Network Scanning & Port Analysis Report

Tool Used: Nmap
Scope: Local Network Scanning (Authorized Environment Only)
Objective: Identify live hosts, open ports, and high-risk exposed services.

Device 1: Network Router / Gateway (192.168.1.1)

The device at 192.168.1.1 was identified as the network gateway/router running a Linux-based operating system. Open services included SSH (22/tcp), DNS (53/tcp), HTTP (80/tcp), and UPnP (1900/tcp). These services provide administrative and network functionality but may introduce security risks if misconfigured.
Risk Level: Medium
Recommendation: Restrict administrative access and secure credentials.

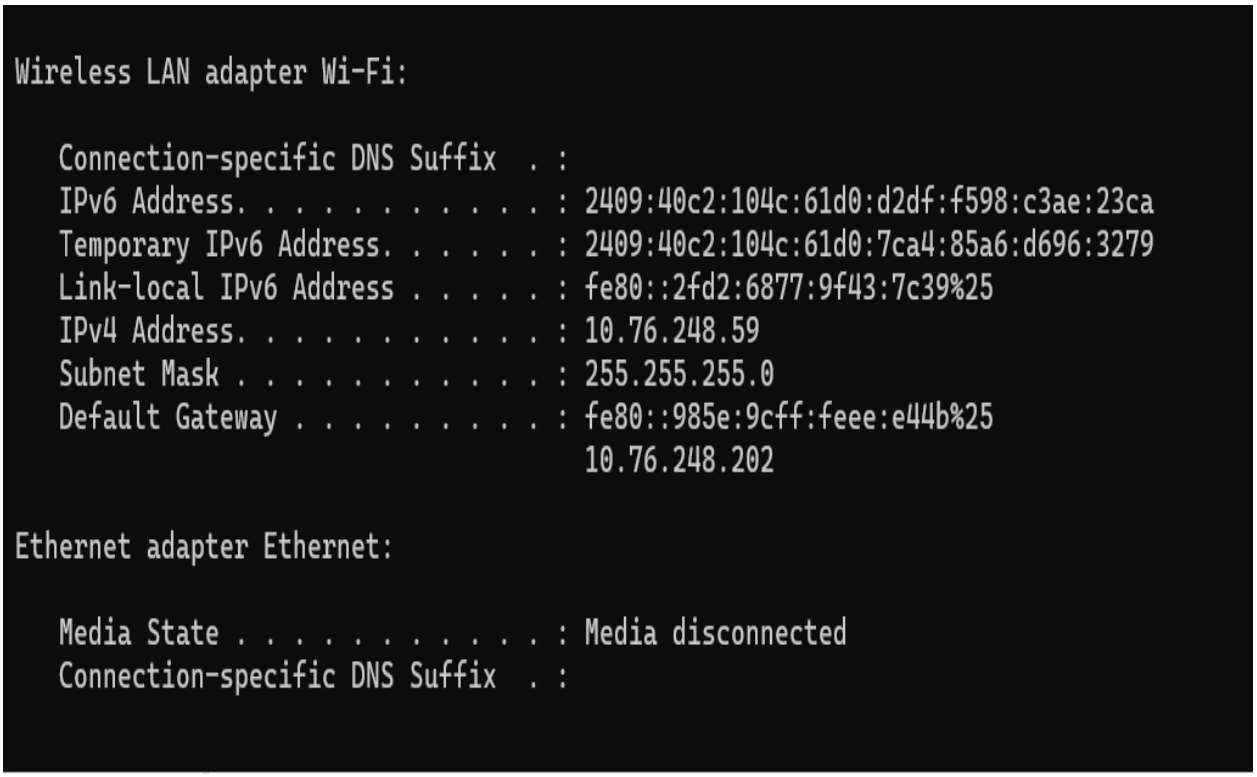
Device 2: Windows Host (192.168.1.104)

The host 192.168.1.104 was identified as a Windows-based system exposing MSRPC (135/tcp), NetBIOS (139/tcp), SMB (445/tcp), and VMware Authentication services (903/tcp). These services are common in Windows environments but are frequently targeted in lateral movement attacks.
Risk Level: Medium to High
Recommendation: Apply firewall restrictions and limit service exposure.

