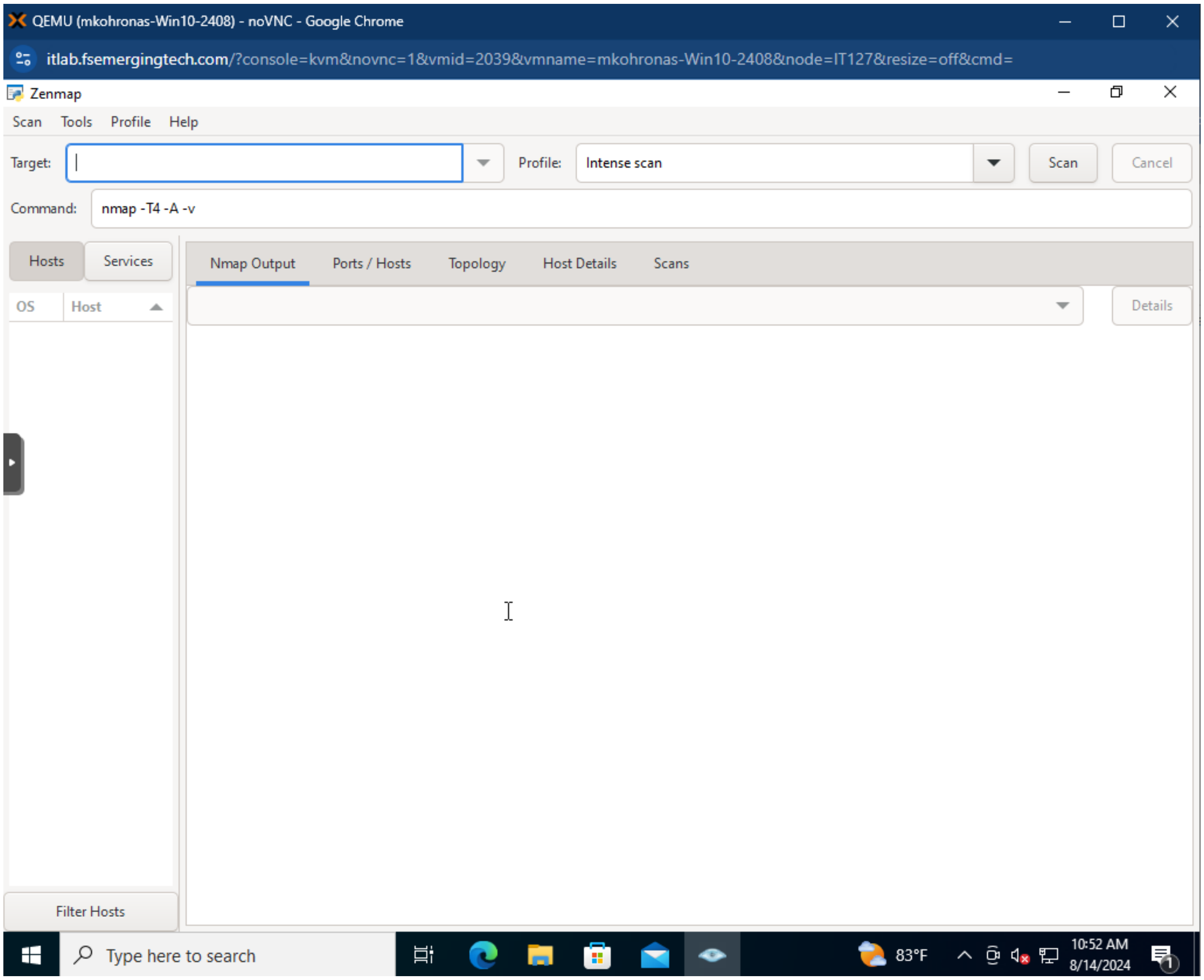
Task 1:



Target:

Profile: Intense scan

Command: nmap -T4 -A -v

Task 2:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 07:58 Pacific Daylight Time

Nmap scan report for OPNsense.localdomain (172.16.1.1)

Host is up (0.0029s latency).

MAC Address: BC:24:11:0F:90:00 (Unknown)

Nmap scan report for 172.16.1.114

Host is up (0.0012s latency).

MAC Address: BC:24:11:F8:E0:0F (Unknown)

Nmap scan report for 172.16.1.115

Host is up (0.0020s latency).

MAC Address: BC:24:11:50:3B:0E (Unknown)

Nmap scan report for 172.16.1.13

Host is up.

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.19 seconds
```

Task 3:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 08:08 Pacific Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating ARP Ping Scan at 08:08
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 08:08, 1.90s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 08:08
Completed Parallel DNS resolution of 3 hosts. at 08:08, 0.00s elapsed
Nmap scan report for 172.16.1.0 [host down]
Nmap scan report for 172.16.1.2 [host down]
Nmap scan report for 172.16.1.3 [host down]
Nmap scan report for 172.16.1.4 [host down]
Nmap scan report for 172.16.1.5 [host down]
Nmap scan report for 172.16.1.6 [host down]
Nmap scan report for 172.16.1.7 [host down]
Nmap scan report for 172.16.1.8 [host down]
Nmap scan report for 172.16.1.9 [host down]
Nmap scan report for 172.16.1.10 [host down]
Nmap scan report for 172.16.1.11 [host down]
Nmap scan report for 172.16.1.12 [host down]
Nmap scan report for 172.16.1.14 [host down]
Nmap scan report for 172.16.1.15 [host down]

Nmap scan report for 172.16.1.16 [host down]

Nmap scan report for 172.16.1.17 [host down]

Nmap scan report for 172.16.1.18 [host down]

Nmap scan report for 172.16.1.19 [host down]

Nmap scan report for 172.16.1.20 [host down]

Nmap scan report for 172.16.1.21 [host down]

Nmap scan report for 172.16.1.22 [host down]

Nmap scan report for 172.16.1.23 [host down]

Nmap scan report for 172.16.1.24 [host down]

Nmap scan report for 172.16.1.25 [host down]

Nmap scan report for 172.16.1.26 [host down]

Nmap scan report for 172.16.1.27 [host down]

Nmap scan report for 172.16.1.28 [host down]

Nmap scan report for 172.16.1.29 [host down]

Nmap scan report for 172.16.1.30 [host down]

Nmap scan report for 172.16.1.31 [host down]

Nmap scan report for 172.16.1.32 [host down]

Nmap scan report for 172.16.1.33 [host down]

Nmap scan report for 172.16.1.34 [host down]

Nmap scan report for 172.16.1.35 [host down]

Nmap scan report for 172.16.1.36 [host down]

Nmap scan report for 172.16.1.37 [host down]

Nmap scan report for 172.16.1.38 [host down]

Nmap scan report for 172.16.1.39 [host down]

Nmap scan report for 172.16.1.40 [host down]

Nmap scan report for 172.16.1.41 [host down]

Nmap scan report for 172.16.1.42 [host down]

Nmap scan report for 172.16.1.43 [host down]
Nmap scan report for 172.16.1.44 [host down]
Nmap scan report for 172.16.1.45 [host down]
Nmap scan report for 172.16.1.46 [host down]
Nmap scan report for 172.16.1.47 [host down]
Nmap scan report for 172.16.1.48 [host down]
Nmap scan report for 172.16.1.49 [host down]
Nmap scan report for 172.16.1.50 [host down]
Nmap scan report for 172.16.1.51 [host down]
Nmap scan report for 172.16.1.52 [host down]
Nmap scan report for 172.16.1.53 [host down]
Nmap scan report for 172.16.1.54 [host down]
Nmap scan report for 172.16.1.55 [host down]
Nmap scan report for 172.16.1.56 [host down]
Nmap scan report for 172.16.1.57 [host down]
Nmap scan report for 172.16.1.58 [host down]
Nmap scan report for 172.16.1.59 [host down]
Nmap scan report for 172.16.1.60 [host down]
Nmap scan report for 172.16.1.61 [host down]
Nmap scan report for 172.16.1.62 [host down]
Nmap scan report for 172.16.1.63 [host down]
Nmap scan report for 172.16.1.64 [host down]
Nmap scan report for 172.16.1.65 [host down]
Nmap scan report for 172.16.1.66 [host down]
Nmap scan report for 172.16.1.67 [host down]
Nmap scan report for 172.16.1.68 [host down]
Nmap scan report for 172.16.1.69 [host down]
Nmap scan report for 172.16.1.70 [host down]
Nmap scan report for 172.16.1.71 [host down]
Nmap scan report for 172.16.1.72 [host down]
Nmap scan report for 172.16.1.73 [host down]
Nmap scan report for 172.16.1.74 [host down]
Nmap scan report for 172.16.1.75 [host down]
Nmap scan report for 172.16.1.76 [host down]
Nmap scan report for 172.16.1.77 [host down]
Nmap scan report for 172.16.1.78 [host down]
Nmap scan report for 172.16.1.79 [host down]
Nmap scan report for 172.16.1.80 [host down]
Nmap scan report for 172.16.1.81 [host down]
Nmap scan report for 172.16.1.82 [host down]
Nmap scan report for 172.16.1.83 [host down]
Nmap scan report for 172.16.1.84 [host down]
Nmap scan report for 172.16.1.85 [host down]
Nmap scan report for 172.16.1.86 [host down]
Nmap scan report for 172.16.1.87 [host down]
Nmap scan report for 172.16.1.88 [host down]
Nmap scan report for 172.16.1.89 [host down]
Nmap scan report for 172.16.1.90 [host down]
Nmap scan report for 172.16.1.91 [host down]
Nmap scan report for 172.16.1.92 [host down]
Nmap scan report for 172.16.1.93 [host down]
Nmap scan report for 172.16.1.94 [host down]
Nmap scan report for 172.16.1.95 [host down]
Nmap scan report for 172.16.1.96 [host down]
Nmap scan report for 172.16.1.97 [host down]
Nmap scan report for 172.16.1.98 [host down]
Nmap scan report for 172.16.1.99 [host down]
Nmap scan report for 172.16.1.100 [host down]
Nmap scan report for 172.16.1.101 [host down]
Nmap scan report for 172.16.1.102 [host down]
Nmap scan report for 172.16.1.103 [host down]
Nmap scan report for 172.16.1.104 [host down]
Nmap scan report for 172.16.1.105 [host down]
Nmap scan report for 172.16.1.106 [host down]
Nmap scan report for 172.16.1.107 [host down]
Nmap scan report for 172.16.1.108 [host down]
Nmap scan report for 172.16.1.109 [host down]
Nmap scan report for 172.16.1.110 [host down]
Nmap scan report for 172.16.1.111 [host down]
Nmap scan report for 172.16.1.112 [host down]
Nmap scan report for 172.16.1.113 [host down]
Nmap scan report for 172.16.1.116 [host down]
Nmap scan report for 172.16.1.117 [host down]
Nmap scan report for 172.16.1.118 [host down]
Nmap scan report for 172.16.1.119 [host down]
Nmap scan report for 172.16.1.120 [host down]
Nmap scan report for 172.16.1.121 [host down]
Nmap scan report for 172.16.1.122 [host down]
Nmap scan report for 172.16.1.123 [host down]
Nmap scan report for 172.16.1.124 [host down]
Nmap scan report for 172.16.1.125 [host down]
Nmap scan report for 172.16.1.126 [host down]
Nmap scan report for 172.16.1.127 [host down]
Nmap scan report for 172.16.1.128 [host down]
Nmap scan report for 172.16.1.129 [host down]
Nmap scan report for 172.16.1.130 [host down]
Nmap scan report for 172.16.1.131 [host down]
Nmap scan report for 172.16.1.132 [host down]
Nmap scan report for 172.16.1.133 [host down]
Nmap scan report for 172.16.1.134 [host down]
Nmap scan report for 172.16.1.135 [host down]
Nmap scan report for 172.16.1.136 [host down]
Nmap scan report for 172.16.1.137 [host down]
Nmap scan report for 172.16.1.138 [host down]
Nmap scan report for 172.16.1.139 [host down]
Nmap scan report for 172.16.1.140 [host down]
Nmap scan report for 172.16.1.141 [host down]
Nmap scan report for 172.16.1.142 [host down]
Nmap scan report for 172.16.1.143 [host down]
Nmap scan report for 172.16.1.144 [host down]
Nmap scan report for 172.16.1.145 [host down]
Nmap scan report for 172.16.1.146 [host down]
Nmap scan report for 172.16.1.147 [host down]
Nmap scan report for 172.16.1.148 [host down]
Nmap scan report for 172.16.1.149 [host down]
Nmap scan report for 172.16.1.150 [host down]
Nmap scan report for 172.16.1.151 [host down]
Nmap scan report for 172.16.1.152 [host down]
Nmap scan report for 172.16.1.153 [host down]
Nmap scan report for 172.16.1.154 [host down]
Nmap scan report for 172.16.1.155 [host down]
Nmap scan report for 172.16.1.156 [host down]
Nmap scan report for 172.16.1.157 [host down]
Nmap scan report for 172.16.1.158 [host down]
Nmap scan report for 172.16.1.159 [host down]
Nmap scan report for 172.16.1.160 [host down]
Nmap scan report for 172.16.1.161 [host down]
Nmap scan report for 172.16.1.162 [host down]
Nmap scan report for 172.16.1.163 [host down]
Nmap scan report for 172.16.1.164 [host down]
Nmap scan report for 172.16.1.165 [host down]
Nmap scan report for 172.16.1.166 [host down]
Nmap scan report for 172.16.1.167 [host down]
Nmap scan report for 172.16.1.168 [host down]
Nmap scan report for 172.16.1.169 [host down]
Nmap scan report for 172.16.1.170 [host down]
Nmap scan report for 172.16.1.171 [host down]
Nmap scan report for 172.16.1.172 [host down]
Nmap scan report for 172.16.1.173 [host down]
Nmap scan report for 172.16.1.174 [host down]
Nmap scan report for 172.16.1.175 [host down]
Nmap scan report for 172.16.1.176 [host down]
Nmap scan report for 172.16.1.177 [host down]
Nmap scan report for 172.16.1.178 [host down]
Nmap scan report for 172.16.1.179 [host down]
Nmap scan report for 172.16.1.180 [host down]
Nmap scan report for 172.16.1.181 [host down]
Nmap scan report for 172.16.1.182 [host down]
Nmap scan report for 172.16.1.183 [host down]
Nmap scan report for 172.16.1.184 [host down]
Nmap scan report for 172.16.1.185 [host down]
Nmap scan report for 172.16.1.186 [host down]
Nmap scan report for 172.16.1.187 [host down]
Nmap scan report for 172.16.1.188 [host down]
Nmap scan report for 172.16.1.189 [host down]
Nmap scan report for 172.16.1.190 [host down]
Nmap scan report for 172.16.1.191 [host down]
Nmap scan report for 172.16.1.192 [host down]
Nmap scan report for 172.16.1.193 [host down]
Nmap scan report for 172.16.1.194 [host down]
Nmap scan report for 172.16.1.195 [host down]
Nmap scan report for 172.16.1.196 [host down]
Nmap scan report for 172.16.1.197 [host down]
Nmap scan report for 172.16.1.198 [host down]
Nmap scan report for 172.16.1.199 [host down]
Nmap scan report for 172.16.1.200 [host down]
Nmap scan report for 172.16.1.201 [host down]
Nmap scan report for 172.16.1.202 [host down]
Nmap scan report for 172.16.1.203 [host down]
Nmap scan report for 172.16.1.204 [host down]
Nmap scan report for 172.16.1.205 [host down]
Nmap scan report for 172.16.1.206 [host down]
Nmap scan report for 172.16.1.207 [host down]
Nmap scan report for 172.16.1.208 [host down]
Nmap scan report for 172.16.1.209 [host down]
Nmap scan report for 172.16.1.210 [host down]
Nmap scan report for 172.16.1.211 [host down]
Nmap scan report for 172.16.1.212 [host down]
Nmap scan report for 172.16.1.213 [host down]
Nmap scan report for 172.16.1.214 [host down]
Nmap scan report for 172.16.1.215 [host down]
Nmap scan report for 172.16.1.216 [host down]
Nmap scan report for 172.16.1.217 [host down]
Nmap scan report for 172.16.1.218 [host down]
Nmap scan report for 172.16.1.219 [host down]
Nmap scan report for 172.16.1.220 [host down]

Nmap scan report for 172.16.1.221 [host down]

Nmap scan report for 172.16.1.222 [host down]

Nmap scan report for 172.16.1.223 [host down]

Nmap scan report for 172.16.1.224 [host down]

Nmap scan report for 172.16.1.225 [host down]

Nmap scan report for 172.16.1.226 [host down]

Nmap scan report for 172.16.1.227 [host down]

Nmap scan report for 172.16.1.228 [host down]

Nmap scan report for 172.16.1.229 [host down]

Nmap scan report for 172.16.1.230 [host down]

Nmap scan report for 172.16.1.231 [host down]

Nmap scan report for 172.16.1.232 [host down]

Nmap scan report for 172.16.1.233 [host down]

Nmap scan report for 172.16.1.234 [host down]

Nmap scan report for 172.16.1.235 [host down]

Nmap scan report for 172.16.1.236 [host down]

Nmap scan report for 172.16.1.237 [host down]

Nmap scan report for 172.16.1.238 [host down]

Nmap scan report for 172.16.1.239 [host down]

Nmap scan report for 172.16.1.240 [host down]

Nmap scan report for 172.16.1.241 [host down]

Nmap scan report for 172.16.1.242 [host down]

Nmap scan report for 172.16.1.243 [host down]

Nmap scan report for 172.16.1.244 [host down]

Nmap scan report for 172.16.1.245 [host down]

Nmap scan report for 172.16.1.246 [host down]

Nmap scan report for 172.16.1.247 [host down]

Nmap scan report for 172.16.1.248 [host down]
Nmap scan report for 172.16.1.249 [host down]
Nmap scan report for 172.16.1.250 [host down]
Nmap scan report for 172.16.1.251 [host down]
Nmap scan report for 172.16.1.252 [host down]
Nmap scan report for 172.16.1.253 [host down]
Nmap scan report for 172.16.1.254 [host down]
Nmap scan report for 172.16.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 08:08
Completed Parallel DNS resolution of 1 host. at 08:08, 0.00s elapsed
Initiating SYN Stealth Scan at 08:08
Scanning 3 hosts [65535 ports/host]
Discovered open port 139/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.114
Discovered open port 80/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.1
Discovered open port 135/tcp on 172.16.1.115
Discovered open port 443/tcp on 172.16.1.114
Discovered open port 443/tcp on 172.16.1.1
Discovered open port 21/tcp on 172.16.1.115
Discovered open port 53/tcp on 172.16.1.1
Discovered open port 445/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 10.19% done; ETC: 08:13 (0:04:33 remaining)
SYN Stealth Scan Timing: About 28.10% done; ETC: 08:11 (0:02:36 remaining)
SYN Stealth Scan Timing: About 48.98% done; ETC: 08:11 (0:01:35 remaining)
Discovered open port 49667/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 65.83% done; ETC: 08:12 (0:01:20 remaining)
Discovered open port 5985/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 81.26% done; ETC: 08:12 (0:00:42 remaining)
Discovered open port 49668/tcp on 172.16.1.115
```

```
Completed SYN Stealth Scan against 172.16.1.114 in 207.97s (2 hosts left)

Completed SYN Stealth Scan against 172.16.1.115 in 208.22s (1 host left)

Completed SYN Stealth Scan at 08:11, 211.97s elapsed (196605 total ports)

Initiating Service scan at 08:11
```

