```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-15 07:45 Central Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:45
Completed NSE at 07:45, 0.00s elapsed
Initiating NSE at 07:45
Completed NSE at 07:45, 0.00s elapsed
Initiating NSE at 07:45
Completed NSE at 07:45, 0.00s elapsed
Initiating ARP Ping Scan at 07:45
Scanning 254 hosts [1 port/host]
Completed ARP Ping Scan at 07:45, 19.17s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 07:45
Completed Parallel DNS resolution of 4 hosts. at 07:45, 5.53s elapsed
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18 [host down]
Nmap scan report for 192.168.1.19 [host down]
Nmap scan report for 192.168.1.20 [host down]
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23 [host down]
Nmap scan report for 192.168.1.24 [host down]
Nmap scan report for 192.168.1.25 [host down]
Nmap scan report for 192.168.1.26 [host down]
Nmap scan report for 192.168.1.27 [host down]
Nmap scan report for 192.168.1.28 [host down]
Nmap scan report for 192.168.1.29 [host down]
Nmap scan report for 192.168.1.30 [host down]
Nmap scan report for 192.168.1.31 [host down]
Nmap scan report for 192.168.1.32 [host down]
Nmap scan report for 192.168.1.33 [host down]
Nmap scan report for 192.168.1.34 [host down]
Nmap scan report for 192.168.1.35 [host down]
Nmap scan report for 192.168.1.36 [host down]
Nmap scan report for 192.168.1.37 [host down]
Nmap scan report for 192.168.1.38 [host down]
Nmap scan report for 192.168.1.39 [host down]
Nmap scan report for 192.168.1.40 [host down]
Nmap scan report for 192.168.1.41 [host down]
Nmap scan report for 192.168.1.42 [host down]
Nmap scan report for 192.168.1.43 [host down]
Nmap scan report for 192.168.1.44 [host down]
Nmap scan report for 192.168.1.45 [host down]
Nmap scan report for 192.168.1.46 [host down]
Nmap scan report for 192.168.1.47 [host down]
Nmap scan report for 192.168.1.48 [host down]
Nmap scan report for 192.168.1.49 [host down]
Nmap scan report for 192.168.1.50 [host down]
Nmap scan report for 192.168.1.51 [host down]
Nmap scan report for 192.168.1.52 [host down]
Nmap scan report for 192.168.1.53 [host down]
Nmap scan report for 192.168.1.54 [host down]
Nmap scan report for 192.168.1.55 [host down]
Nmap scan report for 192.168.1.56 [host down]
Nmap scan report for 192.168.1.57 [host down]
Nmap scan report for 192.168.1.58 [host down]
Nmap scan report for 192.168.1.59 [host down]
Nmap scan report for 192.168.1.60 [host down]
Nmap scan report for 192.168.1.61 [host down]
Nmap scan report for 192.168.1.62 [host down]
Nmap scan report for 192.168.1.63 [host down]
Nmap scan report for 192.168.1.64 [host down]
Nmap scan report for 192.168.1.65 [host down]
Nmap scan report for 192.168.1.66 [host down]
Nmap scan report for 192.168.1.67 [host down]
Nmap scan report for 192.168.1.68 [host down]
Nmap scan report for 192.168.1.69 [host down]
Nmap scan report for 192.168.1.70 [host down]
Nmap scan report for 192.168.1.71 [host down]
Nmap scan report for 192.168.1.72 [host down]
Nmap scan report for 192.168.1.73 [host down]
Nmap scan report for 192.168.1.74 [host down]
Nmap scan report for 192.168.1.75 [host down]
Nmap scan report for 192.168.1.76 [host down]
Nmap scan report for 192.168.1.77 [host down]
Nmap scan report for 192.168.1.78 [host down]
