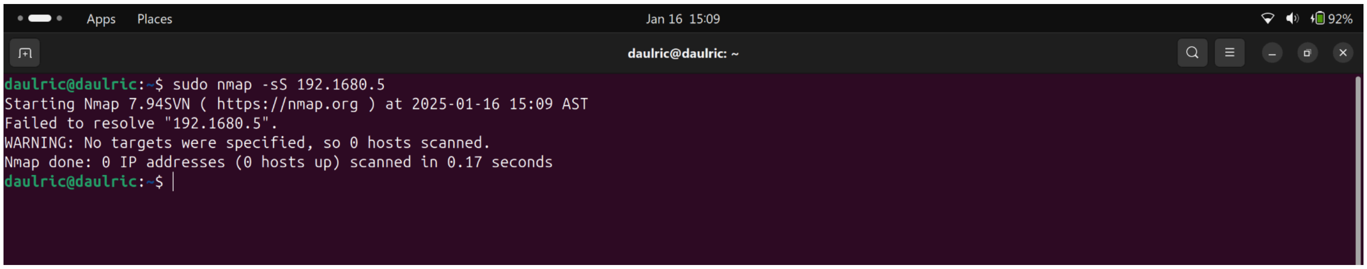
```
daulric@daulric:~$ nmap -sn 192.168.0.1-10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:07 AST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.035s latency).
Nmap scan report for 192.168.0.2
Host is up (0.0020s latency).
Nmap scan report for 192.168.0.10
Host is up (0.0021s latency).
Nmap done: 10 IP addresses (3 hosts up) scanned in 1.74 seconds
daulric@daulric:~$ 
```

SYN Scan



```
daulric@daulric:~$ nmap -A 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:09 AST
WARNING: Service 192.168.0.1:5000 had already soft-matched upnp, but now soft-matched rtsp; ignoring second value
WARNING: Service 192.168.0.1:5000 had already soft-matched upnp, but now soft-matched sip; ignoring second value
```

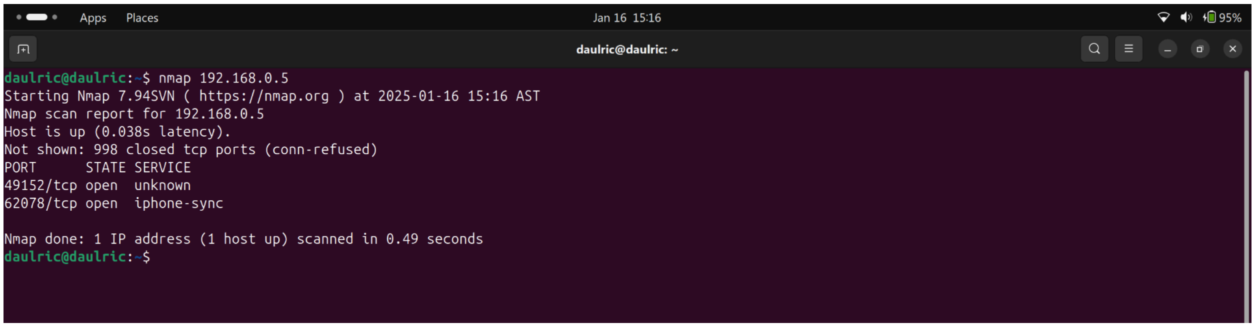
ARP Scan



```
daulric@daulric:~$ sudo nmap -sS 192.1680.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:09 AST
Failed to resolve "192.1680.5".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.17 seconds
daulric@daulric:~$ 
```