Task 3.1 - OPsense.localdomain

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 08:08 Pacific Daylight Time

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating ARP Ping Scan at 08:08

Scanning 255 hosts [1 port/host]

Completed ARP Ping Scan at 08:08, 1.90s elapsed (255 total hosts)

Initiating Parallel DNS resolution of 3 hosts. at 08:08

Completed Parallel DNS resolution of 3 hosts. at 08:08, 0.00s elapsed

Nmap scan report for 172.16.1.0 [host down]

Nmap scan report for 172.16.1.2 [host down]

Nmap scan report for 172.16.1.3 [host down]

Nmap scan report for 172.16.1.4 [host down]

Nmap scan report for 172.16.1.5 [host down]

Nmap scan report for 172.16.1.6 [host down]

Nmap scan report for 172.16.1.7 [host down]

Nmap scan report for 172.16.1.8 [host down]
Nmap scan report for 172.16.1.9 [host down]

Nmap scan report for 172.16.1.10 [host down]

Nmap scan report for 172.16.1.11 [host down]

Nmap scan report for 172.16.1.12 [host down]

Nmap scan report for 172.16.1.14 [host down]

Nmap scan report for 172.16.1.15 [host down]

Nmap scan report for 172.16.1.16 [host down]

Nmap scan report for 172.16.1.17 [host down]

Nmap scan report for 172.16.1.18 [host down]

Nmap scan report for 172.16.1.19 [host down]

Nmap scan report for 172.16.1.20 [host down]

Nmap scan report for 172.16.1.21 [host down]

Nmap scan report for 172.16.1.22 [host down]

Nmap scan report for 172.16.1.23 [host down]

Nmap scan report for 172.16.1.24 [host down]

Nmap scan report for 172.16.1.25 [host down]

Nmap scan report for 172.16.1.26 [host down]

Nmap scan report for 172.16.1.27 [host down]

Nmap scan report for 172.16.1.28 [host down]

Nmap scan report for 172.16.1.29 [host down]

Nmap scan report for 172.16.1.30 [host down]

Nmap scan report for 172.16.1.31 [host down]

Nmap scan report for 172.16.1.32 [host down]

Nmap scan report for 172.16.1.33 [host down]

Nmap scan report for 172.16.1.34 [host down]

Nmap scan report for 172.16.1.35 [host down]

Nmap scan report for 172.16.1.36 [host down]

Nmap scan report for 172.16.1.37 [host down]

Nmap scan report for 172.16.1.38 [host down]
Nmap scan report for 172.16.1.39 [host down]
Nmap scan report for 172.16.1.40 [host down]
Nmap scan report for 172.16.1.41 [host down]
Nmap scan report for 172.16.1.42 [host down]
Nmap scan report for 172.16.1.43 [host down]
Nmap scan report for 172.16.1.44 [host down]
Nmap scan report for 172.16.1.45 [host down]
Nmap scan report for 172.16.1.46 [host down]
Nmap scan report for 172.16.1.47 [host down]
Nmap scan report for 172.16.1.48 [host down]
Nmap scan report for 172.16.1.49 [host down]
Nmap scan report for 172.16.1.50 [host down]
Nmap scan report for 172.16.1.51 [host down]
Nmap scan report for 172.16.1.52 [host down]
Nmap scan report for 172.16.1.53 [host down]
Nmap scan report for 172.16.1.54 [host down]
Nmap scan report for 172.16.1.55 [host down]
Nmap scan report for 172.16.1.56 [host down]
Nmap scan report for 172.16.1.57 [host down]
Nmap scan report for 172.16.1.58 [host down]
Nmap scan report for 172.16.1.59 [host down]
Nmap scan report for 172.16.1.60 [host down]
Nmap scan report for 172.16.1.61 [host down]
Nmap scan report for 172.16.1.62 [host down]
Nmap scan report for 172.16.1.63 [host down]
Nmap scan report for 172.16.1.64 [host down]
Nmap scan report for 172.16.1.65 [host down]
Nmap scan report for 172.16.1.66 [host down]
Nmap scan report for 172.16.1.67 [host down]
Nmap scan report for 172.16.1.68 [host down]
Nmap scan report for 172.16.1.69 [host down]
Nmap scan report for 172.16.1.70 [host down]
Nmap scan report for 172.16.1.71 [host down]
Nmap scan report for 172.16.1.72 [host down]
Nmap scan report for 172.16.1.73 [host down]
Nmap scan report for 172.16.1.74 [host down]
Nmap scan report for 172.16.1.75 [host down]
Nmap scan report for 172.16.1.76 [host down]
Nmap scan report for 172.16.1.77 [host down]
Nmap scan report for 172.16.1.78 [host down]
Nmap scan report for 172.16.1.79 [host down]
Nmap scan report for 172.16.1.80 [host down]
Nmap scan report for 172.16.1.81 [host down]
Nmap scan report for 172.16.1.82 [host down]
Nmap scan report for 172.16.1.83 [host down]
Nmap scan report for 172.16.1.84 [host down]
Nmap scan report for 172.16.1.85 [host down]
Nmap scan report for 172.16.1.86 [host down]
Nmap scan report for 172.16.1.87 [host down]
Nmap scan report for 172.16.1.88 [host down]
Nmap scan report for 172.16.1.89 [host down]
Nmap scan report for 172.16.1.90 [host down]
Nmap scan report for 172.16.1.91 [host down]
Nmap scan report for 172.16.1.92 [host down]
Nmap scan report for 172.16.1.93 [host down]
Nmap scan report for 172.16.1.94 [host down]
Nmap scan report for 172.16.1.95 [host down]
Nmap scan report for 172.16.1.96 [host down]
Nmap scan report for 172.16.1.97 [host down]
Nmap scan report for 172.16.1.98 [host down]
Nmap scan report for 172.16.1.99 [host down]
Nmap scan report for 172.16.1.100 [host down]
Nmap scan report for 172.16.1.101 [host down]
Nmap scan report for 172.16.1.102 [host down]
Nmap scan report for 172.16.1.103 [host down]
Nmap scan report for 172.16.1.104 [host down]
Nmap scan report for 172.16.1.105 [host down]
Nmap scan report for 172.16.1.106 [host down]
Nmap scan report for 172.16.1.107 [host down]
Nmap scan report for 172.16.1.108 [host down]
Nmap scan report for 172.16.1.109 [host down]
Nmap scan report for 172.16.1.110 [host down]
Nmap scan report for 172.16.1.111 [host down]
Nmap scan report for 172.16.1.112 [host down]
Nmap scan report for 172.16.1.113 [host down]
Nmap scan report for 172.16.1.116 [host down]
Nmap scan report for 172.16.1.117 [host down]
Nmap scan report for 172.16.1.118 [host down]
Nmap scan report for 172.16.1.119 [host down]
Nmap scan report for 172.16.1.120 [host down]
Nmap scan report for 172.16.1.121 [host down]
Nmap scan report for 172.16.1.122 [host down]
Nmap scan report for 172.16.1.123 [host down]
Nmap scan report for 172.16.1.124 [host down]
Nmap scan report for 172.16.1.125 [host down]
Nmap scan report for 172.16.1.126 [host down]
Nmap scan report for 172.16.1.127 [host down]
Nmap scan report for 172.16.1.128 [host down]

Nmap scan report for 172.16.1.129 [host down]

Nmap scan report for 172.16.1.130 [host down]

Nmap scan report for 172.16.1.131 [host down]

Nmap scan report for 172.16.1.132 [host down]

Nmap scan report for 172.16.1.133 [host down]

Nmap scan report for 172.16.1.134 [host down]

Nmap scan report for 172.16.1.135 [host down]

Nmap scan report for 172.16.1.136 [host down]

Nmap scan report for 172.16.1.137 [host down]

Nmap scan report for 172.16.1.138 [host down]

Nmap scan report for 172.16.1.139 [host down]

Nmap scan report for 172.16.1.140 [host down]

Nmap scan report for 172.16.1.141 [host down]

Nmap scan report for 172.16.1.142 [host down]

Nmap scan report for 172.16.1.143 [host down]

Nmap scan report for 172.16.1.144 [host down]

Nmap scan report for 172.16.1.145 [host down]

Nmap scan report for 172.16.1.146 [host down]

Nmap scan report for 172.16.1.147 [host down]

Nmap scan report for 172.16.1.148 [host down]

Nmap scan report for 172.16.1.149 [host down]

Nmap scan report for 172.16.1.150 [host down]

Nmap scan report for 172.16.1.151 [host down]

Nmap scan report for 172.16.1.152 [host down]

Nmap scan report for 172.16.1.153 [host down]

Nmap scan report for 172.16.1.154 [host down]

Nmap scan report for 172.16.1.155 [host down]

Nmap scan report for 172.16.1.156 [host down]
Nmap scan report for 172.16.1.157 [host down]
Nmap scan report for 172.16.1.158 [host down]
Nmap scan report for 172.16.1.159 [host down]
Nmap scan report for 172.16.1.160 [host down]
Nmap scan report for 172.16.1.161 [host down]
Nmap scan report for 172.16.1.162 [host down]
Nmap scan report for 172.16.1.163 [host down]
Nmap scan report for 172.16.1.164 [host down]
Nmap scan report for 172.16.1.165 [host down]
Nmap scan report for 172.16.1.166 [host down]
Nmap scan report for 172.16.1.167 [host down]
Nmap scan report for 172.16.1.168 [host down]
Nmap scan report for 172.16.1.169 [host down]
Nmap scan report for 172.16.1.170 [host down]
Nmap scan report for 172.16.1.171 [host down]
Nmap scan report for 172.16.1.172 [host down]
Nmap scan report for 172.16.1.173 [host down]
Nmap scan report for 172.16.1.174 [host down]
Nmap scan report for 172.16.1.175 [host down]
Nmap scan report for 172.16.1.176 [host down]
Nmap scan report for 172.16.1.177 [host down]
Nmap scan report for 172.16.1.178 [host down]
Nmap scan report for 172.16.1.179 [host down]
Nmap scan report for 172.16.1.180 [host down]
Nmap scan report for 172.16.1.181 [host down]
Nmap scan report for 172.16.1.182 [host down]
Nmap scan report for 172.16.1.183 [host down]
Nmap scan report for 172.16.1.184 [host down]
Nmap scan report for 172.16.1.185 [host down]
Nmap scan report for 172.16.1.186 [host down]
Nmap scan report for 172.16.1.187 [host down]
Nmap scan report for 172.16.1.188 [host down]
Nmap scan report for 172.16.1.189 [host down]
Nmap scan report for 172.16.1.190 [host down]
Nmap scan report for 172.16.1.191 [host down]
Nmap scan report for 172.16.1.192 [host down]
Nmap scan report for 172.16.1.193 [host down]
Nmap scan report for 172.16.1.194 [host down]
Nmap scan report for 172.16.1.195 [host down]
Nmap scan report for 172.16.1.196 [host down]
Nmap scan report for 172.16.1.197 [host down]
Nmap scan report for 172.16.1.198 [host down]
Nmap scan report for 172.16.1.199 [host down]
Nmap scan report for 172.16.1.200 [host down]
Nmap scan report for 172.16.1.201 [host down]
Nmap scan report for 172.16.1.202 [host down]
Nmap scan report for 172.16.1.203 [host down]
Nmap scan report for 172.16.1.204 [host down]
Nmap scan report for 172.16.1.205 [host down]
Nmap scan report for 172.16.1.206 [host down]
Nmap scan report for 172.16.1.207 [host down]
Nmap scan report for 172.16.1.208 [host down]
Nmap scan report for 172.16.1.209 [host down]
Nmap scan report for 172.16.1.210 [host down]
Nmap scan report for 172.16.1.211 [host down]
Nmap scan report for 172.16.1.212 [host down]
Nmap scan report for 172.16.1.213 [host down]
Nmap scan report for 172.16.1.214 [host down]
Nmap scan report for 172.16.1.215 [host down]
Nmap scan report for 172.16.1.216 [host down]
Nmap scan report for 172.16.1.217 [host down]
Nmap scan report for 172.16.1.218 [host down]
Nmap scan report for 172.16.1.219 [host down]
Nmap scan report for 172.16.1.220 [host down]
Nmap scan report for 172.16.1.221 [host down]
Nmap scan report for 172.16.1.222 [host down]
Nmap scan report for 172.16.1.223 [host down]
Nmap scan report for 172.16.1.224 [host down]
Nmap scan report for 172.16.1.225 [host down]
Nmap scan report for 172.16.1.226 [host down]
Nmap scan report for 172.16.1.227 [host down]
Nmap scan report for 172.16.1.228 [host down]
Nmap scan report for 172.16.1.229 [host down]
Nmap scan report for 172.16.1.230 [host down]
Nmap scan report for 172.16.1.231 [host down]
Nmap scan report for 172.16.1.232 [host down]
Nmap scan report for 172.16.1.233 [host down]
Nmap scan report for 172.16.1.234 [host down]
Nmap scan report for 172.16.1.235 [host down]
Nmap scan report for 172.16.1.236 [host down]
Nmap scan report for 172.16.1.237 [host down]
Nmap scan report for 172.16.1.238 [host down]
Nmap scan report for 172.16.1.239 [host down]
Nmap scan report for 172.16.1.240 [host down]
Nmap scan report for 172.16.1.241 [host down]
Nmap scan report for 172.16.1.242 [host down]
Nmap scan report for 172.16.1.243 [host down]
Nmap scan report for 172.16.1.244 [host down]
Nmap scan report for 172.16.1.245 [host down]
Nmap scan report for 172.16.1.246 [host down]
Nmap scan report for 172.16.1.247 [host down]
Nmap scan report for 172.16.1.248 [host down]
Nmap scan report for 172.16.1.249 [host down]
Nmap scan report for 172.16.1.250 [host down]
Nmap scan report for 172.16.1.251 [host down]
Nmap scan report for 172.16.1.252 [host down]
Nmap scan report for 172.16.1.253 [host down]
Nmap scan report for 172.16.1.254 [host down]
Nmap scan report for 172.16.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 08:08
Completed Parallel DNS resolution of 1 host. at 08:08, 0.00s elapsed
Initiating SYN Stealth Scan at 08:08
Scanning 3 hosts [65535 ports/host]
Discovered open port 139/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.114
Discovered open port 80/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.1
Discovered open port 135/tcp on 172.16.1.115
Discovered open port 443/tcp on 172.16.1.114
Discovered open port 443/tcp on 172.16.1.1
Discovered open port 21/tcp on 172.16.1.115
Discovered open port 53/tcp on 172.16.1.1
Discovered open port 445/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 10.19% done; ETC: 08:13 (0:04:33 remaining)
SYN Stealth Scan Timing: About 28.10% done; ETC: 08:11 (0:02:36 remaining)
SYN Stealth Scan Timing: About 48.98% done; ETC: 08:11 (0:01:35 remaining)
```

```
Discovered open port 49667/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 65.83% done; ETC: 08:12 (0:01:20 remaining)
Discovered open port 5985/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 81.26% done; ETC: 08:12 (0:00:42 remaining)
Discovered open port 49668/tcp on 172.16.1.115
Completed SYN Stealth Scan against 172.16.1.114 in 207.97s (2 hosts left)
Completed SYN Stealth Scan against 172.16.1.115 in 208.22s (1 host left)
Completed SYN Stealth Scan at 08:11, 211.97s elapsed (196605 total ports)
Initiating Service scan at 08:11
Scanning 13 services on 3 hosts
Completed Service scan at 08:14, 166.63s elapsed (13 services on 3 hosts)
Initiating OS detection (try #1) against 3 hosts
Retrying OS detection (try #2) against 3 hosts
NSE: Script scanning 3 hosts.
Initiating NSE at 08:14
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 08:15, 43.44s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 1.49s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 0.00s elapsed
Nmap scan report for OPNsense.localdomain (172.16.1.1)
Host is up (0.0018s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE  VERSION
53/tcp  open  domain   Unbound 1.17.1
| dns-nsid:
|   id.server: OPNsense.localdomain
|_  bind.version: unbound 1.17.1
```