Nmap scan report for 192.168.1.79 [host down]
Nmap scan report for 192.168.1.80 [host down]
Nmap scan report for 192.168.1.81 [host down]
Nmap scan report for 192.168.1.82 [host down]
Nmap scan report for 192.168.1.83 [host down]
Nmap scan report for 192.168.1.84 [host down]
Nmap scan report for 192.168.1.85 [host down]
Nmap scan report for 192.168.1.86 [host down]
Nmap scan report for 192.168.1.87 [host down]
Nmap scan report for 192.168.1.88 [host down]
Nmap scan report for 192.168.1.89 [host down]
Nmap scan report for 192.168.1.90 [host down]
Nmap scan report for 192.168.1.91 [host down]
Nmap scan report for 192.168.1.92 [host down]
Nmap scan report for 192.168.1.93 [host down]
Nmap scan report for 192.168.1.94 [host down]
Nmap scan report for 192.168.1.95 [host down]
Nmap scan report for 192.168.1.96 [host down]
Nmap scan report for 192.168.1.97 [host down]
Nmap scan report for 192.168.1.98 [host down]
Nmap scan report for 192.168.1.99 [host down]
Nmap scan report for 192.168.1.100 [host down]
Nmap scan report for 192.168.1.101 [host down]
Nmap scan report for 192.168.1.102 [host down]
Nmap scan report for 192.168.1.103 [host down]
Nmap scan report for 192.168.1.104 [host down]
Nmap scan report for 192.168.1.105 [host down]
Nmap scan report for 192.168.1.106 [host down]
Nmap scan report for 192.168.1.107 [host down]
Nmap scan report for 192.168.1.108 [host down]
Nmap scan report for 192.168.1.109 [host down]
Nmap scan report for 192.168.1.110 [host down]
Nmap scan report for 192.168.1.111 [host down]
Nmap scan report for 192.168.1.112 [host down]
Nmap scan report for 192.168.1.113 [host down]
Nmap scan report for 192.168.1.114 [host down]
Nmap scan report for 192.168.1.115 [host down]
Nmap scan report for 192.168.1.116 [host down]
Nmap scan report for 192.168.1.117 [host down]
Nmap scan report for 192.168.1.118 [host down]
Nmap scan report for 192.168.1.119 [host down]
Nmap scan report for 192.168.1.120 [host down]
Nmap scan report for 192.168.1.121 [host down]
Nmap scan report for 192.168.1.122 [host down]
Nmap scan report for 192.168.1.123 [host down]
Nmap scan report for 192.168.1.124 [host down]
Nmap scan report for 192.168.1.125 [host down]
Nmap scan report for 192.168.1.126 [host down]
Nmap scan report for 192.168.1.127 [host down]
Nmap scan report for 192.168.1.128 [host down]
Nmap scan report for 192.168.1.130 [host down]
Nmap scan report for 192.168.1.131 [host down]
Nmap scan report for 192.168.1.132 [host down]
Nmap scan report for 192.168.1.133 [host down]
Nmap scan report for 192.168.1.134 [host down]
Nmap scan report for 192.168.1.135 [host down]
Nmap scan report for 192.168.1.136 [host down]
Nmap scan report for 192.168.1.137 [host down]
Nmap scan report for 192.168.1.138 [host down]
Nmap scan report for 192.168.1.139 [host down]
Nmap scan report for 192.168.1.140 [host down]
Nmap scan report for 192.168.1.141 [host down]
Nmap scan report for 192.168.1.142 [host down]
Nmap scan report for 192.168.1.143 [host down]
Nmap scan report for 192.168.1.144 [host down]
Nmap scan report for 192.168.1.145 [host down]
Nmap scan report for 192.168.1.146 [host down]
Nmap scan report for 192.168.1.147 [host down]
Nmap scan report for 192.168.1.148 [host down]
Nmap scan report for 192.168.1.149 [host down]
Nmap scan report for 192.168.1.150 [host down]
