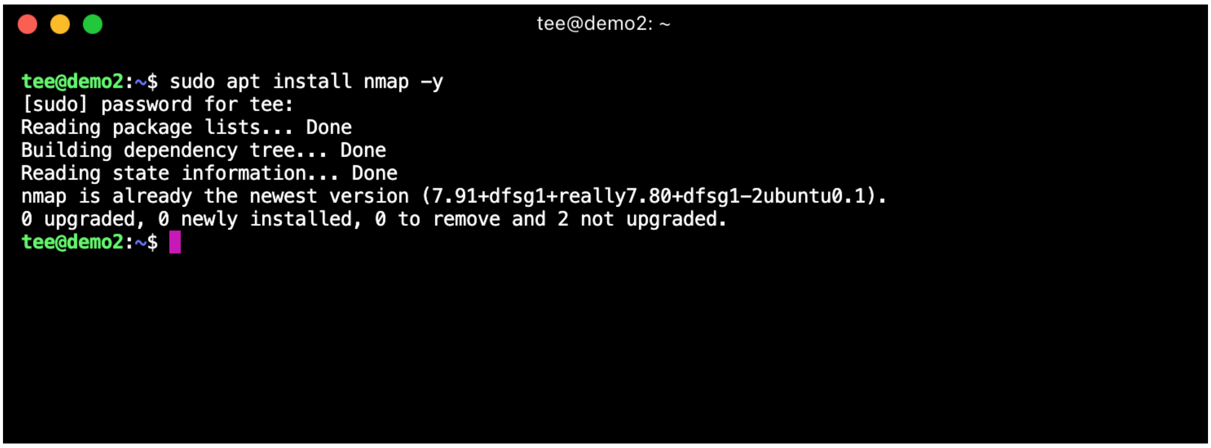
NMAP

Installing and Using NMAP

The first step, like in the use of other applications, is to install nmap. To do this, use the following command: sudo apt install nmap -y as displayed in the terminal below:

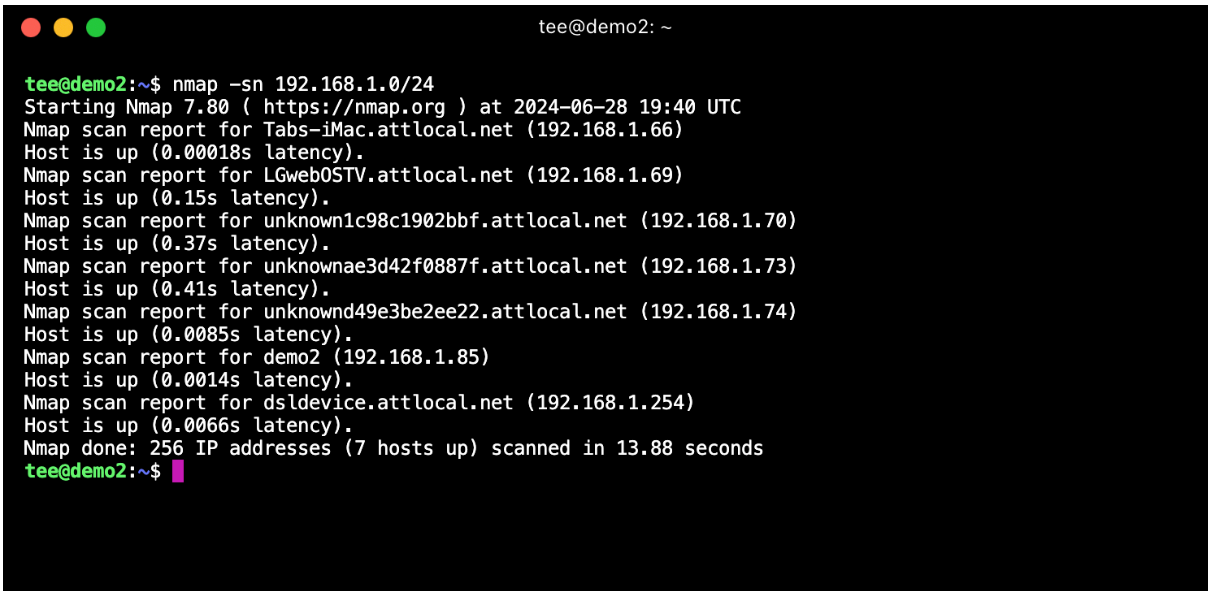


```
tee@demo2:~$ sudo apt install nmap -y
[sudo] password for tee:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
tee@demo2:~$
```

I already have the nmap installed as shown above.

