```
Starting Nmap 7.70 ( https://nmap.org ) at 2021-09-13 19:48 CDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:48
Completed NSE at 19:48, 0.00s elapsed
Initiating NSE at 19:48
Completed NSE at 19:48, 0.00s elapsed
Initiating ARP Ping Scan at 19:48
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:49, 2.71s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 19:49
Completed Parallel DNS resolution of 255 hosts. at 19:49, 0.00s elapsed
Nmap scan report for 172.20.1.0 [host down]
Nmap scan report for 172.20.1.2 [host down]
Nmap scan report for 172.20.1.3 [host down]
Nmap scan report for 172.20.1.4 [host down]
Nmap scan report for 172.20.1.5 [host down]
Nmap scan report for 172.20.1.6 [host down]
Nmap scan report for 172.20.1.7 [host down]
Nmap scan report for 172.20.1.8 [host down]
Nmap scan report for 172.20.1.9 [host down]
Nmap scan report for 172.20.1.10 [host down]
Nmap scan report for 172.20.1.11 [host down]
Nmap scan report for 172.20.1.12 [host down]
Nmap scan report for 172.20.1.13 [host down]
Nmap scan report for 172.20.1.14 [host down]
Nmap scan report for 172.20.1.15 [host down]
Nmap scan report for 172.20.1.16 [host down]
Nmap scan report for 172.20.1.17 [host down]
Nmap scan report for 172.20.1.18 [host down]
Nmap scan report for 172.20.1.19 [host down]
Nmap scan report for 172.20.1.20 [host down]
Nmap scan report for 172.20.1.21 [host down]
Nmap scan report for 172.20.1.22 [host down]
Nmap scan report for 172.20.1.23 [host down]
Nmap scan report for 172.20.1.24 [host down]
Nmap scan report for 172.20.1.25 [host down]
Nmap scan report for 172.20.1.26 [host down]
Nmap scan report for 172.20.1.27 [host down]
Nmap scan report for 172.20.1.28 [host down]
Nmap scan report for 172.20.1.29 [host down]
Nmap scan report for 172.20.1.30 [host down]
Nmap scan report for 172.20.1.31 [host down]
Nmap scan report for 172.20.1.32 [host down]
Nmap scan report for 172.20.1.33 [host down]
Nmap scan report for 172.20.1.34 [host down]
Nmap scan report for 172.20.1.35 [host down]
Nmap scan report for 172.20.1.36 [host down]
Nmap scan report for 172.20.1.37 [host down]
Nmap scan report for 172.20.1.38 [host down]
Nmap scan report for 172.20.1.39 [host down]
Nmap scan report for 172.20.1.40 [host down]
```

```
Nmap scan report for 172.20.1.41 [host down]
Nmap scan report for 172.20.1.42 [host down]
Nmap scan report for 172.20.1.43 [host down]
Nmap scan report for 172.20.1.44 [host down]
Nmap scan report for 172.20.1.45 [host down]
Nmap scan report for 172.20.1.46 [host down]
Nmap scan report for 172.20.1.47 [host down]
Nmap scan report for 172.20.1.48 [host down]
Nmap scan report for 172.20.1.49 [host down]
Nmap scan report for 172.20.1.50 [host down]
Nmap scan report for 172.20.1.51 [host down]
Nmap scan report for 172.20.1.52 [host down]
Nmap scan report for 172.20.1.53 [host down]
Nmap scan report for 172.20.1.54 [host down]
Nmap scan report for 172.20.1.55 [host down]
Nmap scan report for 172.20.1.56 [host down]
Nmap scan report for 172.20.1.57 [host down]
Nmap scan report for 172.20.1.58 [host down]
Nmap scan report for 172.20.1.59 [host down]
Nmap scan report for 172.20.1.60 [host down]
Nmap scan report for 172.20.1.61 [host down]
Nmap scan report for 172.20.1.62 [host down]
Nmap scan report for 172.20.1.63 [host down]
Nmap scan report for 172.20.1.64 [host down]
Nmap scan report for 172.20.1.65 [host down]
Nmap scan report for 172.20.1.66 [host down]
Nmap scan report for 172.20.1.67 [host down]
Nmap scan report for 172.20.1.68 [host down]
Nmap scan report for 172.20.1.69 [host down]
Nmap scan report for 172.20.1.70 [host down]
Nmap scan report for 172.20.1.71 [host down]
Nmap scan report for 172.20.1.72 [host down]
Nmap scan report for 172.20.1.73 [host down]
Nmap scan report for 172.20.1.74 [host down]
Nmap scan report for 172.20.1.75 [host down]
Nmap scan report for 172.20.1.76 [host down]
Nmap scan report for 172.20.1.77 [host down]
Nmap scan report for 172.20.1.78 [host down]
Nmap scan report for 172.20.1.79 [host down]
Nmap scan report for 172.20.1.80 [host down]
Nmap scan report for 172.20.1.81 [host down]
Nmap scan report for 172.20.1.82 [host down]
Nmap scan report for 172.20.1.83 [host down]
Nmap scan report for 172.20.1.84 [host down]
Nmap scan report for 172.20.1.85 [host down]
Nmap scan report for 172.20.1.86 [host down]
Nmap scan report for 172.20.1.87 [host down]
Nmap scan report for 172.20.1.88 [host down]
Nmap scan report for 172.20.1.89 [host down]
Nmap scan report for 172.20.1.90 [host down]
Nmap scan report for 172.20.1.91 [host down]
Nmap scan report for 172.20.1.92 [host down]
```

```
Nmap scan report for 172.20.1.93 [host down]
Nmap scan report for 172.20.1.94 [host down]
Nmap scan report for 172.20.1.95 [host down]