Nmap scan report for 192.168.1.151 [host down]
Nmap scan report for 192.168.1.152 [host down]
Nmap scan report for 192.168.1.153 [host down]
Nmap scan report for 192.168.1.154 [host down]
Nmap scan report for 192.168.1.155 [host down]
Nmap scan report for 192.168.1.156 [host down]
Nmap scan report for 192.168.1.157 [host down]
Nmap scan report for 192.168.1.158 [host down]
Nmap scan report for 192.168.1.159 [host down]
Nmap scan report for 192.168.1.160 [host down]
Nmap scan report for 192.168.1.161 [host down]
Nmap scan report for 192.168.1.162 [host down]
Nmap scan report for 192.168.1.163 [host down]
Nmap scan report for 192.168.1.164 [host down]
Nmap scan report for 192.168.1.165 [host down]
Nmap scan report for 192.168.1.166 [host down]
Nmap scan report for 192.168.1.167 [host down]
Nmap scan report for 192.168.1.168 [host down]
Nmap scan report for 192.168.1.169 [host down]
Nmap scan report for 192.168.1.170 [host down]
Nmap scan report for 192.168.1.171 [host down]
Nmap scan report for 192.168.1.172 [host down]
Nmap scan report for 192.168.1.173 [host down]
Nmap scan report for 192.168.1.174 [host down]
Nmap scan report for 192.168.1.175 [host down]
Nmap scan report for 192.168.1.176 [host down]
Nmap scan report for 192.168.1.177 [host down]
Nmap scan report for 192.168.1.178 [host down]
Nmap scan report for 192.168.1.179 [host down]
Nmap scan report for 192.168.1.180 [host down]
Nmap scan report for 192.168.1.181 [host down]
Nmap scan report for 192.168.1.182 [host down]
Nmap scan report for 192.168.1.183 [host down]
Nmap scan report for 192.168.1.184 [host down]
Nmap scan report for 192.168.1.185 [host down]
Nmap scan report for 192.168.1.186 [host down]
Nmap scan report for 192.168.1.188 [host down]
Nmap scan report for 192.168.1.189 [host down]
Nmap scan report for 192.168.1.190 [host down]
Nmap scan report for 192.168.1.191 [host down]
Nmap scan report for 192.168.1.192 [host down]
Nmap scan report for 192.168.1.193 [host down]
Nmap scan report for 192.168.1.194 [host down]
Nmap scan report for 192.168.1.195 [host down]
Nmap scan report for 192.168.1.196 [host down]
Nmap scan report for 192.168.1.197 [host down]
Nmap scan report for 192.168.1.198 [host down]
Nmap scan report for 192.168.1.199 [host down]
Nmap scan report for 192.168.1.200 [host down]
Nmap scan report for 192.168.1.201 [host down]
Nmap scan report for 192.168.1.202 [host down]
Nmap scan report for 192.168.1.203 [host down]
Nmap scan report for 192.168.1.204 [host down]
Nmap scan report for 192.168.1.205 [host down]
Nmap scan report for 192.168.1.206 [host down]
Nmap scan report for 192.168.1.207 [host down]
Nmap scan report for 192.168.1.208 [host down]
Nmap scan report for 192.168.1.209 [host down]
Nmap scan report for 192.168.1.211 [host down]
Nmap scan report for 192.168.1.212 [host down]
Nmap scan report for 192.168.1.213 [host down]
Nmap scan report for 192.168.1.214 [host down]
Nmap scan report for 192.168.1.215 [host down]
Nmap scan report for 192.168.1.216 [host down]
Nmap scan report for 192.168.1.217 [host down]
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 07:45
```

```
Completed Parallel DNS resolution of 1 host. at 07:45, 0.01s elapsed
Initiating SYN Stealth Scan at 07:45
Scanning 4 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.187