Next step is to conduct discovery scans. These scans are vital to understand the structure of a network, hosts on a network, and potential unwanted guests on the guests.

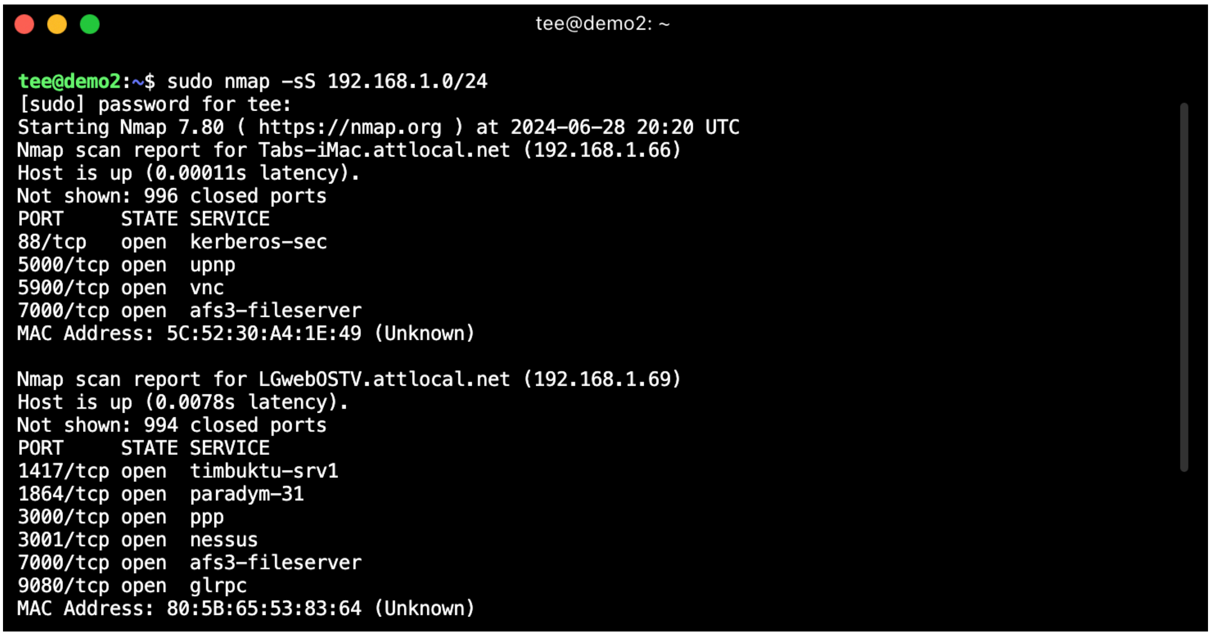
The first scan is the ping scan (ICMP Echo). This can be achieved using the following command: nmap -sn <destination ip address>. This is illustrated below:



```
tee@demo2:~$ nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 19:40 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.00018s latency).
Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.15s latency).
Nmap scan report for unknown1c98c1902bbf.attlocal.net (192.168.1.70)
Host is up (0.37s latency).
Nmap scan report for unknownae3d42f0887f.attlocal.net (192.168.1.73)
Host is up (0.41s latency).
Nmap scan report for unknownd49e3be2ee22.attlocal.net (192.168.1.74)
Host is up (0.0085s latency).
Nmap scan report for demo2 (192.168.1.85)
Host is up (0.0014s latency).
Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.0066s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 13.88 seconds
tee@demo2:~$
```