Task 2: Port Scanning

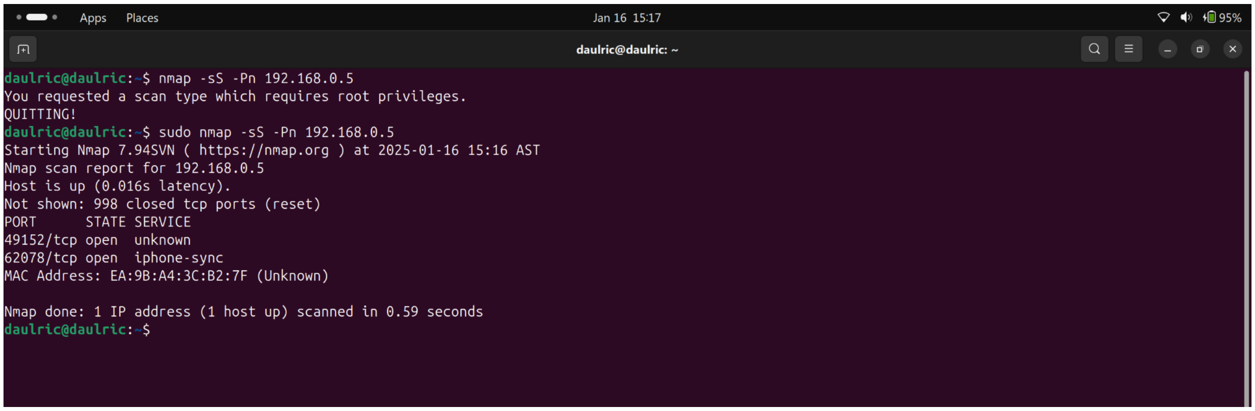
TCP Connect Scan



```
daulric@daulric:~$ nmap 192.168.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:16 AST
Nmap scan report for 192.168.0.5
Host is up (0.038s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
daulric@daulric:~$
```

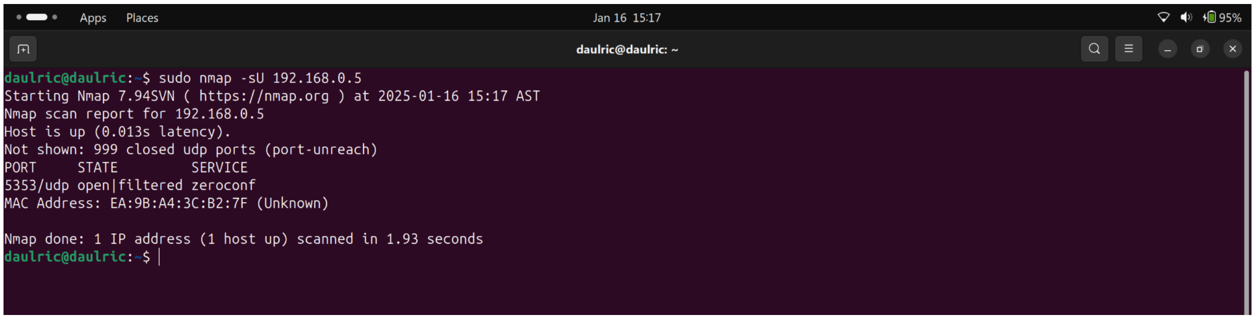
Stealth Scan (SYN Stealth Scan)



```
daulric@daulric:~$ nmap -sS -Pn 192.168.0.5
You requested a scan type which requires root privileges.
QUITTING!
daulric@daulric:~$ sudo nmap -sS -Pn 192.168.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:16 AST
Nmap scan report for 192.168.0.5
Host is up (0.016s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: EA:9B:A4:3C:B2:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
daulric@daulric:~$
```