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.187
Discovered open port 631/tcp on 192.168.1.187
Discovered open port 9080/tcp on 192.168.1.210
Discovered open port 7000/tcp on 192.168.1.210
Completed SYN Stealth Scan against 192.168.1.210 in 0.58s (3 hosts left)
Discovered open port 49152/tcp on 192.168.1.1
Discovered open port 49153/tcp on 192.168.1.1
Discovered open port 49154/tcp on 192.168.1.1
Discovered open port 8000/tcp on 192.168.1.1
Discovered open port 9100/tcp on 192.168.1.187
Discovered open port 515/tcp on 192.168.1.187
Completed SYN Stealth Scan against 192.168.1.187 in 2.41s (2 hosts left)
Completed SYN Stealth Scan against 192.168.1.1 in 2.69s (1 host left)
Increasing send delay for 192.168.1.129 from 0 to 5 due to 47 out of 117 dropped pr
Increasing send delay for 192.168.1.129 from 5 to 10 due to 11 out of 17 dropped pr
Completed SYN Stealth Scan at 07:45, 21.20s elapsed (4000 total ports)
Initiating Service scan at 07:45
Scanning 13 services on 4 hosts
Completed Service scan at 07:48, 156.42s elapsed (14 services on 4 hosts)
Initiating OS detection (try #1) against 4 hosts
Retrying OS detection (try #2) against 2 hosts
WARNING: RST from 192.168.1.187 port 80 -- is this port really open?
Retrying OS detection (try #3) against BRW5C61999450D8 (192.168.1.187)
Retrying OS detection (try #4) against BRW5C61999450D8 (192.168.1.187)
Retrying OS detection (try #5) against BRW5C61999450D8 (192.168.1.187)
NSE: Script scanning 4 hosts.
Initiating NSE at 07:48
Completed NSE at 07:49, 18.27s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 1.55s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 0.00s elapsed
Nmap scan report for Docsis-Gateway (192.168.1.1)
Host is up (0.0035s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open     tcpwrapped
| dns-nsid:
|_  bind.version: dnsmasq-2.83
80/tcp    open     http
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 302 Found
|     Date:
```

```
|     Server:
|     Location:https://account.suddenlink.net/router-portal/login.html
|     Connection: close
|_    Content-Type: text/html
|_http-server-header: <empty>
|_http-title: Did not follow redirect to https://account.suddenlink.net/router-port
| http-methods:
|_  Supported Methods: GET
443/tcp   open     ssl/http   micro_httpd
| ssl-cert: Subject: commonName=example.com/organizationName=Dis/stateOrProvinceNam
| Issuer: commonName=example.com/organizationName=Dis/stateOrProvinceName=Denial/co
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-04T17:25:19
| Not valid after:  2122-07-11T17:25:19
| MD5:   0644:75f4:6305:aaab:4fc7:746d:9f1a:78fa
|_SHA-1: 4017:1f86:1157:cc6f:87a7:ccb4:a3ec:9232:2059:ef77
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
| http-methods:
|_  Supported Methods: GET POST
8000/tcp  open     http-alt
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 302 Found
|     Date:
|     Server:
|     Location:https://account.suddenlink.net/router-portal/login.html
|     Connection: close
|_    Content-Type: text/html
|_http-title: Did not follow redirect to https://account.suddenlink.net/router-port
|_http-server-header: <empty>
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Supported Methods: GET
9000/tcp  filtered cslistener
49152/tcp open     upnp       Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