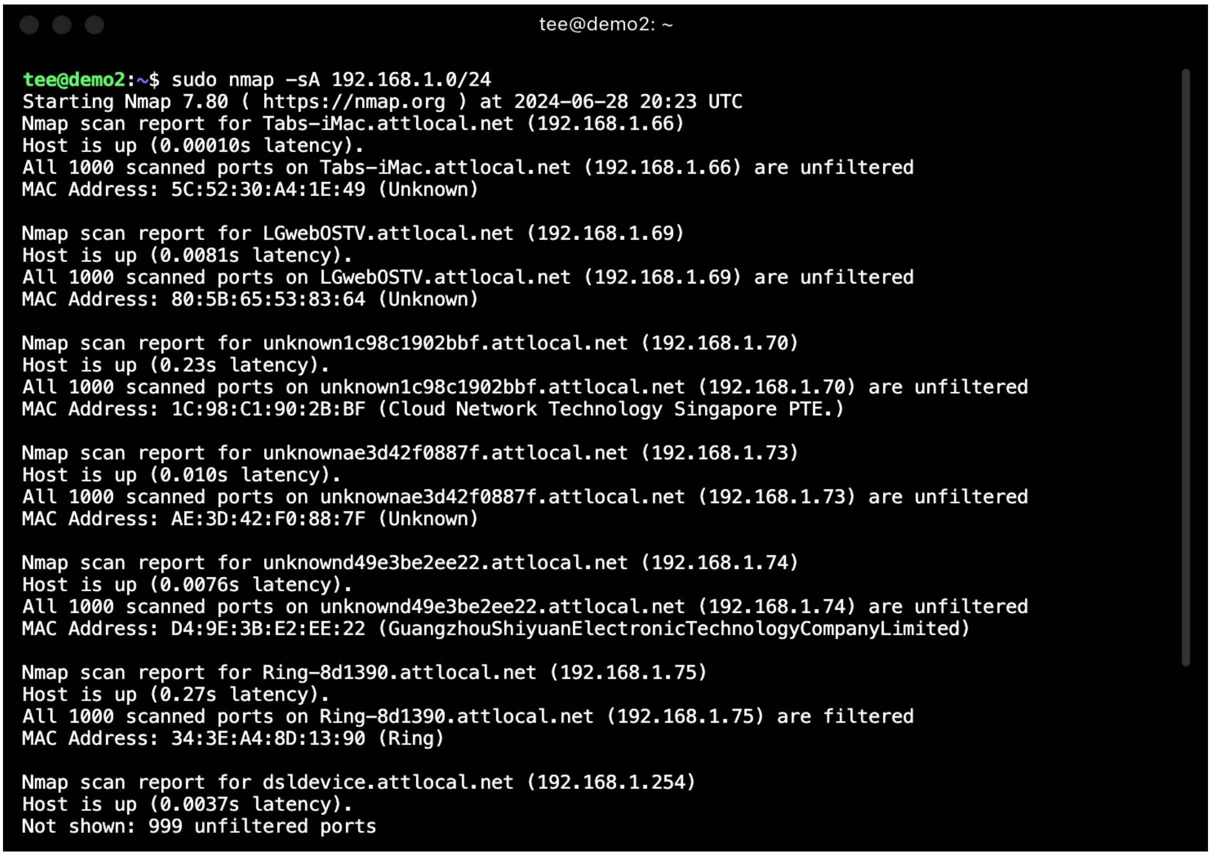
This scan checks target hosts to know if they are online and responsive.

The second scan is the TCP SYN scan to determine if target hosts have open, closed, or filtered ports. This scan is performed using the -sS command. This command requires root privileges, hence use the following command: sudo nmap -sS <destination IP address>. This is illustrated below:



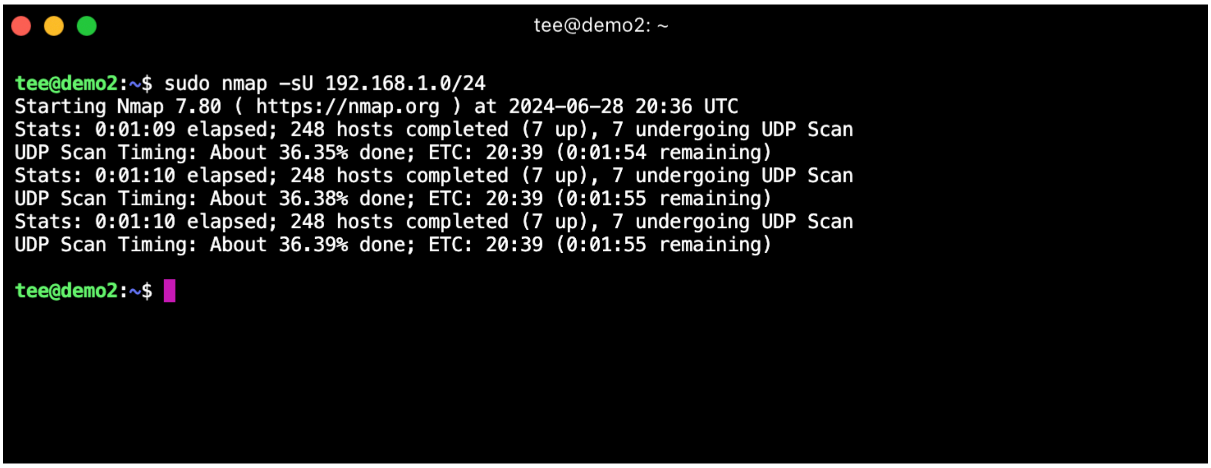
```
tee@demo2:~$ sudo nmap -sS 192.168.1.0/24
[sudo] password for tee:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:20 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.00011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
88/tcp   open  kerberos-sec
5000/tcp open  upnp
5900/tcp open  vnc
7000/tcp open  afs3-fileserver
MAC Address: 5C:52:30:A4:1E:49 (Unknown)

Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.0078s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
1417/tcp open  timbuktu-srv1
1864/tcp open  paradym-31
3000/tcp open  ppp
3001/tcp open  nessus
7000/tcp open  afs3-fileserver
9080/tcp open  glrpc
MAC Address: 80:5B:65:53:83:64 (Unknown)
```