```
80/tcp  open  http     OPNsense
|_http-server-header: OPNsense
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 301 Moved Permanently
|     Location: https:///nice%20ports%2C/Trinity.txt.bak
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:58 GMT
|     Server: OPNsense
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
|     Content-Length: 345
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:58 GMT
|     Server: OPNsense
|     <?xml version="1.0" encoding="iso-8859-1"?>
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|     </html>
|   GetRequest, HTTPOptions:
```

```
|    HTTP/1.0 301 Moved Permanently
|    Location: https:///
|    Content-Length: 0
|    Connection: close
|    Date: Wed, 14 Aug 2024 15:11:53 GMT
|    Server: OPNsense
|  RTSPRequest:
|    HTTP/1.0 400 Bad Request
|    Content-Type: text/html
|    Content-Length: 345
|    Connection: close
|    Date: Wed, 14 Aug 2024 15:11:53 GMT
|    Server: OPNsense
|    <?xml version="1.0" encoding="iso-8859-1"?>
|    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|    <head>
|    <title>400 Bad Request</title>
|    </head>
|    <body>
|    <h1>400 Bad Request</h1>
|    </body>
|_   </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https OPNsense
|_http-server-header: OPNsense
```

```
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Issuer: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-30T20:58:17
| Not valid after:  2024-06-30T20:58:17
| MD5:   7fda:2dce:fbf2:87b4:2732:b165:9f9e:8d03
|_SHA-1: d644:af14:45bb:2f7a:7481:185c:c10d:2265:56f7:75a4
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 1494
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:59 GMT
|   Server: OPNsense
|   <!doctype html>
|   <html lang="en" class="no-js">
|   <head>
|   <meta charset="UTF-8" />
|   <meta http-equiv="X-UA-Compatible" content="IE=edge">
|   <meta name="robots" content="noindex, nofollow" />
|  HTTPOptions:
|   HTTP/1.0 403 Forbidden
|   Set-Cookie: PHPSESSID=f0abfe275459893038daba3f39c73bd9; path=/; secure; HttpOnly
|   Expires: Thu, 19 Nov 1981 08:52:00 GMT
|   Cache-Control: no-store, no-cache, must-revalidate
|   Pragma: no-cache
|   Content-type: text/html; charset=UTF-8
|   Content-Length: 563
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:12:04 GMT
|   Server: OPNsense
|   <html><head><title>CSRF check failed</title>
|   <script>
|   document ).ready(function() {
|   $.ajaxSetup({
|   'beforeSend': function(xhr) {
|   xhr.setRequestHeader("X-CSRFToken", "OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09" );
|   </script>
|   </head>
|   <body>
|_   <p>CSRF check failed. Your form session may have expired, or you may not have cookies enabled.</p>
```

```
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: EDEF051C1ED081894527EAC8509EAC14
|_http-title: Login | OPNsense
|_http-trane-info: Problem with XML parsing of /evox/about
2 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-Port80-TCP:V=7.94%I=7%D=8/14%Time=66BCC939%P=i686-pc-windows-windows%r(
SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20
SF:Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OPNsense\r\n
SF:\r\n")%r(HTTPOptions,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLo
SF:cation:\x20https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\
SF:nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OP
SF:Nsense\r\n\r\n")%r(RTSPRequest,1ED,"HTTP/1\.0\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\
SF:x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nSe
SF:rver:\x20OPNsense\r\n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"iso-8
SF:859-1\"\?>\n<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\
SF:.0\x20Transitional//EN\"\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\"http://
SF:www\.w3\.org/TR/xhtml1/DTD/xhtml1-transitional\.dtd\">\n<html\x20xmlns=
SF:\"http://www\.w3\.org/1999/xhtml\"\x20xml:lang=\"en\"\x20lang=\"en\">\n
SF:\x20<head>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\x20</head>\n
SF:\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</body>\n</html
SF:>\n")%r(FourOhFourRequest,B3,"HTTP/1\.0\x20301\x20Moved\x20Permanently\
SF:r\nLocation:\x20https:///nice%20ports%2C/Trinity\.txt\.bak\r\nContent-L
SF:ength:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x2020
```

```
SF:24\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%r(GenericLines,1
SF:ED,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\
SF:nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\
SF:x20Aug\x202024\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<\?xml\
SF:x20version=\"1\.0\"\x20encoding=\"iso-8859-1\"\?>\n<!DOCTYPE\x20html\x2
SF:0PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Transitional//EN\"\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml
SF:1-transitional\.dtd\">\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml
SF:\"\x20xml:lang=\"en\"\x20lang=\"en\">\n\x20<head>\n\x20\x20<title>400\x
SF:20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20B
SF:ad\x20Request</h1>\n\x20</body>\n</html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94%T=SSL%I=7%D=8/14%Time=66BCC945%P=i686-pc-windows-win
SF:dows%r(GetRequest,88F,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20PHPSESS
SF:ID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/;\x20secure;\x20HttpOnly\
SF:r\nSet-Cookie:\x20PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/
SF:;\x20secure;\x20HttpOnly\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008
SF::52:00\x20GMT\r\nCache-Control:\x20no-store,\x20no-cache,\x20must-reval
SF:idate\r\nPragma:\x20no-cache\r\nContent-Security-Policy:\x20default-src
SF:\x20'self';\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'
SF:;\x20style-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval';\r\nX-Fram
SF:e-Options:\x20SAMEORIGIN\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS
SF:-Protection:\x201;\x20mode=block\r\nReferrer-Policy:\x20same-origin\r\n
SF:Content-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x201494
SF:\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11
SF::59\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!doctype\x20html>\n<html\x20l
SF:ang=\"en\"\x20class=\"no-js\">\n\x20\x20<head>\n\n\x20\x20\x20\x20<meta
SF:\x20charset=\"UTF-8\"\x20/>\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA
SF:-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x20\x20<meta\x20name=
SF:\"robots\"\x20content=\"noindex,\x20nofollow\"\x20/>\n\x20\x20\x20")%r(
SF:HTTPOptions,394,"HTTP/1\.0\x20403\x20Forbidden\r\nSet-Cookie:\x20PHPSES
SF:SID=f0abfe275459893038daba3f39c73bd9;\x20path=/;\x20secure;\x20HttpOnly
SF:\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\nCache-C
SF:ontrol:\x20no-store,\x20no-cache,\x20must-revalidate\r\nPragma:\x20no-c
SF:ache\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:
SF:\x20563\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x
SF:2015:12:04\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<html><head><title>CSRF
SF:\x20check\x20failed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20<script>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\$\(\x20document\x20\)\.ready\(function\(\)\x20{\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\$\.ajaxSetup\({\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:'beforeSend':\x20function\(xhr\)\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20xhr\.setRequest
SF:Header\(\"X-CSRFToken\",\x20\"OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09\"\x20\);
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}
SF:\);\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\);\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20</script>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20</head>\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>CSRF\x20check\x20
SF:failed\.\x20Your\x20form\x20session\x20may\x20have\x20expired,\x20or\x2
SF:0you\x20may\x20not\x20have\x20cookies\x20enabled\.</p>\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20");
MAC Address: BC:24:11:0F:90:00 (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): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Aug 14 08:14:37 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.78 ms OPNsense.localdomain (172.16.1.1)

Nmap scan report for 172.16.1.114
Host is up (0.0013s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd (PHP 5.6.21)
|_http-server-header: Apache
|_http-favicon: Unknown favicon MD5: 4B31A3DA81673FA571F35231D2EBB676
|_http-title: HammersHammersHammers
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
| http-robots.txt: 4 disallowed entries
|_/admin/ /core/ /download/ /system/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open   ssl/http Apache httpd (PHP 5.6.21)
```

```
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-05-10T20:03:33
| Not valid after:  2026-05-08T20:03:33
| MD5:   e2c3:a8ef:0eb8:f9d1:bb1a:72c0:178a:b605
|_SHA-1: e0df:7c75:38af:d191:f69c:cec5:908e:f3ae:02c0:9681
| http-robots.txt: 4 disallowed entries
|_/admin/ /core/ /download/ /system/
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
|_http-title: HammersHammersHammers
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: BC:24:11:F8:E0:0F (Unknown)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.16 - 4.6 (95%), Linux 3.2 - 4.9 (94%),
Linux 4.10 (94%), Linux 3.2 - 3.8 (93%), Linux 3.16 (93%), Linux 4.4 (93%), Linux 3.13 (92%),
Linux 5.1 (92%), Linux 3.13 or 4.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Aug 14 08:12:28 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.29 ms 172.16.1.114
```

```
Nmap scan report for 172.16.1.115
Host is up (0.0014s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip.6u35iss.partial
| 06-02-2016  08:34PM            205824 international-sales-data-HammerCorpInt.xls
| 06-02-2016  09:11PM               250 LogonHelp.txt
| 06-02-2016  08:36PM            113183 Sacramentorealestatetransactions.csv
| 06-02-2016  08:37PM            123637 SalesJan2009.csv
|_06-02-2016  08:37PM             93536 TechCrunchcontinentalUSA.csv
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49667/tcp open  msrpc         Microsoft Windows RPC
```

```
49668/tcp open  msrpc        Microsoft Windows RPC
MAC Address: BC:24:11:50:3B:0E (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 2019 (95%)
Aggressive OS guesses: Microsoft Windows Server 2019 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (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: 2024-08-14T15:14:39
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: HAMMERCORP, NetBIOS user: <unknown>, NetBIOS MAC: bc:24:11:50:3b:0e (unknown)
| Names:
|   HAMMERCORP<00>      Flags: <unique><active>
|   HAMMERS<00>         Flags: <group><active>
|_  HAMMERCORP<20>      Flags: <unique><active>