UDP Scan

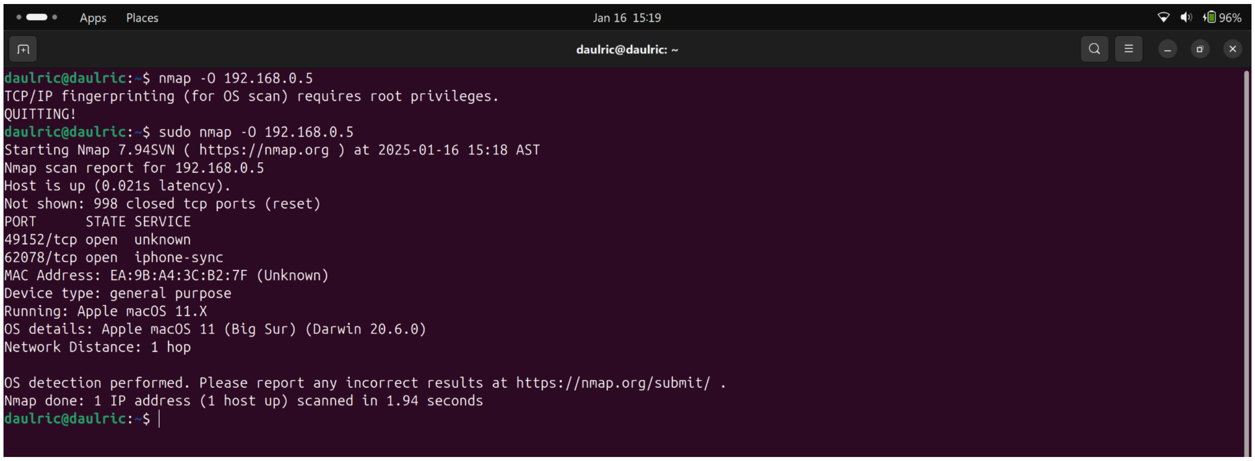


```
daulric@daulric:~$ sudo nmap -sU 192.168.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:17 AST
Nmap scan report for 192.168.0.5
Host is up (0.013s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT     STATE         SERVICE
5353/udp open|filtered zeroconf
MAC Address: EA:9B:A4:3C:B2:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
daulric@daulric:~$
```

Task 3: OS Detection

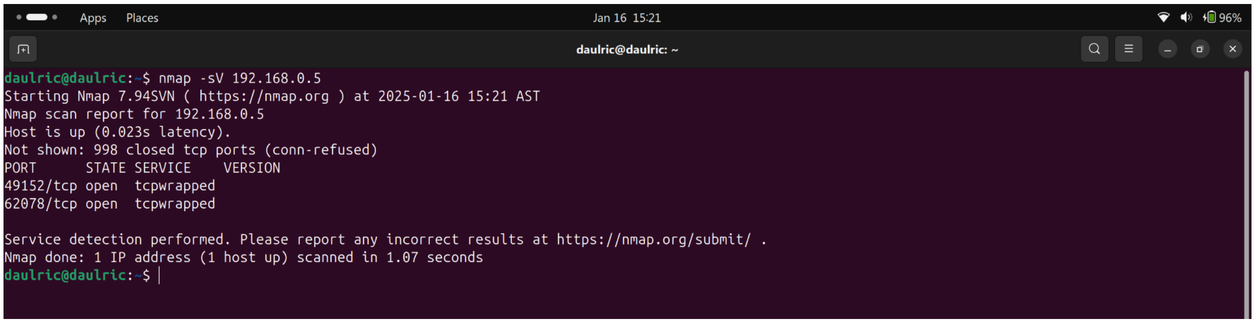
OS Fingerprinting



```
daulric@daulric:~$ nmap -O 192.168.0.5
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
daulric@daulric:~$ sudo nmap -O 192.168.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:18 AST
Nmap scan report for 192.168.0.5
Host is up (0.021s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: EA:9B:A4:3C:B2:7F (Unknown)
Device type: general purpose
Running: Apple macOS 11.X
OS details: Apple macOS 11 (Big Sur) (Darwin 20.6.0)
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 1.94 seconds
daulric@daulric:~$ 
```

Version Detection



```
daulric@daulric:~$ nmap -sV 192.168.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-16 15:21 AST
Nmap scan report for 192.168.0.5
Host is up (0.023s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
49152/tcp open  tcpwrapped
62078/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
daulric@daulric:~$ 
```