Nmap scan report for 172.20.1.96 [host down]
Nmap scan report for 172.20.1.97 [host down]
Nmap scan report for 172.20.1.98 [host down]
Nmap scan report for 172.20.1.99 [host down]
Nmap scan report for 172.20.1.100 [host down]
Nmap scan report for 172.20.1.101 [host down]
Nmap scan report for 172.20.1.102 [host down]
Nmap scan report for 172.20.1.103 [host down]
Nmap scan report for 172.20.1.104 [host down]
Nmap scan report for 172.20.1.105 [host down]
Nmap scan report for 172.20.1.106 [host down]
Nmap scan report for 172.20.1.107 [host down]
Nmap scan report for 172.20.1.108 [host down]
Nmap scan report for 172.20.1.109 [host down]
Nmap scan report for 172.20.1.110 [host down]
Nmap scan report for 172.20.1.111 [host down]
Nmap scan report for 172.20.1.112 [host down]
Nmap scan report for 172.20.1.113 [host down]
Nmap scan report for 172.20.1.114 [host down]
Nmap scan report for 172.20.1.115 [host down]
Nmap scan report for 172.20.1.116 [host down]
Nmap scan report for 172.20.1.117 [host down]
Nmap scan report for 172.20.1.118 [host down]
Nmap scan report for 172.20.1.119 [host down]
Nmap scan report for 172.20.1.120 [host down]
Nmap scan report for 172.20.1.121 [host down]
Nmap scan report for 172.20.1.122 [host down]
Nmap scan report for 172.20.1.123 [host down]
Nmap scan report for 172.20.1.124 [host down]
Nmap scan report for 172.20.1.125 [host down]
Nmap scan report for 172.20.1.126 [host down]
Nmap scan report for 172.20.1.128 [host down]
Nmap scan report for 172.20.1.130 [host down]
Nmap scan report for 172.20.1.133 [host down]
Nmap scan report for 172.20.1.134 [host down]
Nmap scan report for 172.20.1.135 [host down]
Nmap scan report for 172.20.1.137 [host down]
Nmap scan report for 172.20.1.138 [host down]
Nmap scan report for 172.20.1.139 [host down]
Nmap scan report for 172.20.1.140 [host down]
Nmap scan report for 172.20.1.141 [host down]
Nmap scan report for 172.20.1.142 [host down]
Nmap scan report for 172.20.1.143 [host down]
Nmap scan report for 172.20.1.144 [host down]
Nmap scan report for 172.20.1.145 [host down]
Nmap scan report for 172.20.1.146 [host down]
Nmap scan report for 172.20.1.147 [host down]
Nmap scan report for 172.20.1.148 [host down]
Nmap scan report for 172.20.1.149 [host down]
```

```
Nmap scan report for 172.20.1.150 [host down]
Nmap scan report for 172.20.1.151 [host down]
Nmap scan report for 172.20.1.152 [host down]
Nmap scan report for 172.20.1.153 [host down]
Nmap scan report for 172.20.1.154 [host down]
Nmap scan report for 172.20.1.155 [host down]
Nmap scan report for 172.20.1.156 [host down]
Nmap scan report for 172.20.1.157 [host down]
Nmap scan report for 172.20.1.158 [host down]
Nmap scan report for 172.20.1.159 [host down]
Nmap scan report for 172.20.1.160 [host down]
Nmap scan report for 172.20.1.161 [host down]
Nmap scan report for 172.20.1.162 [host down]
Nmap scan report for 172.20.1.163 [host down]
Nmap scan report for 172.20.1.164 [host down]
Nmap scan report for 172.20.1.165 [host down]
Nmap scan report for 172.20.1.166 [host down]
Nmap scan report for 172.20.1.167 [host down]
Nmap scan report for 172.20.1.168 [host down]
Nmap scan report for 172.20.1.169 [host down]
Nmap scan report for 172.20.1.170 [host down]
Nmap scan report for 172.20.1.171 [host down]
Nmap scan report for 172.20.1.172 [host down]
Nmap scan report for 172.20.1.173 [host down]
Nmap scan report for 172.20.1.174 [host down]
Nmap scan report for 172.20.1.175 [host down]
Nmap scan report for 172.20.1.176 [host down]
Nmap scan report for 172.20.1.177 [host down]
Nmap scan report for 172.20.1.178 [host down]
Nmap scan report for 172.20.1.179 [host down]
Nmap scan report for 172.20.1.180 [host down]
Nmap scan report for 172.20.1.181 [host down]
Nmap scan report for 172.20.1.182 [host down]
Nmap scan report for 172.20.1.183 [host down]
Nmap scan report for 172.20.1.184 [host down]
Nmap scan report for 172.20.1.185 [host down]
Nmap scan report for 172.20.1.186 [host down]
Nmap scan report for 172.20.1.187 [host down]
Nmap scan report for 172.20.1.188 [host down]
Nmap scan report for 172.20.1.189 [host down]
Nmap scan report for 172.20.1.190 [host down]
Nmap scan report for 172.20.1.191 [host down]
Nmap scan report for 172.20.1.192 [host down]
Nmap scan report for 172.20.1.193 [host down]
Nmap scan report for 172.20.1.194 [host down]
Nmap scan report for 172.20.1.195 [host down]
Nmap scan report for 172.20.1.196 [host down]
Nmap scan report for 172.20.1.197 [host down]
Nmap scan report for 172.20.1.198 [host down]
Nmap scan report for 172.20.1.199 [host down]
Nmap scan report for 172.20.1.200 [host down]
Nmap scan report for 172.20.1.201 [host down]
```

```
Nmap scan report for 172.20.1.202 [host down]
Nmap scan report for 172.20.1.203 [host down]