TRACEROUTE
```

```
HOP RTT     ADDRESS
1   1.40 ms 172.16.1.115

Initiating SYN Stealth Scan at 08:15
Scanning 172.16.1.13 [65535 ports]
Discovered open port 139/tcp on 172.16.1.13
Discovered open port 135/tcp on 172.16.1.13
Discovered open port 445/tcp on 172.16.1.13
Discovered open port 49665/tcp on 172.16.1.13
Discovered open port 49666/tcp on 172.16.1.13
Discovered open port 49667/tcp on 172.16.1.13
Discovered open port 49671/tcp on 172.16.1.13
Discovered open port 5357/tcp on 172.16.1.13
Discovered open port 5040/tcp on 172.16.1.13
Discovered open port 49668/tcp on 172.16.1.13
Discovered open port 49664/tcp on 172.16.1.13
Completed SYN Stealth Scan at 08:15, 14.00s elapsed (65535 total ports)
Initiating Service scan at 08:15
Scanning 11 services on 172.16.1.13
Service scan Timing: About 45.45% done; ETC: 08:17 (0:01:05 remaining)
```

Task 3.2 - 172.16.1.13

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 08:08 Pacific Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
```

```
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating ARP Ping Scan at 08:08
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 08:08, 1.90s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 08:08
Completed Parallel DNS resolution of 3 hosts. at 08:08, 0.00s elapsed
Nmap scan report for 172.16.1.0 [host down]
Nmap scan report for 172.16.1.2 [host down]
Nmap scan report for 172.16.1.3 [host down]
Nmap scan report for 172.16.1.4 [host down]
Nmap scan report for 172.16.1.5 [host down]
Nmap scan report for 172.16.1.6 [host down]
Nmap scan report for 172.16.1.7 [host down]
Nmap scan report for 172.16.1.8 [host down]
Nmap scan report for 172.16.1.9 [host down]
Nmap scan report for 172.16.1.10 [host down]
Nmap scan report for 172.16.1.11 [host down]
Nmap scan report for 172.16.1.12 [host down]
Nmap scan report for 172.16.1.14 [host down]
Nmap scan report for 172.16.1.15 [host down]
Nmap scan report for 172.16.1.16 [host down]
Nmap scan report for 172.16.1.17 [host down]
Nmap scan report for 172.16.1.18 [host down]
Nmap scan report for 172.16.1.19 [host down]
Nmap scan report for 172.16.1.20 [host down]
Nmap scan report for 172.16.1.21 [host down]
Nmap scan report for 172.16.1.22 [host down]
Nmap scan report for 172.16.1.23 [host down]
Nmap scan report for 172.16.1.24 [host down]
Nmap scan report for 172.16.1.25 [host down]
Nmap scan report for 172.16.1.26 [host down]
Nmap scan report for 172.16.1.27 [host down]
Nmap scan report for 172.16.1.28 [host down]
Nmap scan report for 172.16.1.29 [host down]
Nmap scan report for 172.16.1.30 [host down]
Nmap scan report for 172.16.1.31 [host down]
Nmap scan report for 172.16.1.32 [host down]
Nmap scan report for 172.16.1.33 [host down]
Nmap scan report for 172.16.1.34 [host down]
Nmap scan report for 172.16.1.35 [host down]
Nmap scan report for 172.16.1.36 [host down]
Nmap scan report for 172.16.1.37 [host down]
Nmap scan report for 172.16.1.38 [host down]
Nmap scan report for 172.16.1.39 [host down]
Nmap scan report for 172.16.1.40 [host down]
Nmap scan report for 172.16.1.41 [host down]
Nmap scan report for 172.16.1.42 [host down]
Nmap scan report for 172.16.1.43 [host down]
Nmap scan report for 172.16.1.44 [host down]
Nmap scan report for 172.16.1.45 [host down]
Nmap scan report for 172.16.1.46 [host down]
Nmap scan report for 172.16.1.47 [host down]
Nmap scan report for 172.16.1.48 [host down]
Nmap scan report for 172.16.1.49 [host down]
Nmap scan report for 172.16.1.50 [host down]
Nmap scan report for 172.16.1.51 [host down]

Nmap scan report for 172.16.1.52 [host down]

Nmap scan report for 172.16.1.53 [host down]

Nmap scan report for 172.16.1.54 [host down]

Nmap scan report for 172.16.1.55 [host down]

Nmap scan report for 172.16.1.56 [host down]

Nmap scan report for 172.16.1.57 [host down]

Nmap scan report for 172.16.1.58 [host down]

Nmap scan report for 172.16.1.59 [host down]

Nmap scan report for 172.16.1.60 [host down]

Nmap scan report for 172.16.1.61 [host down]

Nmap scan report for 172.16.1.62 [host down]

Nmap scan report for 172.16.1.63 [host down]

Nmap scan report for 172.16.1.64 [host down]

Nmap scan report for 172.16.1.65 [host down]

Nmap scan report for 172.16.1.66 [host down]

Nmap scan report for 172.16.1.67 [host down]

Nmap scan report for 172.16.1.68 [host down]

Nmap scan report for 172.16.1.69 [host down]

Nmap scan report for 172.16.1.70 [host down]

Nmap scan report for 172.16.1.71 [host down]

Nmap scan report for 172.16.1.72 [host down]

Nmap scan report for 172.16.1.73 [host down]

Nmap scan report for 172.16.1.74 [host down]

Nmap scan report for 172.16.1.75 [host down]

Nmap scan report for 172.16.1.76 [host down]

Nmap scan report for 172.16.1.77 [host down]

Nmap scan report for 172.16.1.78 [host down]

Nmap scan report for 172.16.1.79 [host down]
Nmap scan report for 172.16.1.80 [host down]
Nmap scan report for 172.16.1.81 [host down]
Nmap scan report for 172.16.1.82 [host down]
Nmap scan report for 172.16.1.83 [host down]
Nmap scan report for 172.16.1.84 [host down]
Nmap scan report for 172.16.1.85 [host down]
Nmap scan report for 172.16.1.86 [host down]
Nmap scan report for 172.16.1.87 [host down]
Nmap scan report for 172.16.1.88 [host down]
Nmap scan report for 172.16.1.89 [host down]
Nmap scan report for 172.16.1.90 [host down]
Nmap scan report for 172.16.1.91 [host down]
Nmap scan report for 172.16.1.92 [host down]
Nmap scan report for 172.16.1.93 [host down]
Nmap scan report for 172.16.1.94 [host down]
Nmap scan report for 172.16.1.95 [host down]
Nmap scan report for 172.16.1.96 [host down]
Nmap scan report for 172.16.1.97 [host down]
Nmap scan report for 172.16.1.98 [host down]
Nmap scan report for 172.16.1.99 [host down]
Nmap scan report for 172.16.1.100 [host down]
Nmap scan report for 172.16.1.101 [host down]
Nmap scan report for 172.16.1.102 [host down]
Nmap scan report for 172.16.1.103 [host down]
Nmap scan report for 172.16.1.104 [host down]
Nmap scan report for 172.16.1.105 [host down]
Nmap scan report for 172.16.1.106 [host down]
Nmap scan report for 172.16.1.107 [host down]
Nmap scan report for 172.16.1.108 [host down]
Nmap scan report for 172.16.1.109 [host down]

Nmap scan report for 172.16.1.110 [host down]

Nmap scan report for 172.16.1.111 [host down]

Nmap scan report for 172.16.1.112 [host down]

Nmap scan report for 172.16.1.113 [host down]

Nmap scan report for 172.16.1.116 [host down]

Nmap scan report for 172.16.1.117 [host down]

Nmap scan report for 172.16.1.118 [host down]

Nmap scan report for 172.16.1.119 [host down]

Nmap scan report for 172.16.1.120 [host down]

Nmap scan report for 172.16.1.121 [host down]

Nmap scan report for 172.16.1.122 [host down]

Nmap scan report for 172.16.1.123 [host down]

Nmap scan report for 172.16.1.124 [host down]

Nmap scan report for 172.16.1.125 [host down]

Nmap scan report for 172.16.1.126 [host down]

Nmap scan report for 172.16.1.127 [host down]

Nmap scan report for 172.16.1.128 [host down]

Nmap scan report for 172.16.1.129 [host down]

Nmap scan report for 172.16.1.130 [host down]

Nmap scan report for 172.16.1.131 [host down]

Nmap scan report for 172.16.1.132 [host down]

Nmap scan report for 172.16.1.133 [host down]

Nmap scan report for 172.16.1.134 [host down]

Nmap scan report for 172.16.1.135 [host down]

Nmap scan report for 172.16.1.136 [host down]

Nmap scan report for 172.16.1.137 [host down]

Nmap scan report for 172.16.1.138 [host down]

Nmap scan report for 172.16.1.139 [host down]
Nmap scan report for 172.16.1.140 [host down]
Nmap scan report for 172.16.1.141 [host down]
Nmap scan report for 172.16.1.142 [host down]
Nmap scan report for 172.16.1.143 [host down]
Nmap scan report for 172.16.1.144 [host down]
Nmap scan report for 172.16.1.145 [host down]
Nmap scan report for 172.16.1.146 [host down]
Nmap scan report for 172.16.1.147 [host down]
Nmap scan report for 172.16.1.148 [host down]
Nmap scan report for 172.16.1.149 [host down]
Nmap scan report for 172.16.1.150 [host down]
Nmap scan report for 172.16.1.151 [host down]
Nmap scan report for 172.16.1.152 [host down]
Nmap scan report for 172.16.1.153 [host down]
Nmap scan report for 172.16.1.154 [host down]
Nmap scan report for 172.16.1.155 [host down]
Nmap scan report for 172.16.1.156 [host down]
Nmap scan report for 172.16.1.157 [host down]
Nmap scan report for 172.16.1.158 [host down]
Nmap scan report for 172.16.1.159 [host down]
Nmap scan report for 172.16.1.160 [host down]
Nmap scan report for 172.16.1.161 [host down]
Nmap scan report for 172.16.1.162 [host down]
Nmap scan report for 172.16.1.163 [host down]
Nmap scan report for 172.16.1.164 [host down]
Nmap scan report for 172.16.1.165 [host down]
Nmap scan report for 172.16.1.166 [host down]
Nmap scan report for 172.16.1.167 [host down]
Nmap scan report for 172.16.1.168 [host down]
Nmap scan report for 172.16.1.169 [host down]
Nmap scan report for 172.16.1.170 [host down]
Nmap scan report for 172.16.1.171 [host down]
Nmap scan report for 172.16.1.172 [host down]
Nmap scan report for 172.16.1.173 [host down]
Nmap scan report for 172.16.1.174 [host down]
Nmap scan report for 172.16.1.175 [host down]
Nmap scan report for 172.16.1.176 [host down]
Nmap scan report for 172.16.1.177 [host down]
Nmap scan report for 172.16.1.178 [host down]
Nmap scan report for 172.16.1.179 [host down]
Nmap scan report for 172.16.1.180 [host down]
Nmap scan report for 172.16.1.181 [host down]
Nmap scan report for 172.16.1.182 [host down]
Nmap scan report for 172.16.1.183 [host down]
Nmap scan report for 172.16.1.184 [host down]
Nmap scan report for 172.16.1.185 [host down]
Nmap scan report for 172.16.1.186 [host down]
Nmap scan report for 172.16.1.187 [host down]
Nmap scan report for 172.16.1.188 [host down]
Nmap scan report for 172.16.1.189 [host down]
Nmap scan report for 172.16.1.190 [host down]
Nmap scan report for 172.16.1.191 [host down]
Nmap scan report for 172.16.1.192 [host down]
Nmap scan report for 172.16.1.193 [host down]
Nmap scan report for 172.16.1.194 [host down]
Nmap scan report for 172.16.1.195 [host down]
Nmap scan report for 172.16.1.196 [host down]
Nmap scan report for 172.16.1.197 [host down]
Nmap scan report for 172.16.1.198 [host down]
Nmap scan report for 172.16.1.199 [host down]
Nmap scan report for 172.16.1.200 [host down]
Nmap scan report for 172.16.1.201 [host down]
Nmap scan report for 172.16.1.202 [host down]
Nmap scan report for 172.16.1.203 [host down]
Nmap scan report for 172.16.1.204 [host down]
Nmap scan report for 172.16.1.205 [host down]
Nmap scan report for 172.16.1.206 [host down]
Nmap scan report for 172.16.1.207 [host down]
Nmap scan report for 172.16.1.208 [host down]
Nmap scan report for 172.16.1.209 [host down]
Nmap scan report for 172.16.1.210 [host down]
Nmap scan report for 172.16.1.211 [host down]
Nmap scan report for 172.16.1.212 [host down]
Nmap scan report for 172.16.1.213 [host down]
Nmap scan report for 172.16.1.214 [host down]
Nmap scan report for 172.16.1.215 [host down]
Nmap scan report for 172.16.1.216 [host down]
Nmap scan report for 172.16.1.217 [host down]
Nmap scan report for 172.16.1.218 [host down]
Nmap scan report for 172.16.1.219 [host down]
Nmap scan report for 172.16.1.220 [host down]
Nmap scan report for 172.16.1.221 [host down]
Nmap scan report for 172.16.1.222 [host down]
Nmap scan report for 172.16.1.223 [host down]
Nmap scan report for 172.16.1.224 [host down]
Nmap scan report for 172.16.1.225 [host down]
Nmap scan report for 172.16.1.226 [host down]
Nmap scan report for 172.16.1.227 [host down]
Nmap scan report for 172.16.1.228 [host down]
Nmap scan report for 172.16.1.229 [host down]
Nmap scan report for 172.16.1.230 [host down]
Nmap scan report for 172.16.1.231 [host down]
Nmap scan report for 172.16.1.232 [host down]
Nmap scan report for 172.16.1.233 [host down]
Nmap scan report for 172.16.1.234 [host down]
Nmap scan report for 172.16.1.235 [host down]
Nmap scan report for 172.16.1.236 [host down]
Nmap scan report for 172.16.1.237 [host down]
Nmap scan report for 172.16.1.238 [host down]
Nmap scan report for 172.16.1.239 [host down]
Nmap scan report for 172.16.1.240 [host down]
Nmap scan report for 172.16.1.241 [host down]
Nmap scan report for 172.16.1.242 [host down]
Nmap scan report for 172.16.1.243 [host down]
Nmap scan report for 172.16.1.244 [host down]
Nmap scan report for 172.16.1.245 [host down]
Nmap scan report for 172.16.1.246 [host down]
Nmap scan report for 172.16.1.247 [host down]
Nmap scan report for 172.16.1.248 [host down]
Nmap scan report for 172.16.1.249 [host down]
Nmap scan report for 172.16.1.250 [host down]
Nmap scan report for 172.16.1.251 [host down]
Nmap scan report for 172.16.1.252 [host down]
Nmap scan report for 172.16.1.253 [host down]
Nmap scan report for 172.16.1.254 [host down]
Nmap scan report for 172.16.1.255 [host down]
```

```
Initiating Parallel DNS resolution of 1 host. at 08:08

Completed Parallel DNS resolution of 1 host. at 08:08, 0.00s elapsed

Initiating SYN Stealth Scan at 08:08

Scanning 3 hosts [65535 ports/host]

Discovered open port 139/tcp on 172.16.1.115

Discovered open port 80/tcp on 172.16.1.114

Discovered open port 80/tcp on 172.16.1.115

Discovered open port 80/tcp on 172.16.1.1

Discovered open port 135/tcp on 172.16.1.115

Discovered open port 443/tcp on 172.16.1.114

Discovered open port 443/tcp on 172.16.1.1

Discovered open port 21/tcp on 172.16.1.115

Discovered open port 53/tcp on 172.16.1.1

Discovered open port 445/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 10.19% done; ETC: 08:13 (0:04:33 remaining)

SYN Stealth Scan Timing: About 28.10% done; ETC: 08:11 (0:02:36 remaining)

SYN Stealth Scan Timing: About 48.98% done; ETC: 08:11 (0:01:35 remaining)

Discovered open port 49667/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 65.83% done; ETC: 08:12 (0:01:20 remaining)

Discovered open port 5985/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 81.26% done; ETC: 08:12 (0:00:42 remaining)

Discovered open port 49668/tcp on 172.16.1.115

Completed SYN Stealth Scan against 172.16.1.114 in 207.97s (2 hosts left)

Completed SYN Stealth Scan against 172.16.1.115 in 208.22s (1 host left)

Completed SYN Stealth Scan at 08:11, 211.97s elapsed (196605 total ports)

Initiating Service scan at 08:11

Scanning 13 services on 3 hosts

Completed Service scan at 08:14, 166.63s elapsed (13 services on 3 hosts)

Initiating OS detection (try #1) against 3 hosts
```

```
Retrying OS detection (try #2) against 3 hosts

NSE: Script scanning 3 hosts.

Initiating NSE at 08:14

NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.

Completed NSE at 08:15, 43.44s elapsed

Initiating NSE at 08:15

Completed NSE at 08:15, 1.49s elapsed

Initiating NSE at 08:15

Completed NSE at 08:15, 0.00s elapsed

Nmap scan report for OPNsense.localdomain (172.16.1.1)

Host is up (0.0018s latency).

Not shown: 65532 filtered tcp ports (no-response)

PORT   STATE SERVICE  VERSION

53/tcp  open  domain   Unbound 1.17.1

| dns-nsid:

|  id.server: OPNsense.localdomain

|_  bind.version: unbound 1.17.1

80/tcp  open  http     OPNsense

|_http-server-header: OPNsense

| fingerprint-strings:

|  FourOhFourRequest:

|    HTTP/1.0 301 Moved Permanently

|    Location: https:///nice%20ports%2C/Trinity.txt.bak

|    Content-Length: 0

|    Connection: close

|    Date: Wed, 14 Aug 2024 15:11:58 GMT

|    Server: OPNsense

|  GenericLines:

|    HTTP/1.0 400 Bad Request
|   Content-Type: text/html
|   Content-Length: 345
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:58 GMT
|   Server: OPNsense
|   <?xml version="1.0" encoding="iso-8859-1"?>
|   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|   <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|   <head>
|   <title>400 Bad Request</title>
|   </head>
|   <body>
|   <h1>400 Bad Request</h1>
|   </body>
|   </html>
| GetRequest, HTTPOptions:
|   HTTP/1.0 301 Moved Permanently
|   Location: https:///
|   Content-Length: 0
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:53 GMT
|   Server: OPNsense
| RTSPRequest:
|   HTTP/1.0 400 Bad Request
|   Content-Type: text/html
|   Content-Length: 345
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:53 GMT
|    Server: OPNsense
|    <?xml version="1.0" encoding="iso-8859-1"?>
|    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|    <head>
|    <title>400 Bad Request</title>
|    </head>
|    <body>
|    <h1>400 Bad Request</h1>
|    </body>
|_   </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https OPNsense
|_http-server-header: OPNsense
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Issuer: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-30T20:58:17
| Not valid after:  2024-06-30T20:58:17
| MD5:   7fda:2dce:fbf2:87b4:2732:b165:9f9e:8d03
|_SHA-1: d644:af14:45bb:2f7a:7481:185c:c10d:2265:56f7:75a4
```

```
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 1494
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:59 GMT
|     Server: OPNsense
|     <!doctype html>
|     <html lang="en" class="no-js">
|     <head>
|     <meta charset="UTF-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta name="robots" content="noindex, nofollow" />
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Set-Cookie: PHPSESSID=f0abfe275459893038daba3f39c73bd9; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|   Cache-Control: no-store, no-cache, must-revalidate

|   Pragma: no-cache

|   Content-type: text/html; charset=UTF-8

|   Content-Length: 563

|   Connection: close

|   Date: Wed, 14 Aug 2024 15:12:04 GMT

|   Server: OPNsense

|   <html><head><title>CSRF check failed</title>

|   <script>

|   document ).ready(function() {

|   $.ajaxSetup({

|   'beforeSend': function(xhr) {

|   xhr.setRequestHeader("X-CSRFToken", "OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09" );

|   </script>

|   </head>

|   <body>

|_   <p>CSRF check failed. Your form session may have expired, or you may not have cookies enabled.</p>

|_ssl-date: TLS randomness does not represent time

| http-methods:

|_  Supported Methods: GET HEAD POST OPTIONS

|_http-favicon: Unknown favicon MD5: EDEF051C1ED081894527EAC8509EAC14

|_http-title: Login | OPNsense

|_http-trane-info: Problem with XML parsing of /evox/about

2 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-Port80-TCP:V=7.94%I=7%D=8/14%Time=66BCC939%P=i686-pc-windows-windows%r(

SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20
SF:Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OPNsense\r\n
SF:\r\n")%r(HTTPOptions,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLo
SF:cation:\x20https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\
SF:nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OP
SF:Nsense\r\n\r\n")%r(RTSPRequest,1ED,"HTTP/1\.0\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\
SF:x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nSe
SF:rver:\x20OPNsense\r\n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"iso-8
SF:859-1\"\?>\n<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\
SF:.0\x20Transitional//EN\"\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\"http://
SF:www\.w3\.org/TR/xhtml1/DTD/xhtml1-transitional\.dtd\">\n<html\x20xmlns=
SF:\"http://www\.w3\.org/1999/xhtml\"\x20xml:lang=\"en\"\x20lang=\"en\">\n
SF:\x20<head>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\x20</head>\n
SF:\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</body>\n</html
SF:>\n")%r(FourOhFourRequest,B3,"HTTP/1\.0\x20301\x20Moved\x20Permanently\
SF:r\nLocation:\x20https:///nice%20ports%2C/Trinity\.txt\.bak\r\nContent-L
SF:ength:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x2020
SF:24\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%r(GenericLines,1
SF:ED,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\
SF:nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\
SF:x20Aug\x202024\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<\?xml\
SF:x20version=\"1\.0\"\x20encoding=\"iso-8859-1\"\?>\n<!DOCTYPE\x20html\x2
SF:0PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Transitional//EN\"\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml
SF:1-transitional\.dtd\">\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml
SF:\"\x20xml:lang=\"en\"\x20lang=\"en\">\n\x20<head>\n\x20\x20<title>400\x
SF:20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20B
SF:ad\x20Request</h1>\n\x20</body>\n</html>\n");
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94%T=SSL%I=7%D=8/14%Time=66BCC945%P=i686-pc-windows-win
SF:dows%r(GetRequest,88F,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20PHPSESS
SF:ID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/;\x20secure;\x20HttpOnly\
SF:r\nSet-Cookie:\x20PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/
SF:;\x20secure;\x20HttpOnly\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008
SF::52:00\x20GMT\r\nCache-Control:\x20no-store,\x20no-cache,\x20must-reval
SF:idate\r\nPragma:\x20no-cache\r\nContent-Security-Policy:\x20default-src
SF:\x20'self';\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'
SF:;\x20style-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval';\r\nX-Fram
SF:e-Options:\x20SAMEORIGIN\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS
SF:-Protection:\x201;\x20mode=block\r\nReferrer-Policy:\x20same-origin\r\n
SF:Content-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x201494
SF:\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11
SF::59\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!doctype\x20html>\n<html\x20l
SF:ang=\"en\"\x20class=\"no-js\">\n\x20\x20<head>\n\n\x20\x20\x20\x20<meta
SF:\x20charset=\"UTF-8\"\x20/>\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA
SF:-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x20\x20<meta\x20name=
SF:\"robots\"\x20content=\"noindex,\x20nofollow\"\x20/>\n\x20\x20\x20")%r(
SF:HTTPOptions,394,"HTTP/1\.0\x20403\x20Forbidden\r\nSet-Cookie:\x20PHPSES
SF:SID=f0abfe275459893038daba3f39c73bd9;\x20path=/;\x20secure;\x20HttpOnly
SF:\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\nCache-C
SF:ontrol:\x20no-store,\x20no-cache,\x20must-revalidate\r\nPragma:\x20no-c
SF:ache\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:
SF:\x20563\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x
SF:2015:12:04\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<html><head><title>CSRF
SF:\x20check\x20failed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20<script>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\$\(\x20document\x20\)\.ready\(function\(\)\x20{\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\$\.ajaxSetup\({\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:'beforeSend':\x20function\(xhr\)\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20xhr\.setRequest
SF:Header\(\"X-CSRFToken\",\x20\"OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09\"\x20\);
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}
SF:\);\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\);\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20</script>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20</head>\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>CSRF\x20check\x20
SF:failed\.\x20Your\x20form\x20session\x20may\x20have\x20expired,\x20or\x2
SF:0you\x20may\x20not\x20have\x20cookies\x20enabled\.</p>\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20");

MAC Address: BC:24:11:0F:90:00 (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): FreeBSD 11.X (91%)

OS CPE: cpe:/o:freebsd:freebsd:11.2

Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 0.001 days (since Wed Aug 14 08:14:37 2024)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=264 (Good luck!)

IP ID Sequence Generation: All zeros


TRACEROUTE
```

```
HOP RTT    ADDRESS

1   1.78 ms OPNsense.localdomain (172.16.1.1)


Nmap scan report for 172.16.1.114

Host is up (0.0013s latency).

Not shown: 65532 filtered tcp ports (no-response)

PORT    STATE  SERVICE  VERSION

22/tcp  closed ssh

80/tcp  open   http     Apache httpd (PHP 5.6.21)

|_http-server-header: Apache

|_http-favicon: Unknown favicon MD5: 4B31A3DA81673FA571F35231D2EBB676

|_http-title: HammersHammersHammers

|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution

| http-robots.txt: 4 disallowed entries

|_/admin/ /core/ /download/ /system/

| http-methods:

|_  Supported Methods: GET HEAD POST OPTIONS

443/tcp open   ssl/http Apache httpd (PHP 5.6.21)

|_http-server-header: Apache

| ssl-cert: Subject: commonName=www.example.com

| Issuer: commonName=www.example.com

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2016-05-10T20:03:33

| Not valid after:  2026-05-08T20:03:33

| MD5:   e2c3:a8ef:0eb8:f9d1:bb1a:72c0:178a:b605

|_SHA-1: e0df:7c75:38af:d191:f69c:cec5:908e:f3ae:02c0:9681

| http-robots.txt: 4 disallowed entries
```

```
|_/admin/ /core/ /download/ /system/
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
|_http-title: HammersHammersHammers
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: BC:24:11:F8:E0:0F (Unknown)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.16 - 4.6 (95%), Linux 3.2 - 4.9 (94%), Linux 4.10 (94%), Linux 3.2 - 3.8 (93%), Linux 3.16 (93%), Linux 4.4 (93%), Linux 3.13 (92%), Linux 5.1 (92%), Linux 3.13 or 4.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Aug 14 08:12:28 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.29 ms 172.16.1.114

Nmap scan report for 172.16.1.115
Host is up (0.0014s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip.6u35iss.partial
| 06-02-2016  08:34PM            205824 international-sales-data-HammerCorpInt.xls
| 06-02-2016  09:11PM               250 LogonHelp.txt
| 06-02-2016  08:36PM            113183 Sacramentorealestatetransactions.csv
| 06-02-2016  08:37PM            123637 SalesJan2009.csv
|_06-02-2016  08:37PM             93536 TechCrunchcontinentalUSA.csv
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
MAC Address: BC:24:11:50:3B:0E (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 2019 (95%)
Aggressive OS guesses: Microsoft Windows Server 2019 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (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: 2024-08-14T15:14:39
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: HAMMERCORP, NetBIOS user: <unknown>, NetBIOS MAC: bc:24:11:50:3b:0e (unknown)
| Names:
|   HAMMERCORP<00>       Flags: <unique><active>
|   HAMMERS<00>          Flags: <group><active>
|_  HAMMERCORP<20>       Flags: <unique><active>

TRACEROUTE
HOP RTT     ADDRESS
1   1.40 ms 172.16.1.115

Initiating SYN Stealth Scan at 08:15
Scanning 172.16.1.13 [65535 ports]
Discovered open port 139/tcp on 172.16.1.13
Discovered open port 135/tcp on 172.16.1.13
Discovered open port 445/tcp on 172.16.1.13
Discovered open port 49665/tcp on 172.16.1.13
Discovered open port 49666/tcp on 172.16.1.13
Discovered open port 49667/tcp on 172.16.1.13
Discovered open port 49671/tcp on 172.16.1.13
Discovered open port 5357/tcp on 172.16.1.13
Discovered open port 5040/tcp on 172.16.1.13
Discovered open port 49668/tcp on 172.16.1.13
Discovered open port 49664/tcp on 172.16.1.13
Completed SYN Stealth Scan at 08:15, 14.00s elapsed (65535 total ports)
Initiating Service scan at 08:15
Scanning 11 services on 172.16.1.13
Service scan Timing: About 45.45% done; ETC: 08:17 (0:01:05 remaining)
Completed Service scan at 08:18, 156.31s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against 172.16.1.13
NSE: Script scanning 172.16.1.13.
Initiating NSE at 08:18
Completed NSE at 08:18, 14.94s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 1.02s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Nmap scan report for 172.16.1.13
Host is up (0.00081s latency).
Not shown: 65523 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
135/tcp   open     msrpc        Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
5040/tcp  open     unknown
5357/tcp  open     http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open   msrpc      Microsoft Windows RPC
49665/tcp open   msrpc      Microsoft Windows RPC
49666/tcp open   msrpc      Microsoft Windows RPC
49667/tcp open   msrpc      Microsoft Windows RPC
49668/tcp open   msrpc      Microsoft Windows RPC
49671/tcp open   msrpc      Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 10
OS details: Microsoft Windows 10 2004
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:
| smb2-time:
|   date: 2024-08-14T15:18:19
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
```

```
Completed NSE at 08:18, 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.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 622.09 seconds

     Raw packets sent: 459966 (20.242MB) | Rcvd: 132497 (5.571MB)
```