The third scan is the TCP ACK scan to ascertain if ports are filtered by firewalls. This command also requires root privileges, hence the command for this scan is: sudo nmap -sA <destination IP address>. This is illustrated below:



```
tee@demo2:~$ sudo nmap -sA 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:23 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.00010s latency).
All 1000 scanned ports on Tabs-iMac.attlocal.net (192.168.1.66) are unfiltered
MAC Address: 5C:52:30:A4:1E:49 (Unknown)

Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.0081s latency).
All 1000 scanned ports on LGwebOSTV.attlocal.net (192.168.1.69) are unfiltered
MAC Address: 80:5B:65:53:83:64 (Unknown)

Nmap scan report for unknown1c98c1902bbf.attlocal.net (192.168.1.70)
Host is up (0.23s latency).
All 1000 scanned ports on unknown1c98c1902bbf.attlocal.net (192.168.1.70) are unfiltered
MAC Address: 1C:98:C1:90:2B:BF (Cloud Network Technology Singapore PTE.)

Nmap scan report for unknownae3d42f0887f.attlocal.net (192.168.1.73)
Host is up (0.010s latency).
All 1000 scanned ports on unknownae3d42f0887f.attlocal.net (192.168.1.73) are unfiltered
MAC Address: AE:3D:42:F0:88:7F (Unknown)

Nmap scan report for unknownd49e3be2ee22.attlocal.net (192.168.1.74)
Host is up (0.0076s latency).
All 1000 scanned ports on unknownd49e3be2ee22.attlocal.net (192.168.1.74) are unfiltered
MAC Address: D4:9E:3B:E2:EE:22 (GuangzhouShiyuanElectronicTechnologyCompanyLimited)

Nmap scan report for Ring-8d1390.attlocal.net (192.168.1.75)
Host is up (0.27s latency).
All 1000 scanned ports on Ring-8d1390.attlocal.net (192.168.1.75) are filtered
MAC Address: 34:3E:A4:8D:13:90 (Ring)

Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.0037s latency).
Not shown: 999 unfiltered ports
```