Nmap scan report for 172.20.1.204 [host down]
Nmap scan report for 172.20.1.205 [host down]
Nmap scan report for 172.20.1.206 [host down]
Nmap scan report for 172.20.1.207 [host down]
Nmap scan report for 172.20.1.208 [host down]
Nmap scan report for 172.20.1.209 [host down]
Nmap scan report for 172.20.1.210 [host down]
Nmap scan report for 172.20.1.211 [host down]
Nmap scan report for 172.20.1.212 [host down]
Nmap scan report for 172.20.1.213 [host down]
Nmap scan report for 172.20.1.214 [host down]
Nmap scan report for 172.20.1.215 [host down]
Nmap scan report for 172.20.1.216 [host down]
Nmap scan report for 172.20.1.217 [host down]
Nmap scan report for 172.20.1.218 [host down]
Nmap scan report for 172.20.1.219 [host down]
Nmap scan report for 172.20.1.220 [host down]
Nmap scan report for 172.20.1.221 [host down]
Nmap scan report for 172.20.1.222 [host down]
Nmap scan report for 172.20.1.223 [host down]
Nmap scan report for 172.20.1.224 [host down]
Nmap scan report for 172.20.1.225 [host down]
Nmap scan report for 172.20.1.226 [host down]
Nmap scan report for 172.20.1.227 [host down]
Nmap scan report for 172.20.1.228 [host down]
Nmap scan report for 172.20.1.229 [host down]
Nmap scan report for 172.20.1.230 [host down]
Nmap scan report for 172.20.1.231 [host down]
Nmap scan report for 172.20.1.232 [host down]
Nmap scan report for 172.20.1.233 [host down]
Nmap scan report for 172.20.1.234 [host down]
Nmap scan report for 172.20.1.235 [host down]
Nmap scan report for 172.20.1.236 [host down]
Nmap scan report for 172.20.1.237 [host down]
Nmap scan report for 172.20.1.238 [host down]
Nmap scan report for 172.20.1.239 [host down]
Nmap scan report for 172.20.1.240 [host down]
Nmap scan report for 172.20.1.241 [host down]
Nmap scan report for 172.20.1.242 [host down]
Nmap scan report for 172.20.1.243 [host down]
Nmap scan report for 172.20.1.244 [host down]
Nmap scan report for 172.20.1.245 [host down]
Nmap scan report for 172.20.1.246 [host down]
Nmap scan report for 172.20.1.247 [host down]
Nmap scan report for 172.20.1.248 [host down]
Nmap scan report for 172.20.1.249 [host down]
Nmap scan report for 172.20.1.250 [host down]
Nmap scan report for 172.20.1.251 [host down]
Nmap scan report for 172.20.1.252 [host down]
Nmap scan report for 172.20.1.253 [host down]
```

```
Nmap scan report for 172.20.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 19:49
Completed Parallel DNS resolution of 1 host. at 19:49, 0.00s elapsed
Initiating SYN Stealth Scan at 19:49
Scanning 6 hosts [1000 ports/host]
Discovered open port 139/tcp on 172.20.1.131
Discovered open port 110/tcp on 172.20.1.131
Discovered open port 3306/tcp on 172.20.1.131
Discovered open port 443/tcp on 172.20.1.131
Discovered open port 143/tcp on 172.20.1.131
Discovered open port 21/tcp on 172.20.1.131
Discovered open port 22/tcp on 172.20.1.132
Discovered open port 22/tcp on 172.20.1.129
Discovered open port 80/tcp on 172.20.1.129
Discovered open port 22/tcp on 172.20.1.131
Discovered open port 80/tcp on 172.20.1.131
Discovered open port 135/tcp on 172.20.1.131
Discovered open port 25/tcp on 172.20.1.131
Discovered open port 443/tcp on 172.20.1.127
Discovered open port 79/tcp on 172.20.1.131
Discovered open port 22/tcp on 172.20.1.127
Discovered open port 80/tcp on 172.20.1.127
Discovered open port 49153/tcp on 172.20.1.131
Completed SYN Stealth Scan against 172.20.1.129 in 0.72s (5 hosts left)
Completed SYN Stealth Scan against 172.20.1.132 in 0.73s (4 hosts left)
Completed SYN Stealth Scan against 172.20.1.136 in 0.73s (3 hosts left)
Discovered open port 445/tcp on 172.20.1.131
Discovered open port 49155/tcp on 172.20.1.131
Discovered open port 49154/tcp on 172.20.1.131
Discovered open port 49156/tcp on 172.20.1.131
Discovered open port 106/tcp on 172.20.1.131
Discovered open port 49152/tcp on 172.20.1.131
Completed SYN Stealth Scan against 172.20.1.131 in 1.49s (2 hosts left)
Discovered open port 514/tcp on 172.20.1.127
Completed SYN Stealth Scan against 172.20.1.127 in 10.06s (1 host left)
Completed SYN Stealth Scan at 19:49, 10.17s elapsed (6000 total ports)
Initiating Service scan at 19:49
Scanning 25 services on 6 hosts
Completed Service scan at 19:51, 151.15s elapsed (25 services on 6 hosts)
Initiating OS detection (try #1) against 6 hosts
Retrying OS detection (try #2) against 3 hosts
Retrying OS detection (try #3) against 172.20.1.132
Retrying OS detection (try #4) against 172.20.1.132
Retrying OS detection (try #5) against 172.20.1.132
NSE: Script scanning 6 hosts.
Initiating NSE at 19:51
Completed NSE at 19:52, 33.05s elapsed
Initiating NSE at 19:52
Completed NSE at 19:52, 1.04s elapsed
Nmap scan report for 172.20.1.127
Host is up (0.0032s latency).
Not shown: 996 filtered ports
```