Task 3.3 - 172.16.1.114

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 08:08 Pacific Daylight Time

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating ARP Ping Scan at 08:08

Scanning 255 hosts [1 port/host]

Completed ARP Ping Scan at 08:08, 1.90s elapsed (255 total hosts)

Initiating Parallel DNS resolution of 3 hosts. at 08:08

Completed Parallel DNS resolution of 3 hosts. at 08:08, 0.00s elapsed

Nmap scan report for 172.16.1.0 [host down]

Nmap scan report for 172.16.1.2 [host down]

Nmap scan report for 172.16.1.3 [host down]

Nmap scan report for 172.16.1.4 [host down]

Nmap scan report for 172.16.1.5 [host down]
Nmap scan report for 172.16.1.6 [host down]
Nmap scan report for 172.16.1.7 [host down]
Nmap scan report for 172.16.1.8 [host down]
Nmap scan report for 172.16.1.9 [host down]
Nmap scan report for 172.16.1.10 [host down]
Nmap scan report for 172.16.1.11 [host down]
Nmap scan report for 172.16.1.12 [host down]
Nmap scan report for 172.16.1.14 [host down]
Nmap scan report for 172.16.1.15 [host down]
Nmap scan report for 172.16.1.16 [host down]
Nmap scan report for 172.16.1.17 [host down]
Nmap scan report for 172.16.1.18 [host down]
Nmap scan report for 172.16.1.19 [host down]
Nmap scan report for 172.16.1.20 [host down]
Nmap scan report for 172.16.1.21 [host down]
Nmap scan report for 172.16.1.22 [host down]
Nmap scan report for 172.16.1.23 [host down]
Nmap scan report for 172.16.1.24 [host down]
Nmap scan report for 172.16.1.25 [host down]
Nmap scan report for 172.16.1.26 [host down]
Nmap scan report for 172.16.1.27 [host down]
Nmap scan report for 172.16.1.28 [host down]
Nmap scan report for 172.16.1.29 [host down]
Nmap scan report for 172.16.1.30 [host down]
Nmap scan report for 172.16.1.31 [host down]
Nmap scan report for 172.16.1.32 [host down]
Nmap scan report for 172.16.1.33 [host down]
Nmap scan report for 172.16.1.34 [host down]
Nmap scan report for 172.16.1.35 [host down]
Nmap scan report for 172.16.1.36 [host down]
Nmap scan report for 172.16.1.37 [host down]
Nmap scan report for 172.16.1.38 [host down]
Nmap scan report for 172.16.1.39 [host down]
Nmap scan report for 172.16.1.40 [host down]
Nmap scan report for 172.16.1.41 [host down]
Nmap scan report for 172.16.1.42 [host down]
Nmap scan report for 172.16.1.43 [host down]
Nmap scan report for 172.16.1.44 [host down]
Nmap scan report for 172.16.1.45 [host down]
Nmap scan report for 172.16.1.46 [host down]
Nmap scan report for 172.16.1.47 [host down]
Nmap scan report for 172.16.1.48 [host down]
Nmap scan report for 172.16.1.49 [host down]
Nmap scan report for 172.16.1.50 [host down]
Nmap scan report for 172.16.1.51 [host down]
Nmap scan report for 172.16.1.52 [host down]
Nmap scan report for 172.16.1.53 [host down]
Nmap scan report for 172.16.1.54 [host down]
Nmap scan report for 172.16.1.55 [host down]
Nmap scan report for 172.16.1.56 [host down]
Nmap scan report for 172.16.1.57 [host down]
Nmap scan report for 172.16.1.58 [host down]
Nmap scan report for 172.16.1.59 [host down]
Nmap scan report for 172.16.1.60 [host down]
Nmap scan report for 172.16.1.61 [host down]
Nmap scan report for 172.16.1.62 [host down]
Nmap scan report for 172.16.1.63 [host down]
Nmap scan report for 172.16.1.64 [host down]
Nmap scan report for 172.16.1.65 [host down]
Nmap scan report for 172.16.1.66 [host down]
Nmap scan report for 172.16.1.67 [host down]
Nmap scan report for 172.16.1.68 [host down]
Nmap scan report for 172.16.1.69 [host down]
Nmap scan report for 172.16.1.70 [host down]
Nmap scan report for 172.16.1.71 [host down]
Nmap scan report for 172.16.1.72 [host down]
Nmap scan report for 172.16.1.73 [host down]
Nmap scan report for 172.16.1.74 [host down]
Nmap scan report for 172.16.1.75 [host down]
Nmap scan report for 172.16.1.76 [host down]
Nmap scan report for 172.16.1.77 [host down]
Nmap scan report for 172.16.1.78 [host down]
Nmap scan report for 172.16.1.79 [host down]
Nmap scan report for 172.16.1.80 [host down]
Nmap scan report for 172.16.1.81 [host down]
Nmap scan report for 172.16.1.82 [host down]
Nmap scan report for 172.16.1.83 [host down]
Nmap scan report for 172.16.1.84 [host down]
Nmap scan report for 172.16.1.85 [host down]
Nmap scan report for 172.16.1.86 [host down]
Nmap scan report for 172.16.1.87 [host down]
Nmap scan report for 172.16.1.88 [host down]
Nmap scan report for 172.16.1.89 [host down]
Nmap scan report for 172.16.1.90 [host down]
Nmap scan report for 172.16.1.91 [host down]
Nmap scan report for 172.16.1.92 [host down]
Nmap scan report for 172.16.1.93 [host down]
Nmap scan report for 172.16.1.94 [host down]

Nmap scan report for 172.16.1.95 [host down]

Nmap scan report for 172.16.1.96 [host down]

Nmap scan report for 172.16.1.97 [host down]

Nmap scan report for 172.16.1.98 [host down]

Nmap scan report for 172.16.1.99 [host down]

Nmap scan report for 172.16.1.100 [host down]

Nmap scan report for 172.16.1.101 [host down]

Nmap scan report for 172.16.1.102 [host down]

Nmap scan report for 172.16.1.103 [host down]

Nmap scan report for 172.16.1.104 [host down]

Nmap scan report for 172.16.1.105 [host down]

Nmap scan report for 172.16.1.106 [host down]

Nmap scan report for 172.16.1.107 [host down]

Nmap scan report for 172.16.1.108 [host down]

Nmap scan report for 172.16.1.109 [host down]

Nmap scan report for 172.16.1.110 [host down]

Nmap scan report for 172.16.1.111 [host down]

Nmap scan report for 172.16.1.112 [host down]

Nmap scan report for 172.16.1.113 [host down]

Nmap scan report for 172.16.1.116 [host down]

Nmap scan report for 172.16.1.117 [host down]

Nmap scan report for 172.16.1.118 [host down]

Nmap scan report for 172.16.1.119 [host down]

Nmap scan report for 172.16.1.120 [host down]

Nmap scan report for 172.16.1.121 [host down]

Nmap scan report for 172.16.1.122 [host down]

Nmap scan report for 172.16.1.123 [host down]

Nmap scan report for 172.16.1.124 [host down]
Nmap scan report for 172.16.1.125 [host down]

Nmap scan report for 172.16.1.126 [host down]

Nmap scan report for 172.16.1.127 [host down]

Nmap scan report for 172.16.1.128 [host down]

Nmap scan report for 172.16.1.129 [host down]

Nmap scan report for 172.16.1.130 [host down]

Nmap scan report for 172.16.1.131 [host down]

Nmap scan report for 172.16.1.132 [host down]

Nmap scan report for 172.16.1.133 [host down]

Nmap scan report for 172.16.1.134 [host down]

Nmap scan report for 172.16.1.135 [host down]

Nmap scan report for 172.16.1.136 [host down]

Nmap scan report for 172.16.1.137 [host down]

Nmap scan report for 172.16.1.138 [host down]

Nmap scan report for 172.16.1.139 [host down]

Nmap scan report for 172.16.1.140 [host down]

Nmap scan report for 172.16.1.141 [host down]

Nmap scan report for 172.16.1.142 [host down]

Nmap scan report for 172.16.1.143 [host down]

Nmap scan report for 172.16.1.144 [host down]

Nmap scan report for 172.16.1.145 [host down]

Nmap scan report for 172.16.1.146 [host down]

Nmap scan report for 172.16.1.147 [host down]

Nmap scan report for 172.16.1.148 [host down]

Nmap scan report for 172.16.1.149 [host down]

Nmap scan report for 172.16.1.150 [host down]

Nmap scan report for 172.16.1.151 [host down]

Nmap scan report for 172.16.1.152 [host down]

Nmap scan report for 172.16.1.153 [host down]
Nmap scan report for 172.16.1.154 [host down]

Nmap scan report for 172.16.1.155 [host down]

Nmap scan report for 172.16.1.156 [host down]

Nmap scan report for 172.16.1.157 [host down]

Nmap scan report for 172.16.1.158 [host down]

Nmap scan report for 172.16.1.159 [host down]

Nmap scan report for 172.16.1.160 [host down]

Nmap scan report for 172.16.1.161 [host down]

Nmap scan report for 172.16.1.162 [host down]

Nmap scan report for 172.16.1.163 [host down]

Nmap scan report for 172.16.1.164 [host down]

Nmap scan report for 172.16.1.165 [host down]

Nmap scan report for 172.16.1.166 [host down]

Nmap scan report for 172.16.1.167 [host down]

Nmap scan report for 172.16.1.168 [host down]

Nmap scan report for 172.16.1.169 [host down]

Nmap scan report for 172.16.1.170 [host down]

Nmap scan report for 172.16.1.171 [host down]

Nmap scan report for 172.16.1.172 [host down]

Nmap scan report for 172.16.1.173 [host down]

Nmap scan report for 172.16.1.174 [host down]

Nmap scan report for 172.16.1.175 [host down]

Nmap scan report for 172.16.1.176 [host down]

Nmap scan report for 172.16.1.177 [host down]

Nmap scan report for 172.16.1.178 [host down]

Nmap scan report for 172.16.1.179 [host down]

Nmap scan report for 172.16.1.180 [host down]

Nmap scan report for 172.16.1.181 [host down]

Nmap scan report for 172.16.1.182 [host down]
Nmap scan report for 172.16.1.183 [host down]
Nmap scan report for 172.16.1.184 [host down]
Nmap scan report for 172.16.1.185 [host down]
Nmap scan report for 172.16.1.186 [host down]
Nmap scan report for 172.16.1.187 [host down]
Nmap scan report for 172.16.1.188 [host down]
Nmap scan report for 172.16.1.189 [host down]
Nmap scan report for 172.16.1.190 [host down]
Nmap scan report for 172.16.1.191 [host down]
Nmap scan report for 172.16.1.192 [host down]
Nmap scan report for 172.16.1.193 [host down]
Nmap scan report for 172.16.1.194 [host down]
Nmap scan report for 172.16.1.195 [host down]
Nmap scan report for 172.16.1.196 [host down]
Nmap scan report for 172.16.1.197 [host down]
Nmap scan report for 172.16.1.198 [host down]
Nmap scan report for 172.16.1.199 [host down]
Nmap scan report for 172.16.1.200 [host down]
Nmap scan report for 172.16.1.201 [host down]
Nmap scan report for 172.16.1.202 [host down]
Nmap scan report for 172.16.1.203 [host down]
Nmap scan report for 172.16.1.204 [host down]
Nmap scan report for 172.16.1.205 [host down]
Nmap scan report for 172.16.1.206 [host down]
Nmap scan report for 172.16.1.207 [host down]
Nmap scan report for 172.16.1.208 [host down]
Nmap scan report for 172.16.1.209 [host down]
Nmap scan report for 172.16.1.210 [host down]
Nmap scan report for 172.16.1.211 [host down]
Nmap scan report for 172.16.1.212 [host down]
Nmap scan report for 172.16.1.213 [host down]
Nmap scan report for 172.16.1.214 [host down]
Nmap scan report for 172.16.1.215 [host down]
Nmap scan report for 172.16.1.216 [host down]
Nmap scan report for 172.16.1.217 [host down]
Nmap scan report for 172.16.1.218 [host down]
Nmap scan report for 172.16.1.219 [host down]
Nmap scan report for 172.16.1.220 [host down]
Nmap scan report for 172.16.1.221 [host down]
Nmap scan report for 172.16.1.222 [host down]
Nmap scan report for 172.16.1.223 [host down]
Nmap scan report for 172.16.1.224 [host down]
Nmap scan report for 172.16.1.225 [host down]
Nmap scan report for 172.16.1.226 [host down]
Nmap scan report for 172.16.1.227 [host down]
Nmap scan report for 172.16.1.228 [host down]
Nmap scan report for 172.16.1.229 [host down]
Nmap scan report for 172.16.1.230 [host down]
Nmap scan report for 172.16.1.231 [host down]
Nmap scan report for 172.16.1.232 [host down]
Nmap scan report for 172.16.1.233 [host down]
Nmap scan report for 172.16.1.234 [host down]
Nmap scan report for 172.16.1.235 [host down]
Nmap scan report for 172.16.1.236 [host down]
Nmap scan report for 172.16.1.237 [host down]
Nmap scan report for 172.16.1.238 [host down]
Nmap scan report for 172.16.1.239 [host down]
Nmap scan report for 172.16.1.240 [host down]
Nmap scan report for 172.16.1.241 [host down]
Nmap scan report for 172.16.1.242 [host down]
Nmap scan report for 172.16.1.243 [host down]
Nmap scan report for 172.16.1.244 [host down]
Nmap scan report for 172.16.1.245 [host down]
Nmap scan report for 172.16.1.246 [host down]
Nmap scan report for 172.16.1.247 [host down]
Nmap scan report for 172.16.1.248 [host down]
Nmap scan report for 172.16.1.249 [host down]
Nmap scan report for 172.16.1.250 [host down]
Nmap scan report for 172.16.1.251 [host down]
Nmap scan report for 172.16.1.252 [host down]
Nmap scan report for 172.16.1.253 [host down]
Nmap scan report for 172.16.1.254 [host down]
Nmap scan report for 172.16.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 08:08
Completed Parallel DNS resolution of 1 host. at 08:08, 0.00s elapsed
Initiating SYN Stealth Scan at 08:08
Scanning 3 hosts [65535 ports/host]
Discovered open port 139/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.114
Discovered open port 80/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.1
Discovered open port 135/tcp on 172.16.1.115
Discovered open port 443/tcp on 172.16.1.114
Discovered open port 443/tcp on 172.16.1.1
Discovered open port 21/tcp on 172.16.1.115
Discovered open port 53/tcp on 172.16.1.1
Discovered open port 445/tcp on 172.16.1.115
```