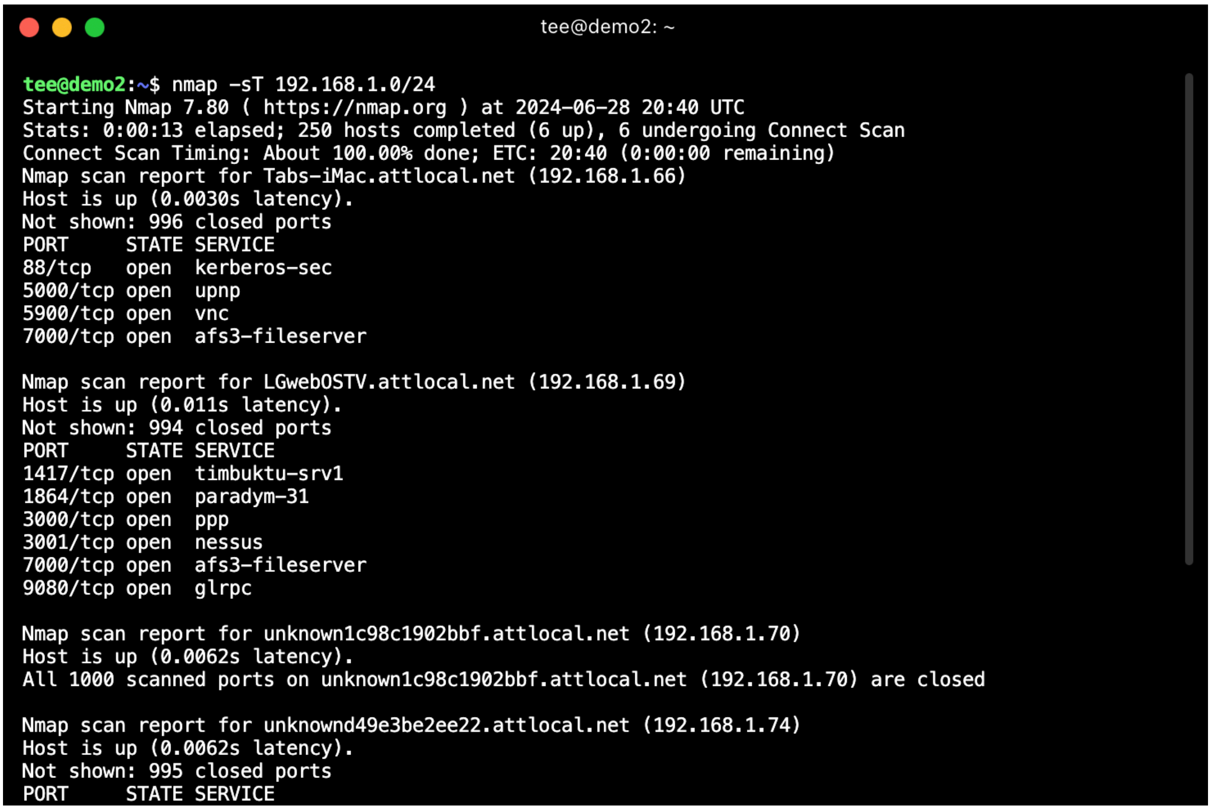
The fourth scan is the UDP scan. This scan sends UDP packets to the target host to identify UDP ports. The command for this is: sudo cleanmap -sU <target IP address>. This is illustrated below:



tee@demo2: ~

```
tee@demo2:~$ sudo nmap -sU 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:36 UTC
Stats: 0:01:09 elapsed; 248 hosts completed (7 up), 7 undergoing UDP Scan
UDP Scan Timing: About 36.35% done; ETC: 20:39 (0:01:54 remaining)
Stats: 0:01:10 elapsed; 248 hosts completed (7 up), 7 undergoing UDP Scan
UDP Scan Timing: About 36.38% done; ETC: 20:39 (0:01:55 remaining)
Stats: 0:01:10 elapsed; 248 hosts completed (7 up), 7 undergoing UDP Scan
UDP Scan Timing: About 36.39% done; ETC: 20:39 (0:01:55 remaining)

tee@demo2:~$
```