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.7p1 (protocol 2.0)
| ssh-hostkey:
|_  2048 e0:9f:21:98:29:b7:d3:43:e1:40:5e:23:34:17:3d:f7 (RSA)
80/tcp  open  http     Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://172.20.1.127/
443/tcp open  ssl/http Apache httpd
|_http-favicon: Unknown favicon MD5: D2506DE914F9B03553C4BCDC7B6EB614
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
| http-title:  AlienVault OSSIM
|_Requested resource was session/login.php
| ssl-cert: Subject: commonName=alienvault
| Issuer: commonName=alienvault
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-07-16T04:14:13
| Not valid after:  2029-07-13T04:14:13
| MD5:   fb6d 0b01 f635 fb40 94b2 bdd4 8f2f 8cd9
|_SHA-1: 7be0 deb7 fca9 0543 79d2 bd07 a327 4263 674c f95e
|_ssl-date: TLS randomness does not represent time
514/tcp open  shell?
MAC Address: 00:0C:29:91:74:D5 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 ope
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.12 - 4.10
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   3.25 ms 172.20.1.127

Nmap scan report for 172.20.1.129
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:4c:39:29:36:a0:45:68:b4:77:fa:52:e1:cd:b1:fe (RSA)
|   256 da:76:1e:16:7f:a6:8a:eb:9b:5e:93:28:28:80:aa:de (ECDSA)
|_  256 01:ef:2b:67:2b:3b:d6:1d:3e:11:6d:2c:5c:2a:5d:c3 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
```