```
SYN Stealth Scan Timing: About 10.19% done; ETC: 08:13 (0:04:33 remaining)
SYN Stealth Scan Timing: About 28.10% done; ETC: 08:11 (0:02:36 remaining)
SYN Stealth Scan Timing: About 48.98% done; ETC: 08:11 (0:01:35 remaining)
Discovered open port 49667/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 65.83% done; ETC: 08:12 (0:01:20 remaining)
Discovered open port 5985/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 81.26% done; ETC: 08:12 (0:00:42 remaining)
Discovered open port 49668/tcp on 172.16.1.115
Completed SYN Stealth Scan against 172.16.1.114 in 207.97s (2 hosts left)
Completed SYN Stealth Scan against 172.16.1.115 in 208.22s (1 host left)
Completed SYN Stealth Scan at 08:11, 211.97s elapsed (196605 total ports)
Initiating Service scan at 08:11
Scanning 13 services on 3 hosts
Completed Service scan at 08:14, 166.63s elapsed (13 services on 3 hosts)
Initiating OS detection (try #1) against 3 hosts
Retrying OS detection (try #2) against 3 hosts
NSE: Script scanning 3 hosts.
Initiating NSE at 08:14
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 08:15, 43.44s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 1.49s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 0.00s elapsed
Nmap scan report for OPNsense.localdomain (172.16.1.1)
Host is up (0.0018s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE  VERSION
53/tcp  open  domain   Unbound 1.17.1
```

```
| dns-nsid:
|  id.server: OPNsense.localdomain
|_  bind.version: unbound 1.17.1
80/tcp  open  http     OPNsense
|_http-server-header: OPNsense
| fingerprint-strings:
|  FourOhFourRequest:
|    HTTP/1.0 301 Moved Permanently
|    Location: https:///nice%20ports%2C/Trinity.txt.bak
|    Content-Length: 0
|    Connection: close
|    Date: Wed, 14 Aug 2024 15:11:58 GMT
|    Server: OPNsense
|  GenericLines:
|    HTTP/1.0 400 Bad Request
|    Content-Type: text/html
|    Content-Length: 345
|    Connection: close
|    Date: Wed, 14 Aug 2024 15:11:58 GMT
|    Server: OPNsense
|    <?xml version="1.0" encoding="iso-8859-1"?>
|    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|    <head>
|    <title>400 Bad Request</title>
|    </head>
|    <body>
|    <h1>400 Bad Request</h1>
|   </body>
|   </html>
|  GetRequest, HTTPOptions:
|   HTTP/1.0 301 Moved Permanently
|   Location: https:///
|   Content-Length: 0
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:53 GMT
|   Server: OPNsense
|  RTSPRequest:
|   HTTP/1.0 400 Bad Request
|   Content-Type: text/html
|   Content-Length: 345
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:53 GMT
|   Server: OPNsense
|   <?xml version="1.0" encoding="iso-8859-1"?>
|   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|   <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|   <head>
|   <title>400 Bad Request</title>
|   </head>
|   <body>
|   <h1>400 Bad Request</h1>
|   </body>
|_   </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
| http-methods:
```

```
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https OPNsense
|_http-server-header: OPNsense
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Issuer: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-30T20:58:17
| Not valid after:  2024-06-30T20:58:17
| MD5:   7fda:2dce:fbf2:87b4:2732:b165:9f9e:8d03
|_SHA-1: d644:af14:45bb:2f7a:7481:185c:c10d:2265:56f7:75a4
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|   Content-Length: 1494
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:11:59 GMT
|   Server: OPNsense
|   <!doctype html>
|   <html lang="en" class="no-js">
|   <head>
|   <meta charset="UTF-8" />
|   <meta http-equiv="X-UA-Compatible" content="IE=edge">
|   <meta name="robots" content="noindex, nofollow" />
|  HTTPOptions:
|   HTTP/1.0 403 Forbidden
|   Set-Cookie: PHPSESSID=f0abfe275459893038daba3f39c73bd9; path=/; secure; HttpOnly
|   Expires: Thu, 19 Nov 1981 08:52:00 GMT
|   Cache-Control: no-store, no-cache, must-revalidate
|   Pragma: no-cache
|   Content-type: text/html; charset=UTF-8
|   Content-Length: 563
|   Connection: close
|   Date: Wed, 14 Aug 2024 15:12:04 GMT
|   Server: OPNsense
|   <html><head><title>CSRF check failed</title>
|   <script>
|   document ).ready(function() {
|   $.ajaxSetup({
|   'beforeSend': function(xhr) {
|   xhr.setRequestHeader("X-CSRFToken", "OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09" );
|   </script>
|   </head>
|    <body>
|_   <p>CSRF check failed. Your form session may have expired, or you may not have cookies enabled.</p>
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: EDEF051C1ED081894527EAC8509EAC14
|_http-title: Login | OPNsense
|_http-trane-info: Problem with XML parsing of /evox/about
2 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-Port80-TCP:V=7.94%I=7%D=8/14%Time=66BCC939%P=i686-pc-windows-windows%r(
SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20
SF:Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OPNsense\r\n
SF:\r\n")%r(HTTPOptions,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLo
SF:cation:\x20https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\
SF:nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OP
SF:Nsense\r\n\r\n")%r(RTSPRequest,1ED,"HTTP/1\.0\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\
SF:x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nSe
SF:rver:\x20OPNsense\r\n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"iso-8
SF:859-1\"\?>\n<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\
SF:.0\x20Transitional//EN\"\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\"http://
SF:www\.w3\.org/TR/xhtml1/DTD/xhtml1-transitional\.dtd\">\n<html\x20xmlns=
SF:\"http://www\.w3\.org/1999/xhtml\"\x20xml:lang=\"en\"\x20lang=\"en\">\n
SF:\x20<head>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\x20</head>\n
SF:\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</body>\n</html
```

```
SF:>\n")%r(FourOhFourRequest,B3,"HTTP/1\.0\x20301\x20Moved\x20Permanently\
SF:r\nLocation:\x20https:///nice%20ports%2C/Trinity\.txt\.bak\r\nContent-L
SF:ength:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x2020
SF:24\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%r(GenericLines,1
SF:ED,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\
SF:nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\
SF:x20Aug\x202024\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<\?xml\
SF:x20version=\"1\.0\"\x20encoding=\"iso-8859-1\"\?>\n<!DOCTYPE\x20html\x2
SF:0PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Transitional//EN\"\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml
SF:1-transitional\.dtd\">\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml
SF:\"\x20xml:lang=\"en\"\x20lang=\"en\">\n\x20<head>\n\x20\x20<title>400\x
SF:20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20B
SF:ad\x20Request</h1>\n\x20</body>\n</html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94%T=SSL%I=7%D=8/14%Time=66BCC945%P=i686-pc-windows-win
SF:dows%r(GetRequest,88F,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20PHPSESS
SF:ID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/;\x20secure;\x20HttpOnly\
SF:r\nSet-Cookie:\x20PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/
SF:;\x20secure;\x20HttpOnly\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008
SF::52:00\x20GMT\r\nCache-Control:\x20no-store,\x20no-cache,\x20must-reval
SF:idate\r\nPragma:\x20no-cache\r\nContent-Security-Policy:\x20default-src
SF:\x20'self';\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'
SF:;\x20style-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval';\r\nX-Fram
SF:e-Options:\x20SAMEORIGIN\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS
SF:-Protection:\x201;\x20mode=block\r\nReferrer-Policy:\x20same-origin\r\n
SF:Content-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x201494
SF:\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11
SF::59\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!doctype\x20html>\n<html\x20l
```

```
SF:ang=\"en\"\x20class=\"no-js\">\n\x20\x20<head>\n\n\x20\x20\x20\x20<meta
SF:\x20charset=\"UTF-8\"\x20/>\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA
SF:-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x20\x20<meta\x20name=
SF:\"robots\"\x20content=\"noindex,\x20nofollow\"\x20/>\n\x20\x20\x20")%r(
SF:HTTPOptions,394,"HTTP/1\.0\x20403\x20Forbidden\r\nSet-Cookie:\x20PHPSES
SF:SID=f0abfe275459893038daba3f39c73bd9;\x20path=/;\x20secure;\x20HttpOnly
SF:\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\nCache-C
SF:ontrol:\x20no-store,\x20no-cache,\x20must-revalidate\r\nPragma:\x20no-c
SF:ache\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:
SF:\x20563\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x
SF:2015:12:04\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<html><head><title>CSRF
SF:\x20check\x20failed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20<script>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\$\(\x20document\x20\)\.ready\(function\(\)\x20{\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\$\.ajaxSetup\({\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:'beforeSend':\x20function\(xhr\)\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20xhr\.setRequest
SF:Header\(\"X-CSRFToken\",\x20\"OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09\"\x20\);
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}
SF:\);\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\);\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20</script>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20</head>\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>CSRF\x20check\x20
SF:failed\.\x20Your\x20form\x20session\x20may\x20have\x20expired,\x20or\x2
SF:0you\x20may\x20not\x20have\x20cookies\x20enabled\.</p>\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20");
```

```
MAC Address: BC:24:11:0F:90:00 (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): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Aug 14 08:14:37 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.78 ms OPNsense.localdomain (172.16.1.1)

Nmap scan report for 172.16.1.114
Host is up (0.0013s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd (PHP 5.6.21)
|_http-server-header: Apache
|_http-favicon: Unknown favicon MD5: 4B31A3DA81673FA571F35231D2EBB676
|_http-title: HammersHammersHammers
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
| http-robots.txt: 4 disallowed entries
|_/admin/ /core/ /download/ /system/
```

```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open   ssl/http Apache httpd (PHP 5.6.21)
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-05-10T20:03:33
| Not valid after:  2026-05-08T20:03:33
| MD5:   e2c3:a8ef:0eb8:f9d1:bb1a:72c0:178a:b605
|_SHA-1: e0df:7c75:38af:d191:f69c:cec5:908e:f3ae:02c0:9681
| http-robots.txt: 4 disallowed entries
|_/admin/ /core/ /download/ /system/
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
|_http-title: HammersHammersHammers
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: BC:24:11:F8:E0:0F (Unknown)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.16 - 4.6 (95%), Linux 3.2 - 4.9 (94%),
Linux 4.10 (94%), Linux 3.2 - 3.8 (93%), Linux 3.16 (93%), Linux 4.4 (93%), Linux 3.13 (92%),
Linux 5.1 (92%), Linux 3.13 or 4.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Aug 14 08:12:28 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

```
TRACEROUTE

HOP RTT     ADDRESS

1   1.29 ms 172.16.1.114


Nmap scan report for 172.16.1.115

Host is up (0.0014s latency).

Not shown: 65527 filtered tcp ports (no-response)

PORT     STATE SERVICE      VERSION

21/tcp    open  ftp          Microsoft ftpd

| ftp-syst:

|_  SYST: Windows_NT

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip

| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip.6u35iss.partial

| 06-02-2016  08:34PM            205824 international-sales-data-HammerCorpInt.xls

| 06-02-2016  09:11PM               250 LogonHelp.txt

| 06-02-2016  08:36PM            113183 Sacramentorealestatetransactions.csv

| 06-02-2016  08:37PM            123637 SalesJan2009.csv

|_06-02-2016  08:37PM             93536 TechCrunchcontinentalUSA.csv

80/tcp    open  http         Microsoft IIS httpd 10.0

|_http-server-header: Microsoft-IIS/10.0

|_http-title: IIS Windows Server

| http-methods:

|   Supported Methods: OPTIONS TRACE GET HEAD POST

|_  Potentially risky methods: TRACE

135/tcp   open  msrpc        Microsoft Windows RPC

139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn

445/tcp   open  microsoft-ds?

5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49667/tcp open  msrpc        Microsoft Windows RPC

49668/tcp open  msrpc        Microsoft Windows RPC

MAC Address: BC:24:11:50:3B:0E (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 2019 (95%)

Aggressive OS guesses: Microsoft Windows Server 2019 (95%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=262 (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: 2024-08-14T15:14:39

|_  start_date: N/A

| smb2-security-mode:

|   3:1:1:

|_    Message signing enabled but not required

| nbstat: NetBIOS name: HAMMERCORP, NetBIOS user: <unknown>, NetBIOS MAC:
bc:24:11:50:3b:0e (unknown)

| Names:

|   HAMMERCORP<00>       Flags: <unique><active>

|   HAMMERS<00>          Flags: <group><active>
```

```
|_ HAMMERCORP<20>      Flags: <unique><active>

TRACEROUTE
HOP RTT     ADDRESS
1   1.40 ms 172.16.1.115

Initiating SYN Stealth Scan at 08:15
Scanning 172.16.1.13 [65535 ports]
Discovered open port 139/tcp on 172.16.1.13
Discovered open port 135/tcp on 172.16.1.13
Discovered open port 445/tcp on 172.16.1.13
Discovered open port 49665/tcp on 172.16.1.13
Discovered open port 49666/tcp on 172.16.1.13
Discovered open port 49667/tcp on 172.16.1.13
Discovered open port 49671/tcp on 172.16.1.13
Discovered open port 5357/tcp on 172.16.1.13
Discovered open port 5040/tcp on 172.16.1.13
Discovered open port 49668/tcp on 172.16.1.13
Discovered open port 49664/tcp on 172.16.1.13
Completed SYN Stealth Scan at 08:15, 14.00s elapsed (65535 total ports)
Initiating Service scan at 08:15
Scanning 11 services on 172.16.1.13
Service scan Timing: About 45.45% done; ETC: 08:17 (0:01:05 remaining)
Completed Service scan at 08:18, 156.31s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against 172.16.1.13
NSE: Script scanning 172.16.1.13.
Initiating NSE at 08:18
Completed NSE at 08:18, 14.94s elapsed
Initiating NSE at 08:18
```

```
Completed NSE at 08:18, 1.02s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Nmap scan report for 172.16.1.13
Host is up (0.00081s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
135/tcp   open     msrpc        Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
5040/tcp  open     unknown
5357/tcp  open     http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open     msrpc        Microsoft Windows RPC
49665/tcp open     msrpc        Microsoft Windows RPC
49666/tcp open     msrpc        Microsoft Windows RPC
49667/tcp open     msrpc        Microsoft Windows RPC
49668/tcp open     msrpc        Microsoft Windows RPC
49671/tcp open     msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 10
OS details: Microsoft Windows 10 2004
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:

| smb2-time:

|   date: 2024-08-14T15:18:19

|_  start_date: N/A

| smb2-security-mode:

|   3:1:1:

|_    Message signing enabled but not required


NSE: Script Post-scanning.

Initiating NSE at 08:18

Completed NSE at 08:18, 0.00s elapsed

Initiating NSE at 08:18

Completed NSE at 08:18, 0.00s elapsed

Initiating NSE at 08:18

Completed NSE at 08:18, 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.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 622.09 seconds

           Raw packets sent: 459966 (20.242MB) | Rcvd: 132497 (5.571MB)
```

Task 3.4 172.16.1.115

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-14 08:08 Pacific Daylight Time

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed
```

```
Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating NSE at 08:08

Completed NSE at 08:08, 0.00s elapsed

Initiating ARP Ping Scan at 08:08

Scanning 255 hosts [1 port/host]

Completed ARP Ping Scan at 08:08, 1.90s elapsed (255 total hosts)

Initiating Parallel DNS resolution of 3 hosts. at 08:08

Completed Parallel DNS resolution of 3 hosts. at 08:08, 0.00s elapsed

Nmap scan report for 172.16.1.0 [host down]

Nmap scan report for 172.16.1.2 [host down]

Nmap scan report for 172.16.1.3 [host down]

Nmap scan report for 172.16.1.4 [host down]

Nmap scan report for 172.16.1.5 [host down]

Nmap scan report for 172.16.1.6 [host down]