49153/tcp open     upnp       Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
49154/tcp open     upnp       Portable SDK for UPnP devices 1.6.22 (Linux 4.9.248-p
2 services unrecognized despite returning data. If you know the service/version, pl
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94%I=7%D=7/15%Time=64B29506%P=i686-pc-windows-windows%r(
SF:GetRequest,93,"HTTP/1\.1\x20302\x20Found\r\nDate:\r\nServer:\r\nLocatio
SF:n:https://account\.suddenlink\.net/router-portal/login\.html\r\nConnect
SF:ion:\x20close\r\nContent-Type:\x20text/html\r\n\n")%r(FourOhFourRequest
SF:,93,"HTTP/1\.1\x20302\x20Found\r\nDate:\r\nServer:\r\nLocation:https://
SF:account\.suddenlink\.net/router-portal/login\.html\r\nConnection:\x20cl
SF:ose\r\nContent-Type:\x20text/html\r\n\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8000-TCP:V=7.94%I=7%D=7/15%Time=64B29506%P=i686-pc-windows-windows%
SF:r(GetRequest,93,"HTTP/1\.1\x20302\x20Found\r\nDate:\r\nServer:\r\nLocat
SF:ion:https://account\.suddenlink\.net/router-portal/login\.html\r\nConne
SF:ction:\x20close\r\nContent-Type:\x20text/html\r\n\n")%r(FourOhFourReque
SF:st,93,"HTTP/1\.1\x20302\x20Found\r\nDate:\r\nServer:\r\nLocation:https:
SF://account\.suddenlink\.net/router-portal/login\.html\r\nConnection:\x20
SF:close\r\nContent-Type:\x20text/html\r\n\n");
MAC Address: 5C:53:C3:89:D5:23 (Ubee Interactive, Limited)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 37.529 days (since Wed Jun  7 19:06:56 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/h:cisco:e4200, cpe:/o:linux:linux_kernel:4.9.248

TRACEROUTE
HOP RTT     ADDRESS
1   3.52 ms Docsis-Gateway (192.168.1.1)

Nmap scan report for Galaxy-Tab-A7-Lite (192.168.1.129)
Host is up (0.038s latency).
All 1000 scanned ports on Galaxy-Tab-A7-Lite (192.168.1.129) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 2A:BA:23:F5:D8:B0 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   38.46 ms Galaxy-Tab-A7-Lite (192.168.1.129)

Nmap scan report for BRW5C61999450D8 (192.168.1.187)
Host is up (0.0069s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Debut embedded httpd 1.30 (Brother/HP printer http admin)
|_http-server-header: debut/1.30
| http-title: Brother MFC-L2730DW series
|_Requested resource was /general/status.html
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
443/tcp  open  ssl/http   Debut embedded httpd 1.30 (Brother/HP printer http admin)
| ssl-cert: Subject: commonName=BRW5C61999450D8.local
| Issuer: commonName=BRW5C61999450D8.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2000-01-01T00:00:00
| Not valid after:  2110-12-31T23:59:59
| MD5:   4745:7f8f:4788:de8d:de04:bc7f:ab0d:7ac3
|_SHA-1: d787:73c1:5ef8:914d:e77d:3665:0856:bf7b:2eb6:166d
|_ssl-date: TLS randomness does not represent time
|_http-server-header: debut/1.30
| http-methods:
|_  Supported Methods: POST OPTIONS
515/tcp  open  printer
631/tcp  open  http       Debut embedded httpd 1.30 (Brother/HP printer http admin)
|_http-server-header: debut/1.30
| http-robots.txt: 1 disallowed entry
|_/
| http-title: Brother MFC-L2730DW series
|_Requested resource was /general/status.html
| http-methods:
|_  Supported Methods: POST HEAD OPTIONS
9100/tcp open  jetdirect?
MAC Address: 5C:61:99:94:50:D8 (Cloud Network Technology Singapore PTE.)