```
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:71:17:81 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 32.488 days (since Thu Aug 12 08:09:12 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.09 ms 172.20.1.129

Nmap scan report for 172.20.1.131
Host is up (0.0016s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp    open  ssh          Bitvise WinSSHD 8.39 (FlowSsh 8.38; protocol 2.0; non
| ssh-hostkey:
|   3072 03:2c:15:69:8a:e1:1f:c0:f2:3f:db:66:5b:01:a0:f3 (RSA)
|_  384 3f:b5:2a:7b:fa:64:97:ff:9f:f0:95:8f:30:9a:28:03 (ECDSA)
25/tcp    open  smtp         Mercury/32 smtpd (Mail server account Maiser)
|_smtp-commands: localhost Hello nmap.scanme.org; ESMTPs are:, TIME,
79/tcp    open  finger       Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator\x0D
| \x0D
|_[No profile information]\x0D
80/tcp    open  http         Apache httpd 2.4.37 ((Win32) OpenSSL/1.0.2p PHP/7.0.3
|_http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
| http-title: Welcome to XAMPP
|_Requested resource was http://172.20.1.131/dashboard/
106/tcp   open  pop3pw       Mercury/32 poppass service
110/tcp   open  pop3         Mercury/32 pop3d
|_pop3-capabilities: APOP TOP USER EXPIRE(NEVER) UIDL
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         Mercury/32 imapd 4.62
|_imap-capabilities: X-MERCURY-1A0001 complete AUTH=PLAIN CAPABILITY IMAP4rev1 OK
443/tcp   open  ssl/http     Apache httpd 2.4.37 ((Win32) OpenSSL/1.0.2p PHP/7.0.3
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-methods:
```