Nmap scan report for 172.16.1.7 [host down]

Nmap scan report for 172.16.1.8 [host down]

Nmap scan report for 172.16.1.9 [host down]

Nmap scan report for 172.16.1.10 [host down]

Nmap scan report for 172.16.1.11 [host down]

Nmap scan report for 172.16.1.12 [host down]

Nmap scan report for 172.16.1.14 [host down]

Nmap scan report for 172.16.1.15 [host down]

Nmap scan report for 172.16.1.16 [host down]

Nmap scan report for 172.16.1.17 [host down]

Nmap scan report for 172.16.1.18 [host down]

Nmap scan report for 172.16.1.19 [host down]

Nmap scan report for 172.16.1.20 [host down]

Nmap scan report for 172.16.1.21 [host down]
Nmap scan report for 172.16.1.22 [host down]
Nmap scan report for 172.16.1.23 [host down]
Nmap scan report for 172.16.1.24 [host down]
Nmap scan report for 172.16.1.25 [host down]
Nmap scan report for 172.16.1.26 [host down]
Nmap scan report for 172.16.1.27 [host down]
Nmap scan report for 172.16.1.28 [host down]
Nmap scan report for 172.16.1.29 [host down]
Nmap scan report for 172.16.1.30 [host down]
Nmap scan report for 172.16.1.31 [host down]
Nmap scan report for 172.16.1.32 [host down]
Nmap scan report for 172.16.1.33 [host down]
Nmap scan report for 172.16.1.34 [host down]
Nmap scan report for 172.16.1.35 [host down]
Nmap scan report for 172.16.1.36 [host down]
Nmap scan report for 172.16.1.37 [host down]
Nmap scan report for 172.16.1.38 [host down]
Nmap scan report for 172.16.1.39 [host down]
Nmap scan report for 172.16.1.40 [host down]
Nmap scan report for 172.16.1.41 [host down]
Nmap scan report for 172.16.1.42 [host down]
Nmap scan report for 172.16.1.43 [host down]
Nmap scan report for 172.16.1.44 [host down]
Nmap scan report for 172.16.1.45 [host down]
Nmap scan report for 172.16.1.46 [host down]
Nmap scan report for 172.16.1.47 [host down]
Nmap scan report for 172.16.1.48 [host down]
Nmap scan report for 172.16.1.49 [host down]
Nmap scan report for 172.16.1.50 [host down]
Nmap scan report for 172.16.1.51 [host down]
Nmap scan report for 172.16.1.52 [host down]
Nmap scan report for 172.16.1.53 [host down]
Nmap scan report for 172.16.1.54 [host down]
Nmap scan report for 172.16.1.55 [host down]
Nmap scan report for 172.16.1.56 [host down]
Nmap scan report for 172.16.1.57 [host down]
Nmap scan report for 172.16.1.58 [host down]
Nmap scan report for 172.16.1.59 [host down]
Nmap scan report for 172.16.1.60 [host down]
Nmap scan report for 172.16.1.61 [host down]
Nmap scan report for 172.16.1.62 [host down]
Nmap scan report for 172.16.1.63 [host down]
Nmap scan report for 172.16.1.64 [host down]
Nmap scan report for 172.16.1.65 [host down]
Nmap scan report for 172.16.1.66 [host down]
Nmap scan report for 172.16.1.67 [host down]
Nmap scan report for 172.16.1.68 [host down]
Nmap scan report for 172.16.1.69 [host down]
Nmap scan report for 172.16.1.70 [host down]
Nmap scan report for 172.16.1.71 [host down]
Nmap scan report for 172.16.1.72 [host down]
Nmap scan report for 172.16.1.73 [host down]
Nmap scan report for 172.16.1.74 [host down]
Nmap scan report for 172.16.1.75 [host down]
Nmap scan report for 172.16.1.76 [host down]
Nmap scan report for 172.16.1.77 [host down]
Nmap scan report for 172.16.1.78 [host down]
Nmap scan report for 172.16.1.79 [host down]
Nmap scan report for 172.16.1.80 [host down]
Nmap scan report for 172.16.1.81 [host down]
Nmap scan report for 172.16.1.82 [host down]
Nmap scan report for 172.16.1.83 [host down]
Nmap scan report for 172.16.1.84 [host down]
Nmap scan report for 172.16.1.85 [host down]
Nmap scan report for 172.16.1.86 [host down]
Nmap scan report for 172.16.1.87 [host down]
Nmap scan report for 172.16.1.88 [host down]
Nmap scan report for 172.16.1.89 [host down]
Nmap scan report for 172.16.1.90 [host down]
Nmap scan report for 172.16.1.91 [host down]
Nmap scan report for 172.16.1.92 [host down]
Nmap scan report for 172.16.1.93 [host down]
Nmap scan report for 172.16.1.94 [host down]
Nmap scan report for 172.16.1.95 [host down]
Nmap scan report for 172.16.1.96 [host down]
Nmap scan report for 172.16.1.97 [host down]
Nmap scan report for 172.16.1.98 [host down]
Nmap scan report for 172.16.1.99 [host down]
Nmap scan report for 172.16.1.100 [host down]
Nmap scan report for 172.16.1.101 [host down]
Nmap scan report for 172.16.1.102 [host down]
Nmap scan report for 172.16.1.103 [host down]
Nmap scan report for 172.16.1.104 [host down]
Nmap scan report for 172.16.1.105 [host down]
Nmap scan report for 172.16.1.106 [host down]
Nmap scan report for 172.16.1.107 [host down]
Nmap scan report for 172.16.1.108 [host down]
Nmap scan report for 172.16.1.109 [host down]

Nmap scan report for 172.16.1.110 [host down]

Nmap scan report for 172.16.1.111 [host down]

Nmap scan report for 172.16.1.112 [host down]

Nmap scan report for 172.16.1.113 [host down]

Nmap scan report for 172.16.1.116 [host down]

Nmap scan report for 172.16.1.117 [host down]

Nmap scan report for 172.16.1.118 [host down]

Nmap scan report for 172.16.1.119 [host down]

Nmap scan report for 172.16.1.120 [host down]

Nmap scan report for 172.16.1.121 [host down]

Nmap scan report for 172.16.1.122 [host down]

Nmap scan report for 172.16.1.123 [host down]

Nmap scan report for 172.16.1.124 [host down]

Nmap scan report for 172.16.1.125 [host down]

Nmap scan report for 172.16.1.126 [host down]

Nmap scan report for 172.16.1.127 [host down]

Nmap scan report for 172.16.1.128 [host down]

Nmap scan report for 172.16.1.129 [host down]

Nmap scan report for 172.16.1.130 [host down]

Nmap scan report for 172.16.1.131 [host down]

Nmap scan report for 172.16.1.132 [host down]

Nmap scan report for 172.16.1.133 [host down]

Nmap scan report for 172.16.1.134 [host down]

Nmap scan report for 172.16.1.135 [host down]

Nmap scan report for 172.16.1.136 [host down]

Nmap scan report for 172.16.1.137 [host down]

Nmap scan report for 172.16.1.138 [host down]

Nmap scan report for 172.16.1.139 [host down]
Nmap scan report for 172.16.1.140 [host down]

Nmap scan report for 172.16.1.141 [host down]

Nmap scan report for 172.16.1.142 [host down]

Nmap scan report for 172.16.1.143 [host down]

Nmap scan report for 172.16.1.144 [host down]

Nmap scan report for 172.16.1.145 [host down]

Nmap scan report for 172.16.1.146 [host down]

Nmap scan report for 172.16.1.147 [host down]

Nmap scan report for 172.16.1.148 [host down]

Nmap scan report for 172.16.1.149 [host down]

Nmap scan report for 172.16.1.150 [host down]

Nmap scan report for 172.16.1.151 [host down]

Nmap scan report for 172.16.1.152 [host down]

Nmap scan report for 172.16.1.153 [host down]

Nmap scan report for 172.16.1.154 [host down]

Nmap scan report for 172.16.1.155 [host down]

Nmap scan report for 172.16.1.156 [host down]

Nmap scan report for 172.16.1.157 [host down]

Nmap scan report for 172.16.1.158 [host down]

Nmap scan report for 172.16.1.159 [host down]

Nmap scan report for 172.16.1.160 [host down]

Nmap scan report for 172.16.1.161 [host down]

Nmap scan report for 172.16.1.162 [host down]

Nmap scan report for 172.16.1.163 [host down]

Nmap scan report for 172.16.1.164 [host down]

Nmap scan report for 172.16.1.165 [host down]

Nmap scan report for 172.16.1.166 [host down]

Nmap scan report for 172.16.1.167 [host down]

Nmap scan report for 172.16.1.168 [host down]
Nmap scan report for 172.16.1.169 [host down]
Nmap scan report for 172.16.1.170 [host down]
Nmap scan report for 172.16.1.171 [host down]
Nmap scan report for 172.16.1.172 [host down]
Nmap scan report for 172.16.1.173 [host down]
Nmap scan report for 172.16.1.174 [host down]
Nmap scan report for 172.16.1.175 [host down]
Nmap scan report for 172.16.1.176 [host down]
Nmap scan report for 172.16.1.177 [host down]
Nmap scan report for 172.16.1.178 [host down]
Nmap scan report for 172.16.1.179 [host down]
Nmap scan report for 172.16.1.180 [host down]
Nmap scan report for 172.16.1.181 [host down]
Nmap scan report for 172.16.1.182 [host down]
Nmap scan report for 172.16.1.183 [host down]
Nmap scan report for 172.16.1.184 [host down]
Nmap scan report for 172.16.1.185 [host down]
Nmap scan report for 172.16.1.186 [host down]
Nmap scan report for 172.16.1.187 [host down]
Nmap scan report for 172.16.1.188 [host down]
Nmap scan report for 172.16.1.189 [host down]
Nmap scan report for 172.16.1.190 [host down]
Nmap scan report for 172.16.1.191 [host down]
Nmap scan report for 172.16.1.192 [host down]
Nmap scan report for 172.16.1.193 [host down]
Nmap scan report for 172.16.1.194 [host down]
Nmap scan report for 172.16.1.195 [host down]
Nmap scan report for 172.16.1.196 [host down]
Nmap scan report for 172.16.1.197 [host down]
Nmap scan report for 172.16.1.198 [host down]
Nmap scan report for 172.16.1.199 [host down]
Nmap scan report for 172.16.1.200 [host down]
Nmap scan report for 172.16.1.201 [host down]
Nmap scan report for 172.16.1.202 [host down]
Nmap scan report for 172.16.1.203 [host down]
Nmap scan report for 172.16.1.204 [host down]
Nmap scan report for 172.16.1.205 [host down]
Nmap scan report for 172.16.1.206 [host down]
Nmap scan report for 172.16.1.207 [host down]
Nmap scan report for 172.16.1.208 [host down]
Nmap scan report for 172.16.1.209 [host down]
Nmap scan report for 172.16.1.210 [host down]
Nmap scan report for 172.16.1.211 [host down]
Nmap scan report for 172.16.1.212 [host down]
Nmap scan report for 172.16.1.213 [host down]
Nmap scan report for 172.16.1.214 [host down]
Nmap scan report for 172.16.1.215 [host down]
Nmap scan report for 172.16.1.216 [host down]
Nmap scan report for 172.16.1.217 [host down]
Nmap scan report for 172.16.1.218 [host down]
Nmap scan report for 172.16.1.219 [host down]
Nmap scan report for 172.16.1.220 [host down]
Nmap scan report for 172.16.1.221 [host down]
Nmap scan report for 172.16.1.222 [host down]
Nmap scan report for 172.16.1.223 [host down]
Nmap scan report for 172.16.1.224 [host down]
Nmap scan report for 172.16.1.225 [host down]
Nmap scan report for 172.16.1.226 [host down]
Nmap scan report for 172.16.1.227 [host down]
Nmap scan report for 172.16.1.228 [host down]
Nmap scan report for 172.16.1.229 [host down]
Nmap scan report for 172.16.1.230 [host down]
Nmap scan report for 172.16.1.231 [host down]
Nmap scan report for 172.16.1.232 [host down]
Nmap scan report for 172.16.1.233 [host down]
Nmap scan report for 172.16.1.234 [host down]
Nmap scan report for 172.16.1.235 [host down]
Nmap scan report for 172.16.1.236 [host down]
Nmap scan report for 172.16.1.237 [host down]
Nmap scan report for 172.16.1.238 [host down]
Nmap scan report for 172.16.1.239 [host down]
Nmap scan report for 172.16.1.240 [host down]
Nmap scan report for 172.16.1.241 [host down]
Nmap scan report for 172.16.1.242 [host down]
Nmap scan report for 172.16.1.243 [host down]
Nmap scan report for 172.16.1.244 [host down]
Nmap scan report for 172.16.1.245 [host down]
Nmap scan report for 172.16.1.246 [host down]
Nmap scan report for 172.16.1.247 [host down]
Nmap scan report for 172.16.1.248 [host down]
Nmap scan report for 172.16.1.249 [host down]
Nmap scan report for 172.16.1.250 [host down]
Nmap scan report for 172.16.1.251 [host down]
Nmap scan report for 172.16.1.252 [host down]
Nmap scan report for 172.16.1.253 [host down]
Nmap scan report for 172.16.1.254 [host down]
Nmap scan report for 172.16.1.255 [host down]
```

```
Initiating Parallel DNS resolution of 1 host. at 08:08

Completed Parallel DNS resolution of 1 host. at 08:08, 0.00s elapsed

Initiating SYN Stealth Scan at 08:08

Scanning 3 hosts [65535 ports/host]

Discovered open port 139/tcp on 172.16.1.115

Discovered open port 80/tcp on 172.16.1.114

Discovered open port 80/tcp on 172.16.1.115

Discovered open port 80/tcp on 172.16.1.1

Discovered open port 135/tcp on 172.16.1.115

Discovered open port 443/tcp on 172.16.1.114

Discovered open port 443/tcp on 172.16.1.1

Discovered open port 21/tcp on 172.16.1.115

Discovered open port 53/tcp on 172.16.1.1

Discovered open port 445/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 10.19% done; ETC: 08:13 (0:04:33 remaining)

SYN Stealth Scan Timing: About 28.10% done; ETC: 08:11 (0:02:36 remaining)

SYN Stealth Scan Timing: About 48.98% done; ETC: 08:11 (0:01:35 remaining)

Discovered open port 49667/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 65.83% done; ETC: 08:12 (0:01:20 remaining)

Discovered open port 5985/tcp on 172.16.1.115

SYN Stealth Scan Timing: About 81.26% done; ETC: 08:12 (0:00:42 remaining)

Discovered open port 49668/tcp on 172.16.1.115

Completed SYN Stealth Scan against 172.16.1.114 in 207.97s (2 hosts left)

Completed SYN Stealth Scan against 172.16.1.115 in 208.22s (1 host left)

Completed SYN Stealth Scan at 08:11, 211.97s elapsed (196605 total ports)

Initiating Service scan at 08:11

Scanning 13 services on 3 hosts

Completed Service scan at 08:14, 166.63s elapsed (13 services on 3 hosts)

Initiating OS detection (try #1) against 3 hosts
```

```
Retrying OS detection (try #2) against 3 hosts
NSE: Script scanning 3 hosts.
Initiating NSE at 08:14
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 08:15, 43.44s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 1.49s elapsed
Initiating NSE at 08:15
Completed NSE at 08:15, 0.00s elapsed
Nmap scan report for OPNsense.localdomain (172.16.1.1)
Host is up (0.0018s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE  VERSION
53/tcp  open  domain   Unbound 1.17.1
| dns-nsid:
|   id.server: OPNsense.localdomain
|_  bind.version: unbound 1.17.1
80/tcp  open  http     OPNsense
|_http-server-header: OPNsense
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 301 Moved Permanently
|     Location: https:///nice%20ports%2C/Trinity.txt.bak
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:58 GMT
|     Server: OPNsense
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
|     Content-Length: 345
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:58 GMT
|     Server: OPNsense
|     <?xml version="1.0" encoding="iso-8859-1"?>
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|     </html>
|   GetRequest, HTTPOptions:
|     HTTP/1.0 301 Moved Permanently
|     Location: https:///
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:53 GMT
|     Server: OPNsense
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
|     Content-Length: 345
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:53 GMT
|    Server: OPNsense
|    <?xml version="1.0" encoding="iso-8859-1"?>
|    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
|    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
|    <head>
|    <title>400 Bad Request</title>
|    </head>
|    <body>
|    <h1>400 Bad Request</h1>
|    </body>
|_    </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https OPNsense
|_http-server-header: OPNsense
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Issuer: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-30T20:58:17
| Not valid after:  2024-06-30T20:58:17
| MD5:   7fda:2dce:fbf2:87b4:2732:b165:9f9e:8d03
|_SHA-1: d644:af14:45bb:2f7a:7481:185c:c10d:2265:56f7:75a4
```

```
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Set-Cookie: PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 1494
|     Connection: close
|     Date: Wed, 14 Aug 2024 15:11:59 GMT
|     Server: OPNsense
|     <!doctype html>
|     <html lang="en" class="no-js">
|     <head>
|     <meta charset="UTF-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta name="robots" content="noindex, nofollow" />
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Set-Cookie: PHPSESSID=f0abfe275459893038daba3f39c73bd9; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|    Cache-Control: no-store, no-cache, must-revalidate
|    Pragma: no-cache
|    Content-type: text/html; charset=UTF-8
|    Content-Length: 563
|    Connection: close
|    Date: Wed, 14 Aug 2024 15:12:04 GMT
|    Server: OPNsense
|    <html><head><title>CSRF check failed</title>
|    <script>
|    document ).ready(function() {
|    $.ajaxSetup({
|    'beforeSend': function(xhr) {
|    xhr.setRequestHeader("X-CSRFToken", "OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09" );
|    </script>
|    </head>
|    <body>
|_    <p>CSRF check failed. Your form session may have expired, or you may not have cookies enabled.</p>
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: EDEF051C1ED081894527EAC8509EAC14
|_http-title: Login | OPNsense
|_http-trane-info: Problem with XML parsing of /evox/about
2 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-Port80-TCP:V=7.94%I=7%D=8/14%Time=66BCC939%P=i686-pc-windows-windows%r(
SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20