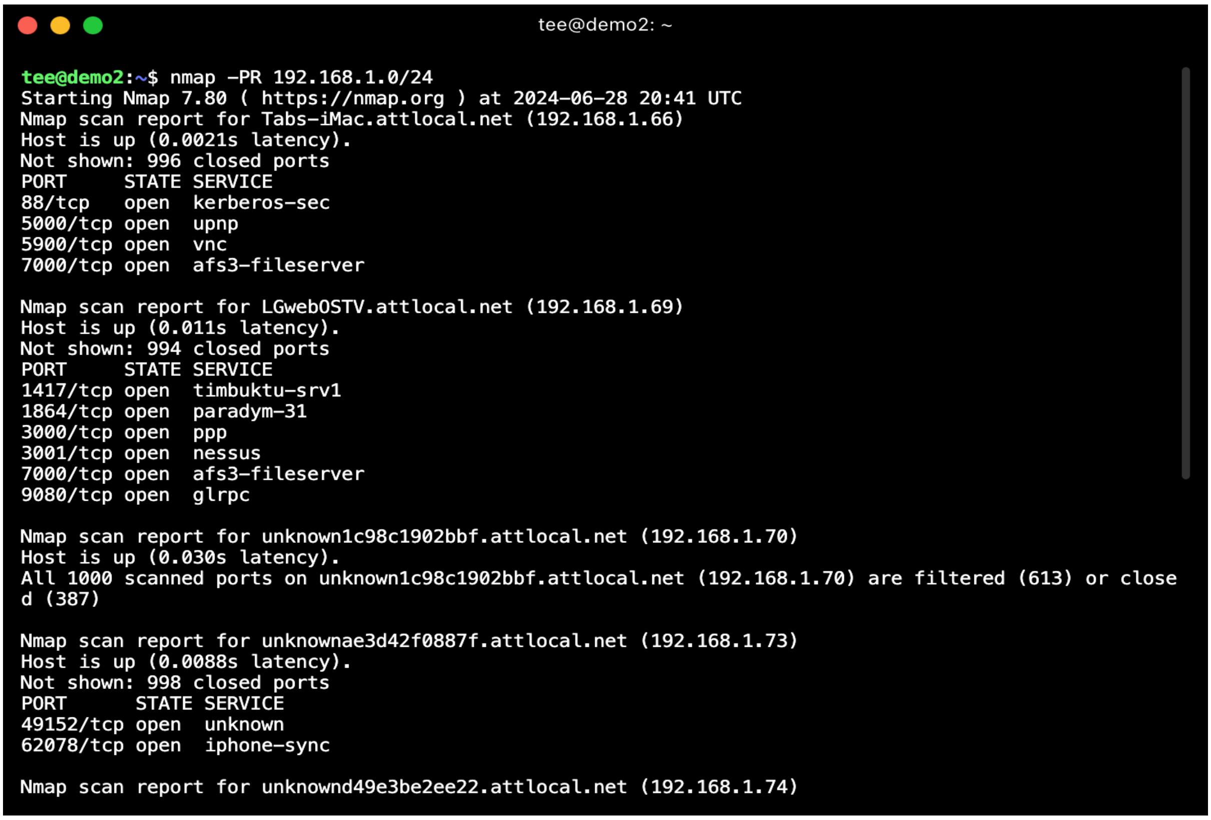
The fifth scan is the TCP scan. Here, nmap attempts to create a connection with the target host to determine if the ports are open. Use the following command: sudo nmap -sT <target IP address>. This is also illustrated below:



tee@demo2: ~

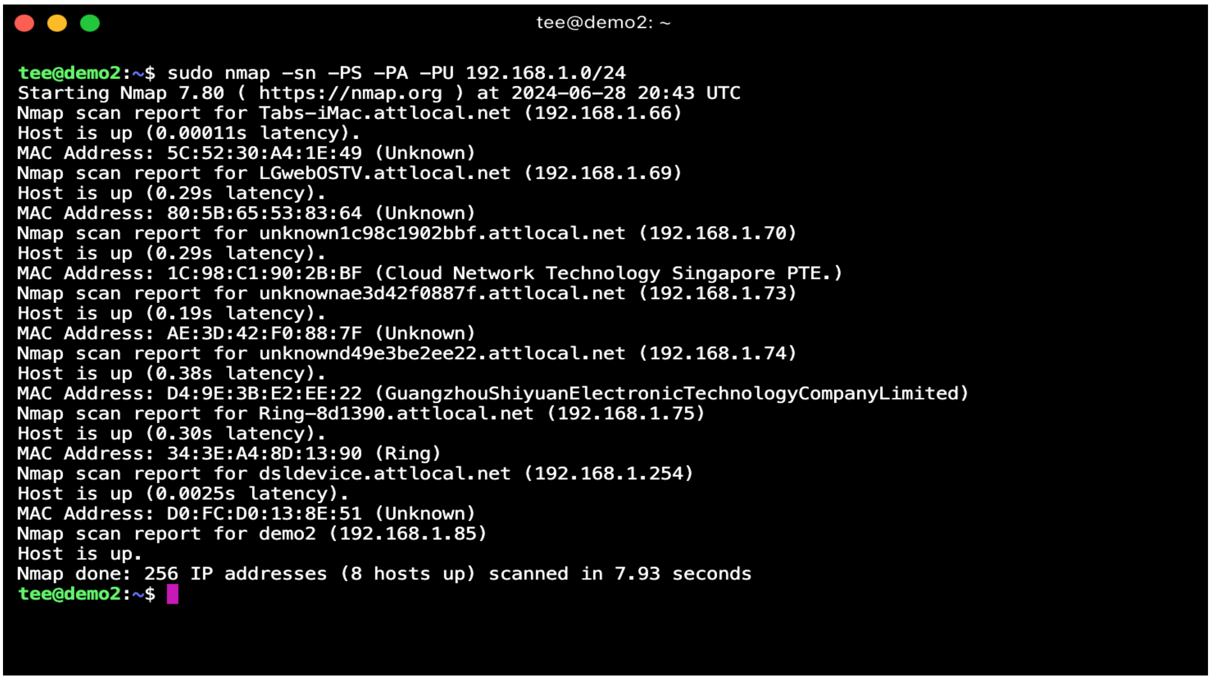
```
tee@demo2:~$ nmap -sT 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:40 UTC
Stats: 0:00:13 elapsed; 250 hosts completed (6 up), 6 undergoing Connect Scan
Connect Scan Timing: About 100.00% done; ETC: 20:40 (0:00:00 remaining)
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.0030s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
88/tcp   open  kerberos-sec
5000/tcp open  upnp
5900/tcp open  vnc
7000/tcp open  afs3-fileserver

Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.011s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
1417/tcp open  timbuktu-srv1
1864/tcp open  paradym-31
3000/tcp open  ppp
3001/tcp open  nessus
7000/tcp open  afs3-fileserver
9080/tcp open  glrpc

Nmap scan report for unknown1c98c1902bbf.attlocal.net (192.168.1.70)
Host is up (0.0062s latency).
All 1000 scanned ports on unknown1c98c1902bbf.attlocal.net (192.168.1.70) are closed

Nmap scan report for unknownd49e3be2ee22.attlocal.net (192.168.1.74)
Host is up (0.0062s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
```