```
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
| http-title: Welcome to XAMPP
|_Requested resource was https://172.20.1.131/dashboard/
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
```

```
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
```

```
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
|    http/1.1
```

```
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|   http/1.1
|_  http/1.1
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (
3306/tcp  open  mysql        MariaDB (unauthorized)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:E1:3E:41 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:micro
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server
Uptime guess: 0.601 days (since Mon Sep 13 05:27:38 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: localhost, UCERTIFY-PC; OS: Windows; CPE: cpe:/o:microsoft:wi

Host script results:
|_clock-skew: mean: 2h19m58s, deviation: 4h02m30s, median: -1s
| nbstat: NetBIOS name: UCERTIFY-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:2
| Names:
|   UCERTIFY-PC<20>      Flags: <unique><active>
|   UCERTIFY-PC<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
```

```
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: uCertify-PC
|   NetBIOS computer name: UCERTIFY-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-13T17:51:55-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-09-13 19:51:56
|_  start_date: 2020-01-24 06:51:37

TRACEROUTE
HOP RTT     ADDRESS
1   1.58 ms 172.20.1.131

Nmap scan report for 172.20.1.132
Host is up (0.00073s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3 (protocol 2.0)
MAC Address: 00:0C:29:28:12:F4 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nm
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=9/13%OT=22%CT=1%CU=30175%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=613FF24D%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=3%ISR=10A%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Uptime guess: 2.138 days (since Sat Sep 11 16:33:50 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
```

```
1   0.73 ms 172.20.1.132

Nmap scan report for 172.20.1.136
Host is up (0.0017s latency).
All 1000 scanned ports on 172.20.1.136 are closed
MAC Address: 00:0C:29:5B:2F:D1 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.70 ms 172.20.1.136

Nmap scan report for 172.20.1.254
Host is up (0.00097s latency).
All 1000 scanned ports on 172.20.1.254 are filtered
MAC Address: 00:0C:29:91:74:D5 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.97 ms 172.20.1.254

Initiating SYN Stealth Scan at 19:52
Scanning 172.20.1.1 [1000 ports]
Discovered open port 443/tcp on 172.20.1.1
Discovered open port 80/tcp on 172.20.1.1
Discovered open port 23/tcp on 172.20.1.1
Discovered open port 902/tcp on 172.20.1.1
Completed SYN Stealth Scan at 19:52, 0.09s elapsed (1000 total ports)
Initiating Service scan at 19:52
Scanning 4 services on 172.20.1.1
Completed Service scan at 19:54, 134.93s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 172.20.1.1
NSE: Script scanning 172.20.1.1.
Initiating NSE at 19:54
Completed NSE at 19:55, 60.31s elapsed
Initiating NSE at 19:55
Completed NSE at 19:55, 0.00s elapsed
Nmap scan report for 172.20.1.1
Host is up (0.00010s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE         VERSION
23/tcp  open  ssh             OpenSSH 7.8p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   2048 96:fa:64:53:99:6b:94:e8:e3:4d:29:99:05:56:a6:4e (RSA)
|   256 cc:88:e1:53:c0:61:fd:4a:c3:ca:80:8e:8b:34:f5:ed (ECDSA)
|_  256 35:f3:93:d0:fd:97:f2:1b:5d:7a:7f:62:0a:78:21:a6 (ED25519)
80/tcp  open  http            Apache httpd 2.4.34 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
```