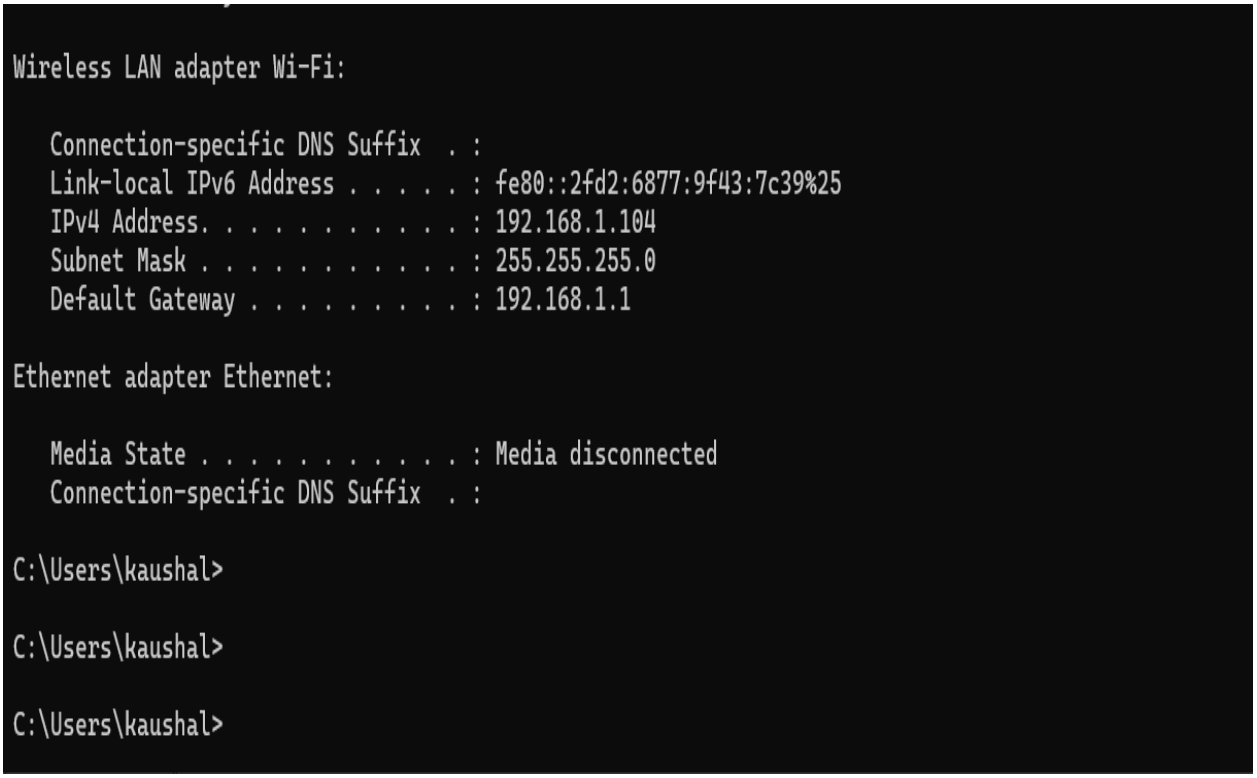
Device 3: Network Client / IoT Device (192.168.1.100)

The device at 192.168.1.100 did not expose any open TCP ports during scanning. All scanned ports were filtered or closed, indicating a minimal attack surface and proper network restrictions.
Risk Level: Low
Recommendation: Continue monitoring and maintain current security posture.