The sixth scan is the ARP scan. This is used to discover hosts on a local network without having to go through the hassle of sending packets to each individual IP address. This can be accomplished using the nmap -PR <target IP address>. This is illustrated below:



```
tee@demo2:~$ nmap -PR 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:41 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.0021s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
88/tcp   open  kerberos-sec
5000/tcp open  upnp
5900/tcp open  vnc
7000/tcp open  afs3-fileserver

Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.011s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
1417/tcp open  timbuktu-srv1
1864/tcp open  paradym-31
3000/tcp open  ppp
3001/tcp open  nessus
7000/tcp open  afs3-fileserver
9080/tcp open  glrpc

Nmap scan report for unknown1c98c1902bbf.attlocal.net (192.168.1.70)
Host is up (0.030s latency).
All 1000 scanned ports on unknown1c98c1902bbf.attlocal.net (192.168.1.70) are filtered (613) or close
d (387)

Nmap scan report for unknownae3d42f0887f.attlocal.net (192.168.1.73)
Host is up (0.0088s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync

Nmap scan report for unknownd49e3be2ee22.attlocal.net (192.168.1.74)
```

The last scan is the host discovery scan. The purpose of this scan is to identify live hosts on the network. This scan combines a number of discovery techniques such as APR scanning, ICMP ping, and TCP ping. To accomplish the host discovery scan, use the following command: sudo nmap -sn -PS -PA -PU <target IP address>. This is illustrated below:



```
tee@demo2:~$ sudo nmap -sn -PS -PA -PU 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-28 20:43 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.00011s latency).
MAC Address: 5C:52:30:A4:1E:49 (Unknown)
Nmap scan report for LGwebOSTV.attlocal.net (192.168.1.69)
Host is up (0.29s latency).
MAC Address: 80:5B:65:53:83:64 (Unknown)
Nmap scan report for unknown1c98c1902bbf.attlocal.net (192.168.1.70)
Host is up (0.29s latency).
MAC Address: 1C:98:C1:90:2B:BF (Cloud Network Technology Singapore PTE.)
Nmap scan report for unknownae3d42f0887f.attlocal.net (192.168.1.73)
Host is up (0.19s latency).
MAC Address: AE:3D:42:F0:88:7F (Unknown)
Nmap scan report for unknownd49e3be2ee22.attlocal.net (192.168.1.74)
Host is up (0.38s latency).
MAC Address: D4:9E:3B:E2:EE:22 (GuangzhouShiyuanElectronicTechnologyCompanyLimited)
Nmap scan report for Ring-8d1390.attlocal.net (192.168.1.75)
Host is up (0.30s latency).
MAC Address: 34:3E:A4:8D:13:90 (Ring)
Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.0025s latency).
MAC Address: D0:FC:D0:13:8E:51 (Unknown)
Nmap scan report for demo2 (192.168.1.85)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 7.93 seconds
tee@demo2:~$
```

These are a few examples of how nmap scans can be used on a network.