```
|_http-server-header: Apache/2.4.34 (Debian)
|_http-title: Apache2 Debian Default Page: It works
443/tcp open  ssl/https
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Date: Tue, 14 Sep 2021 00:52:42 GMT
|     Connection: close
|     Content-Security-Policy: block-all-mixed-content
|     Content-Type: text/plain; charset=utf-8
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: DENY
|     Content-Length: 0
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Date: Tue, 14 Sep 2021 00:52:42 GMT
|     Connection: close
|     Content-Security-Policy: block-all-mixed-content
|     Content-Type: text/plain; charset=utf-8
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: DENY
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.1 501 Not Implemented
|     Date: Tue, 14 Sep 2021 00:52:42 GMT
|     Connection: close
|     Content-Security-Policy: block-all-mixed-content
|     Content-Type: text/plain; charset=utf-8
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: DENY
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Tue, 14 Sep 2021 00:52:52 GMT
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 50
|     <HTML><BODY><H1>400 Bad Request</H1></BODY></HTML>
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Date: Tue, 14 Sep 2021 00:53:54 GMT
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 50
|_    <HTML><BODY><H1>400 Bad Request</H1></BODY></HTML>
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| ssl-cert: Subject: commonName=VMware/countryName=US
```

```
| Issuer: commonName=VMware/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-09T04:25:55
| Not valid after:  2019-10-09T04:25:55
| MD5:   b556 d86d 2458 9f1d 4d82 47d8 0128 f4b3
|_SHA-1: c327 2ed1 57a8 70a7 3fd7 df19 d513 0cde b7f3 d5af
|_ssl-date: TLS randomness does not represent time
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
1 service unrecognized despite returning data. If you know the service/version, pl
SF-Port443-TCP:V=7.70%T=SSL%I=7%D=9/13%Time=613FF25A%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,125,"HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x20Tue,\x2014
SF:\x20Sep\x202021\x2000:52:42\x20GMT\r\nConnection:\x20close\r\nContent-S
SF:ecurity-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text/pla
SF:in;\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\
SF:r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nCo
SF:ntent-Length:\x200\r\n\r\n")%r(HTTPOptions,12B,"HTTP/1\.1\x20501\x20Not
SF:\x20Implemented\r\nDate:\x20Tue,\x2014\x20Sep\x202021\x2000:52:42\x20GM
SF:T\r\nConnection:\x20close\r\nContent-Security-Policy:\x20block-all-mixe
SF:d-content\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nStrict-Tr
SF:ansport-Security:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nos
SF:niff\r\nX-Frame-Options:\x20DENY\r\nContent-Length:\x200\r\n\r\n")%r(Fo
SF:urOhFourRequest,125,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\
SF:x2014\x20Sep\x202021\x2000:52:42\x20GMT\r\nConnection:\x20close\r\nCont
SF:ent-Security-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20tex
SF:t/plain;\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=3153
SF:6000\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\
SF:r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,B3,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\nDate:\x20Tue,\x2014\x20Sep\x202021\x2000:52:52\x20GM
SF:T\r\nConnection:\x20close\r\nContent-Type:\x20text/html\r\nContent-Leng
SF:th:\x2050\r\n\r\n<HTML><BODY><H1>400\x20Bad\x20Request</H1></BODY></HTM
SF:L>")%r(SIPOptions,B3,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Tu
SF:e,\x2014\x20Sep\x202021\x2000:53:54\x20GMT\r\nConnection:\x20close\r\nC
SF:ontent-Type:\x20text/html\r\nContent-Length:\x2050\r\n\r\n<HTML><BODY><
SF:H1>400\x20Bad\x20Request</H1></BODY></HTML>");
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.14
Uptime guess: 7.877 days (since Sun Sep  5 22:53:35 2021)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 19:55
Completed NSE at 19:55, 0.00s elapsed
Initiating NSE at 19:55
Completed NSE at 19:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
OS and Service detection performed. Please report any incorrect results at https:/
Nmap done: 256 IP addresses (7 hosts up) scanned in 410.05 seconds
           Raw packets sent: 9758 (435.178KB) | Rcvd: 6205 (260.800KB)
```