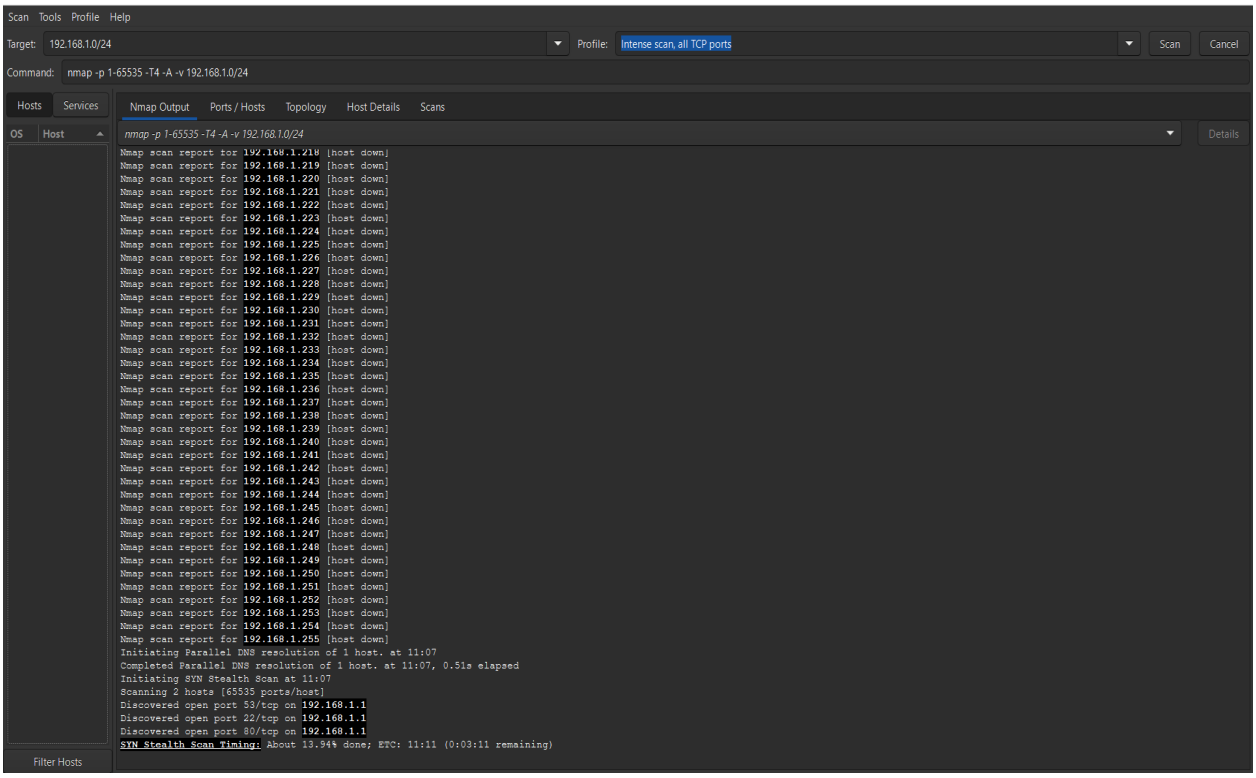
Scan Evidence & Screenshots

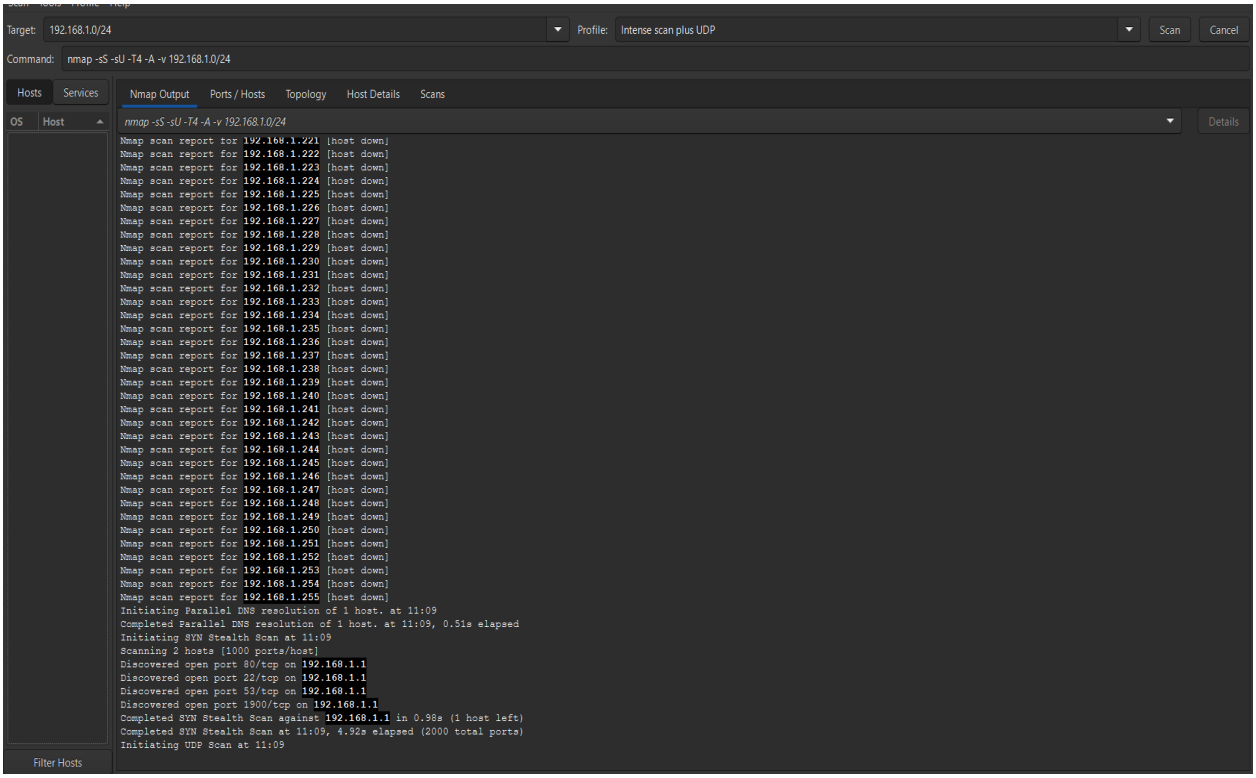


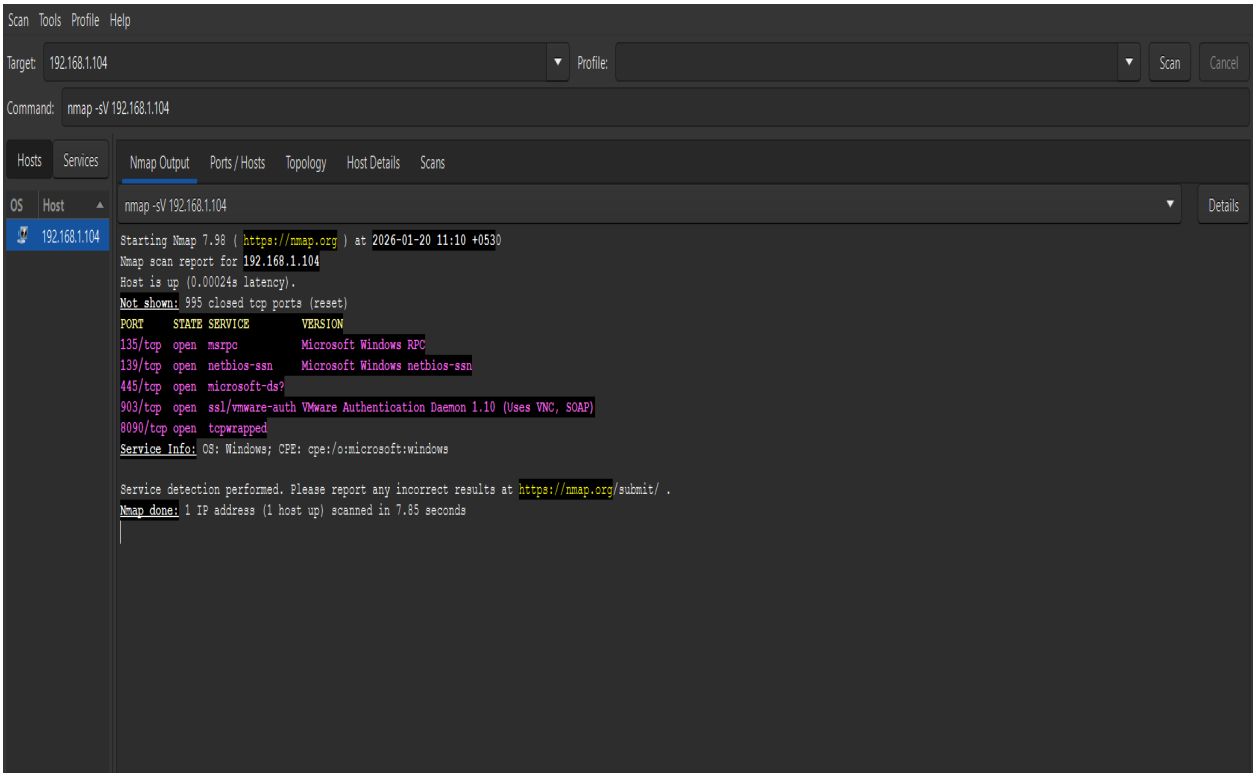
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c2:104c:61d0:d2df:f598:c3ae:23ca
   Temporary IPv6 Address. . . . . . : 2409:40c2:104c:61d0:7ca4:85a6:d696:3279
   Link-local IPv6 Address . . . . . : fe80::2fd2:6877:9f43:7c39%25
   IPv4 Address. . . . . . . . . . . : 10.76.248.59
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::985e:9cff:feee:e44b%25
                                       10.76.248.202