SF:Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OPNsense\r\n

SF:\r\n")%r(HTTPOptions,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLo

SF:cation:\x20https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\

SF:nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nServer:\x20OP

SF:Nsense\r\n\r\n")%r(RTSPRequest,1ED,"HTTP/1\.0\x20400\x20Bad\x20Request\

SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20345\r\nConnection:\

SF:x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11:53\x20GMT\r\nSe

SF:rver:\x20OPNsense\r\n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"iso-8

SF:859-1\"\?>\n<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\

SF:.0\x20Transitional//EN\"\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\"http://

SF:www\.w3\.org/TR/xhtml1/DTD/xhtml1-transitional\.dtd\">\n<html\x20xmlns=

SF:\"http://www\.w3\.org/1999/xhtml\"\x20xml:lang=\"en\"\x20lang=\"en\">\n

SF:\x20<head>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\x20</head>\n

SF:\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</body>\n</html

SF:>\n")%r(FourOhFourRequest,B3,"HTTP/1\.0\x20301\x20Moved\x20Permanently\

SF:r\nLocation:\x20https:///nice%20ports%2C/Trinity\.txt\.bak\r\nContent-L

SF:ength:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x2020

SF:24\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n")%r(GenericLines,1

SF:ED,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\r\

SF:nContent-Length:\x20345\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\

SF:x20Aug\x202024\x2015:11:58\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<\?xml\

SF:x20version=\"1\.0\"\x20encoding=\"iso-8859-1\"\?>\n<!DOCTYPE\x20html\x2

SF:0PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Transitional//EN\"\n\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\"http://www\.w3\.org/TR/xhtml1/DTD/xhtml

SF:1-transitional\.dtd\">\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml

SF:\"\x20xml:lang=\"en\"\x20lang=\"en\">\n\x20<head>\n\x20\x20<title>400\x

SF:20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20B

SF:ad\x20Request</h1>\n\x20</body>\n</html>\n");
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.94%T=SSL%I=7%D=8/14%Time=66BCC945%P=i686-pc-windows-win

SF:dows%r(GetRequest,88F,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20PHPSESS

SF:ID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/;\x20secure;\x20HttpOnly\

SF:r\nSet-Cookie:\x20PHPSESSID=b61e05519ed2ea7a2f26fb5503ec1738;\x20path=/

SF:;\x20secure;\x20HttpOnly\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008

SF::52:00\x20GMT\r\nCache-Control:\x20no-store,\x20no-cache,\x20must-reval

SF:idate\r\nPragma:\x20no-cache\r\nContent-Security-Policy:\x20default-src

SF:\x20'self';\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'

SF:;\x20style-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval';\r\nX-Fram

SF:e-Options:\x20SAMEORIGIN\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS

SF:-Protection:\x201;\x20mode=block\r\nReferrer-Policy:\x20same-origin\r\n

SF:Content-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x201494

SF:\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x2015:11

SF::59\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!doctype\x20html>\n<html\x20l

SF:ang=\"en\"\x20class=\"no-js\">\n\x20\x20<head>\n\n\x20\x20\x20\x20<meta

SF:\x20charset=\"UTF-8\"\x20/>\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA

SF:-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x20\x20<meta\x20name=

SF:\"robots\"\x20content=\"noindex,\x20nofollow\"\x20/>\n\x20\x20\x20")%r(

SF:HTTPOptions,394,"HTTP/1\.0\x20403\x20Forbidden\r\nSet-Cookie:\x20PHPSES

SF:SID=f0abfe275459893038daba3f39c73bd9;\x20path=/;\x20secure;\x20HttpOnly

SF:\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\nCache-C

SF:ontrol:\x20no-store,\x20no-cache,\x20must-revalidate\r\nPragma:\x20no-c

SF:ache\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:

SF:\x20563\r\nConnection:\x20close\r\nDate:\x20Wed,\x2014\x20Aug\x202024\x

SF:2015:12:04\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<html><head><title>CSRF

SF:\x20check\x20failed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20<script>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

SF:0\$\(\x20document\x20\)\.ready\(function\(\)\x20{\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\$\.ajaxSetup\({\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:'beforeSend':\x20function\(xhr\)\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20xhr\.setRequest
SF:Header\(\"X-CSRFToken\",\x20\"OWh1cXNpSmd0VVVjVDVuU1BJRDNndz09\"\x20\);
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}
SF:\);\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\);\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20</script>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20</head>\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>CSRF\x20check\x20
SF:failed\.\x20Your\x20form\x20session\x20may\x20have\x20expired,\x20or\x2
SF:0you\x20may\x20not\x20have\x20cookies\x20enabled\.</p>\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20");
MAC Address: BC:24:11:0F:90:00 (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): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Aug 14 08:14:37 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
```

```
HOP RTT     ADDRESS

1   1.78 ms OPNsense.localdomain (172.16.1.1)


Nmap scan report for 172.16.1.114

Host is up (0.0013s latency).

Not shown: 65532 filtered tcp ports (no-response)

PORT    STATE  SERVICE  VERSION

22/tcp  closed ssh

80/tcp  open   http     Apache httpd (PHP 5.6.21)

|_http-server-header: Apache

|_http-favicon: Unknown favicon MD5: 4B31A3DA81673FA571F35231D2EBB676

|_http-title: HammersHammersHammers

|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution

| http-robots.txt: 4 disallowed entries

|_/admin/ /core/ /download/ /system/

| http-methods:

|_  Supported Methods: GET HEAD POST OPTIONS

443/tcp open   ssl/http Apache httpd (PHP 5.6.21)

|_http-server-header: Apache

| ssl-cert: Subject: commonName=www.example.com

| Issuer: commonName=www.example.com

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2016-05-10T20:03:33

| Not valid after:  2026-05-08T20:03:33

| MD5:   e2c3:a8ef:0eb8:f9d1:bb1a:72c0:178a:b605

|_SHA-1: e0df:7c75:38af:d191:f69c:cec5:908e:f3ae:02c0:9681

| http-robots.txt: 4 disallowed entries
```

```
|_/admin/ /core/ /download/ /system/
|_http-generator: AbanteCart v1.2.6 - Open Source eCommerce solution
|_http-title: HammersHammersHammers
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: BC:24:11:F8:E0:0F (Unknown)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.16 - 4.6 (95%), Linux 3.2 - 4.9 (94%), Linux 4.10 (94%), Linux 3.2 - 3.8 (93%), Linux 3.16 (93%), Linux 4.4 (93%), Linux 3.13 (92%), Linux 5.1 (92%), Linux 3.13 or 4.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Wed Aug 14 08:12:28 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.29 ms 172.16.1.114

Nmap scan report for 172.16.1.115
Host is up (0.0014s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip
| 06-02-2016  08:36PM            866400 FL_insurance_sample.csv.zip.6u35iss.partial
| 06-02-2016  08:34PM           205824 international-sales-data-HammerCorpInt.xls
| 06-02-2016  09:11PM              250 LogonHelp.txt
| 06-02-2016  08:36PM           113183 Sacramentorealestatetransactions.csv
| 06-02-2016  08:37PM           123637 SalesJan2009.csv
|_06-02-2016  08:37PM            93536 TechCrunchcontinentalUSA.csv
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
MAC Address: BC:24:11:50:3B:0E (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 2019 (95%)
Aggressive OS guesses: Microsoft Windows Server 2019 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (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: 2024-08-14T15:14:39
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: HAMMERCORP, NetBIOS user: <unknown>, NetBIOS MAC:
bc:24:11:50:3b:0e (unknown)
| Names:
|   HAMMERCORP<00>       Flags: <unique><active>
|   HAMMERS<00>          Flags: <group><active>
|_  HAMMERCORP<20>       Flags: <unique><active>

TRACEROUTE
HOP RTT     ADDRESS
1   1.40 ms 172.16.1.115

Initiating SYN Stealth Scan at 08:15
Scanning 172.16.1.13 [65535 ports]
Discovered open port 139/tcp on 172.16.1.13
Discovered open port 135/tcp on 172.16.1.13
Discovered open port 445/tcp on 172.16.1.13
Discovered open port 49665/tcp on 172.16.1.13
Discovered open port 49666/tcp on 172.16.1.13
Discovered open port 49667/tcp on 172.16.1.13
Discovered open port 49671/tcp on 172.16.1.13

Discovered open port 5357/tcp on 172.16.1.13

Discovered open port 5040/tcp on 172.16.1.13

Discovered open port 49668/tcp on 172.16.1.13

Discovered open port 49664/tcp on 172.16.1.13

Completed SYN Stealth Scan at 08:15, 14.00s elapsed (65535 total ports)

Initiating Service scan at 08:15

Scanning 11 services on 172.16.1.13

Service scan Timing: About 45.45% done; ETC: 08:17 (0:01:05 remaining)

Completed Service scan at 08:18, 156.31s elapsed (11 services on 1 host)

Initiating OS detection (try #1) against 172.16.1.13

NSE: Script scanning 172.16.1.13.

Initiating NSE at 08:18

Completed NSE at 08:18, 14.94s elapsed

Initiating NSE at 08:18

Completed NSE at 08:18, 1.02s elapsed

Initiating NSE at 08:18

Completed NSE at 08:18, 0.00s elapsed

Nmap scan report for 172.16.1.13

Host is up (0.00081s latency).

Not shown: 65523 closed tcp ports (reset)

PORT     STATE    SERVICE      VERSION

135/tcp   open     msrpc        Microsoft Windows RPC

137/tcp   filtered netbios-ns

139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn

445/tcp   open     microsoft-ds?

5040/tcp  open     unknown

5357/tcp  open     http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Service Unavailable
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open   msrpc       Microsoft Windows RPC
49665/tcp open   msrpc       Microsoft Windows RPC
49666/tcp open   msrpc       Microsoft Windows RPC
49667/tcp open   msrpc       Microsoft Windows RPC
49668/tcp open   msrpc       Microsoft Windows RPC
49671/tcp open   msrpc       Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 10
OS details: Microsoft Windows 10 2004
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:
| smb2-time:
|   date: 2024-08-14T15:18:19
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
```

```
Completed NSE at 08:18, 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.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 622.09 seconds

     Raw packets sent: 459966 (20.242MB) | Rcvd: 132497 (5.571MB)
```

Task 4

1. How many hosts were located?

   Four host were located – 172.16.1. 1,114,115, and 13

2. What operating systems did it find?

   172.167.1.1 – FreeBSD

   172.16.1.114 – Linux

   172.16.1.115 Microsoft windows server 2019

   172.16.1.13 Windows 10 2004

3. Which systems had telnet running?

   No host had port 23 open which is the default telnet port

4. Which Ips had FTP running? (Hint: Look for the ports)

   172.16.1.115 had FTP running on port 21

5. What login information was used for FTP?

   FTP service allowed “anonymous” to login

6. What is insecure about this FTP site? (There are two major problems)

   Allowing Anonymous to login to the FTP server without any authentication is a major security risk as well as including the login information over plain text. This should be encrypted.

7. Were there any files found? If so, name them.

   FL_Insurance_Sample.cvs.zip

   FL_Insurance_Sample.cvs.zip.6u35iss.partial

   International-sales-data-HammerCorpInt.xls

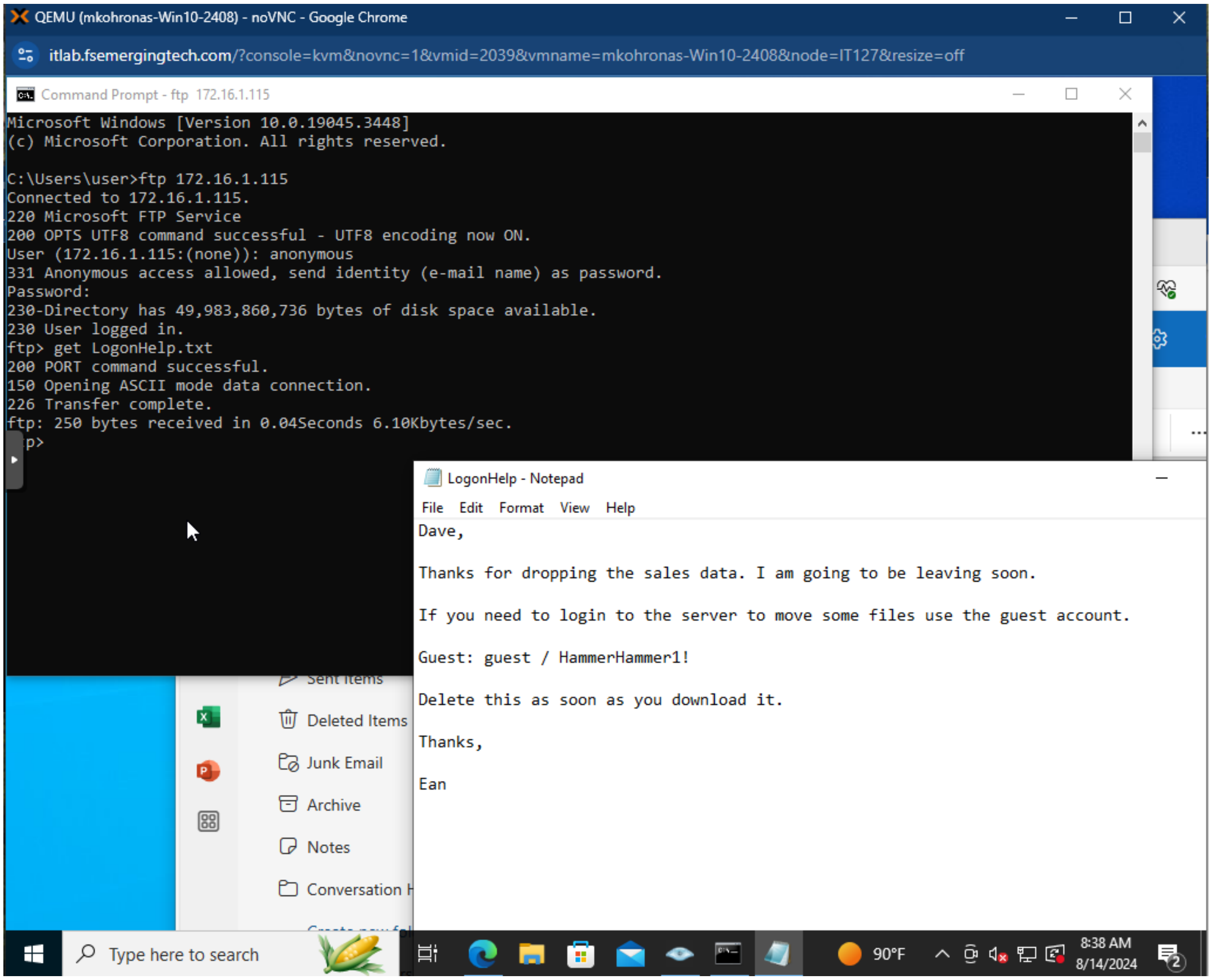
LogonHelp.txt

Sacramentoreleasestatetransacations.csv

SalesJan2009.csv

TechCrunchcontinentalUSA.csv

Bonus: Did you find any files that may have logon information?



QEMU (mkohronas-Win10-2408) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=2039&vmname=mkohronas-Win10-2408&node=IT127&resize=off
Command Prompt - ftp 172.16.1.115
LogonHelp - Notepad
File
Edit
Format
View
Help
Sent Items
Deleted Items
Junk Email
Archive
Notes
Conversation H
Type here to search
90°F
8:38 AM
8/14/2024

```
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ftp 172.16.1.115
Connected to 172.16.1.115.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (172.16.1.115:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Directory has 49,983,860,736 bytes of disk space available.
230 User logged in.
ftp> get LogonHelp.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
ftp: 250 bytes received in 0.04Seconds 6.10Kbytes/sec.
 p>
```

```
Dave,

Thanks for dropping the sales data. I am going to be leaving soon.

If you need to login to the server to move some files use the guest account.

Guest: guest / HammerHammer1!

Delete this as soon as you download it.

Thanks,

Ean
```

Deliverable: Capture the answers in your deliverable document.

Lab Write-up

Write at least one sentence for the following questions related to the lab.

1. Why is scanning your own network important?

   Scanning your own network is important as it views anything that is accessible on your network. This can help detect account information stored improperly and allow an attacker to get into an network if they find an unsecure port.

2. Are there any reasons you shouldn’t scan your own network?

   The only reason not to scan your own network is when the IT security team doesn’t know about it. This could cause a false red flag as the security team may think an attacker is scanning the ports.

3. What other tools could you use to discover information about a system?

   Tools like wireshark, Nessus, and Metasploit can be used to gather detailed information about a system. These tools help assist in finding vulnerabilities and analyzing network traffic

4. Do you think scanning public systems should be a crime? Why or why not?

   I think that scanning a public network should be a crime although with a warning before any serious action. Usually when people are scanning ports is to find stuff that the normal person shouldn’t have access to. So some action should be taken depending on the severity of the event and the number of offenses.