No exact OS matches for host (If you know what OS is running on it, see https://nma
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/15%OT=80%CT=1%CU=36290%PV=Y%DS=1%DC=D%G=Y%M=5C6199%T
OS:M=64B295BD%P=i686-pc-windows-windows)SEQ()SEQ(SP=102%GCD=1%ISR=108%TS=A)
OS:SEQ(SP=103%GCD=1%ISR=108%TI=RI%TS=A)SEQ(SP=103%GCD=1%ISR=108%TI=RI%CI=I%
OS:TS=A)SEQ(SP=104%GCD=1%ISR=10E%TI=I%CI=I%II=I%TS=A)OPS(O1=M5B4NW0NNT11%O2
OS:=%O3=%O4=%O5=%O6=)OPS(O1=M5B4NW0NNT11%O2=M578NW0NNSNNT11%O3=M280NW0NNT11
OS:%O4=M5B4NW0NNSNNT11%O5=M218NW0NNSNNT11%O6=M109NNSNNT11)OPS(O1=NNT11%O2=N
OS:NT11%O3=NNT11%O4=NNT11%O5=NNT11%O6=NNT11)WIN(W1=21F0%W2=0%W3=0%W4=0%W5=0
OS:%W6=0)WIN(W1=21F0%W2=2088%W3=2258%W4=21F0%W5=20C0%W6=209D)ECN(R=Y%DF=N%T
OS:=40%W=2238%O=%CC=N%Q=)ECN(R=Y%DF=N%T=40%W=2238%O=M5B4NW0NNS%CC=N%Q=)T1(R
OS:=Y%DF=N%T=40%S=O%A=O%F=A%RD=0%Q=)T1(R=Y%DF=N%T=40%S=O%A=O%F=AS%RD=0%Q=)T
OS:1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T1(R=Y%DF=N%T=40%S=O%A=Z%F=R%RD=0%
OS:Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N
OS:%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IP
OS:L=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=S)

Uptime guess: 5.861 days (since Sun Jul  9 11:08:54 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Random positive increments
Service Info: Device: printer

TRACEROUTE
HOP RTT     ADDRESS
1   6.90 ms BRW5C61999450D8 (192.168.1.187)

Nmap scan report for RokuPremiere (192.168.1.210)
Host is up (0.0073s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
7000/tcp open  rtsp    AirTunes rtspd 377.40.00
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
|_irc-info: Unable to open connection
```

```
9080/tcp open  glrpc?
MAC Address: CC:6D:A0:FB:E1:34 (Roku)
Device type: phone
Running: Google Android 5.X
OS CPE: cpe:/o:google:android:5.1.1
OS details: Android 5.1.1
Uptime guess: 13.477 days (since Sat Jul  1 20:22:12 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   7.28 ms RokuPremiere (192.168.1.210)

Initiating SYN Stealth Scan at 07:49
Scanning DESKTOP-3SHPIF1 (192.168.1.15) [1000 ports]
Discovered open port 445/tcp on 192.168.1.15
Discovered open port 135/tcp on 192.168.1.15
Discovered open port 139/tcp on 192.168.1.15
Completed SYN Stealth Scan at 07:49, 0.14s elapsed (1000 total ports)
Initiating Service scan at 07:49
Scanning 3 services on DESKTOP-3SHPIF1 (192.168.1.15)
Completed Service scan at 07:49, 6.04s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against DESKTOP-3SHPIF1 (192.168.1.15)
Retrying OS detection (try #2) against DESKTOP-3SHPIF1 (192.168.1.15)
NSE: Script scanning 192.168.1.15.
Initiating NSE at 07:49
Completed NSE at 07:49, 24.29s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 0.01s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 0.00s elapsed
Nmap scan report for DESKTOP-3SHPIF1 (192.168.1.15)
Host is up (0.00055s latency).
Not shown: 997 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?
Aggressive OS guesses: Microsoft Windows 10 1607 (98%), Microsoft Windows 11 21H2
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.293 days (since Wed Jul 12 00:47:54 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1s
| smb2-time: 
|   date: 2023-07-15T12:49:12
|_  start_date: N/A
```

```
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 07:49
Completed NSE at 07:49, 0.00s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 0.00s elapsed
Initiating NSE at 07:49
Completed NSE at 07:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://
Nmap done: 255 IP addresses (5 hosts up) scanned in 270.01 seconds
           Raw packets sent: 6054 (270.778KB) | Rcvd: 6356 (268.350KB)
```