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

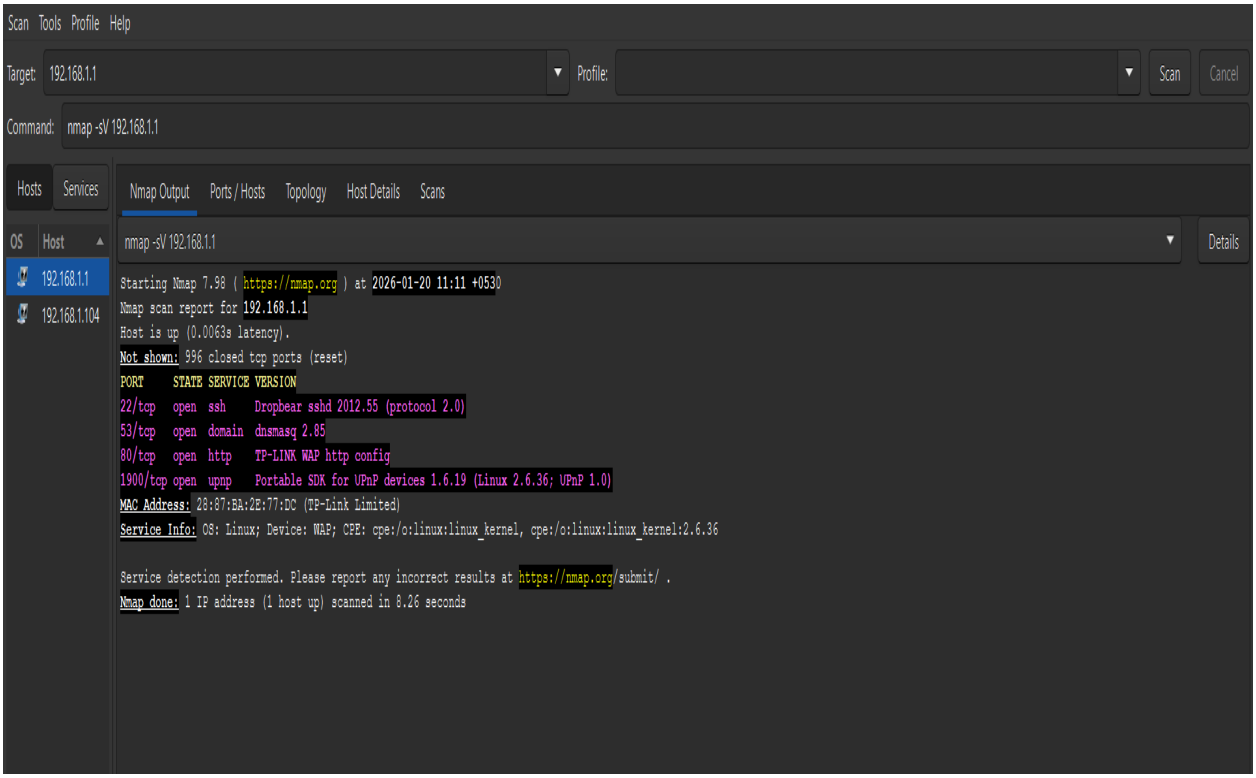


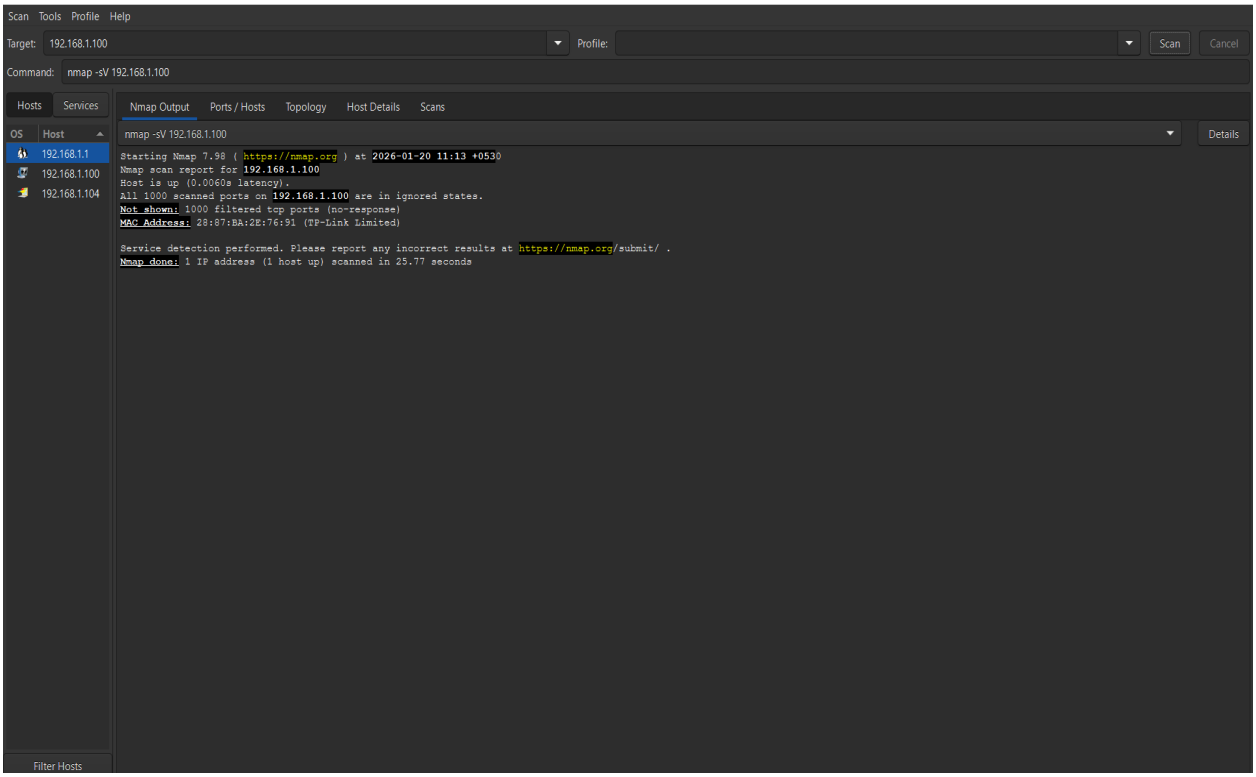
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2fd2:6877:9f43:7c39%25
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\kaushal>

C:\Users\kaushal>

C:\Users\kaushal>
```


Scan Tools Profile Help
Target: 192.168.1.0/24
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.1.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -p 1-65535 -T4 -A -v 192.168.1.0/24
Details
Nmap scan report for 192.168.1.218 [host down]
Nmap scan report for 192.168.1.219 [host down]
Nmap scan report for 192.168.1.220 [host down]
Nmap scan report for 192.168.1.221 [host down]
Nmap scan report for 192.168.1.222 [host down]
Nmap scan report for 192.168.1.223 [host down]
Nmap scan report for 192.168.1.224 [host down]
Nmap scan report for 192.168.1.225 [host down]
Nmap scan report for 192.168.1.226 [host down]
Nmap scan report for 192.168.1.227 [host down]
Nmap scan report for 192.168.1.228 [host down]
Nmap scan report for 192.168.1.229 [host down]
Nmap scan report for 192.168.1.230 [host down]
Nmap scan report for 192.168.1.231 [host down]
Nmap scan report for 192.168.1.232 [host down]
Nmap scan report for 192.168.1.233 [host down]
Nmap scan report for 192.168.1.234 [host down]
Nmap scan report for 192.168.1.235 [host down]
Nmap scan report for 192.168.1.236 [host down]
Nmap scan report for 192.168.1.237 [host down]
Nmap scan report for 192.168.1.238 [host down]
Nmap scan report for 192.168.1.239 [host down]
Nmap scan report for 192.168.1.240 [host down]
Nmap scan report for 192.168.1.241 [host down]
Nmap scan report for 192.168.1.242 [host down]
Nmap scan report for 192.168.1.243 [host down]
Nmap scan report for 192.168.1.244 [host down]
Nmap scan report for 192.168.1.245 [host down]
Nmap scan report for 192.168.1.246 [host down]
Nmap scan report for 192.168.1.247 [host down]
Nmap scan report for 192.168.1.248 [host down]
Nmap scan report for 192.168.1.249 [host down]
Nmap scan report for 192.168.1.250 [host down]
Nmap scan report for 192.168.1.251 [host down]
Nmap scan report for 192.168.1.252 [host down]
Nmap scan report for 192.168.1.253 [host down]
Nmap scan report for 192.168.1.254 [host down]
Nmap scan report for 192.168.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.51s elapsed
Initiating SYN Stealth Scan at 11:07
Scanning 2 hosts [65535 ports/host]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
SYN Stealth Scan Timing: About 13.94% done; ETC: 11:11 (0:03:11 remaining)
Filter Hosts


Target: 192.168.1.0/24
Profile: Intense scan plus UDP
Scan
Cancel
Command: nmap -sS -sU -T4 -A -v 192.168.1.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -sS -sU -T4 -A -v 192.168.1.0/24
Details
Nmap scan report for 192.168.1.221 [host down]
Nmap scan report for 192.168.1.222 [host down]
Nmap scan report for 192.168.1.223 [host down]
Nmap scan report for 192.168.1.224 [host down]
Nmap scan report for 192.168.1.225 [host down]
Nmap scan report for 192.168.1.226 [host down]
Nmap scan report for 192.168.1.227 [host down]
Nmap scan report for 192.168.1.228 [host down]
Nmap scan report for 192.168.1.229 [host down]
Nmap scan report for 192.168.1.230 [host down]
Nmap scan report for 192.168.1.231 [host down]
Nmap scan report for 192.168.1.232 [host down]
Nmap scan report for 192.168.1.233 [host down]
Nmap scan report for 192.168.1.234 [host down]
Nmap scan report for 192.168.1.235 [host down]
Nmap scan report for 192.168.1.236 [host down]
Nmap scan report for 192.168.1.237 [host down]
Nmap scan report for 192.168.1.238 [host down]
Nmap scan report for 192.168.1.239 [host down]
Nmap scan report for 192.168.1.240 [host down]
Nmap scan report for 192.168.1.241 [host down]
Nmap scan report for 192.168.1.242 [host down]
Nmap scan report for 192.168.1.243 [host down]
Nmap scan report for 192.168.1.244 [host down]
Nmap scan report for 192.168.1.245 [host down]
Nmap scan report for 192.168.1.246 [host down]
Nmap scan report for 192.168.1.247 [host down]
Nmap scan report for 192.168.1.248 [host down]
Nmap scan report for 192.168.1.249 [host down]
Nmap scan report for 192.168.1.250 [host down]
Nmap scan report for 192.168.1.251 [host down]
Nmap scan report for 192.168.1.252 [host down]
Nmap scan report for 192.168.1.253 [host down]
Nmap scan report for 192.168.1.254 [host down]
Nmap scan report for 192.168.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 11:09
Completed Parallel DNS resolution of 1 host. at 11:09, 0.51s elapsed
Initiating SYN Stealth Scan at 11:09
Scanning 2 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 1900/tcp on 192.168.1.1
Completed SYN Stealth Scan against 192.168.1.1 in 0.98s (1 host left)
Completed SYN Stealth Scan at 11:09, 4.92s elapsed (2000 total ports)
Initiating UDP Scan at 11:09
Filter Hosts


Scan Tools Profile Help
Target: 192.168.1.104
Profile:
Scan
Cancel
Command: nmap -sV 192.168.1.104
Hosts
Services
OS
Host
192.168.1.104
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV 192.168.1.104
Details
Starting Nmap 7.98 (https://nmap.org) at 2026-01-20 11:10 +0530
Nmap scan report for 192.168.1.104
Host is up (0.00024s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
903/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
8090/tcp open tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds


Scan Tools Profile Help
Target: 192.168.1.1
Profile:
Scan
Cancel
Command: nmap -sV 192.168.1.1
Hosts
Services
OS
Host
192.168.1.1
192.168.1.104
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV 192.168.1.1
Details
Starting Nmap 7.98 (https://nmap.org) at 2026-01-20 11:11 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh Dropbear sshd 2012.55 (protocol 2.0)
53/tcp open domain dnsmasq 2.85
80/tcp open http TP-LINK WAP http config
1900/tcp open upnp Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UPnP 1.0)
MAC Address: 28:87:BA:2E:77:DC (TP-Link Limited)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel, cpe:/o:linux:linux_kernel:2.6.36
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds


Scan Tools Profile Help
Target: 192.168.1.100
Profile:
Scan
Cancel
Command: nmap -sV 192.168.1.100
Hosts
Services
OS
Host
192.168.1.1
192.168.1.100
192.168.1.104
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV 192.168.1.100
Details
Starting Nmap 7.98 (https://nmap.org) at 2026-01-20 11:13 +0530
Nmap scan report for 192.168.1.100
Host is up (0.0060s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 28:87:BA:2E:76:91 (TP-Link Limited)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.77 seconds