

Meghana Vinjam
18BCN7070

Nmap

Scan a System with Hostname and Ip Address

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans |
nmap vitap.ac.in 67.222.140.114

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 16:28 IST
Nmap scan report for vitap.ac.in (67.222.140.114)
Host is up (0.10s latency).
rDNS record for 67.222.140.114: ailsh2.auroinfotech.com
Not shown: 985 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    closed ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp  closed https-alt

Nmap scan report for ailsh2.auroinfotech.com (67.222.140.114)
Host is up (0.10s latency).
Not shown: 985 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    closed ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp  closed https-alt
```

Scan using Ip Address

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans |
nmap 67.222.140.114

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 16:30 IST
Nmap scan report for ailsh2.auroinfotech.com (67.222.140.114)
Host is up (0.11s latency).
Not shown: 985 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    closed ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp  closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 21.05 seconds
```

“-v” option

```
nmap -v vitap.ac.in

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 16:32 IST
Initiating Ping Scan at 16:32
Scanning vitap.ac.in (67.222.140.114) [4 ports]
Completed Ping Scan at 16:32, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:32
Completed Parallel DNS resolution of 1 host. at 16:32, 0.00s elapsed
Initiating SYN Stealth Scan at 16:32
Scanning vitap.ac.in (67.222.140.114) [1000 ports]
Discovered open port 993/tcp on 67.222.140.114
Discovered open port 110/tcp on 67.222.140.114
Discovered open port 53/tcp on 67.222.140.114
Discovered open port 587/tcp on 67.222.140.114
Discovered open port 443/tcp on 67.222.140.114
Discovered open port 143/tcp on 67.222.140.114
Discovered open port 995/tcp on 67.222.140.114
Discovered open port 21/tcp on 67.222.140.114
Discovered open port 80/tcp on 67.222.140.114
Discovered open port 25/tcp on 67.222.140.114
Discovered open port 26/tcp on 67.222.140.114
Discovered open port 465/tcp on 67.222.140.114
Completed SYN Stealth Scan at 16:32, 20.54s elapsed (1000 total ports)
Nmap scan report for vitap.ac.in (67.222.140.114)
Host is up (0.12s latency).
rDNS record for 67.222.140.114: ailsh2.auroinfotech.com
Not shown: 985 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    closed ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8443/tcp  closed https-alt

Read data files from: /usr/local/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.32 seconds
Raw packets sent: 2001 (87.972KB) | Rcvd: 30 (1.240KB)
```

Scan a whole Subnet

nmap 192.168.43.0/24

```
Nmap scan report for 192.168.43.177
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.43.177 are filtered

Nmap scan report for 192.168.43.178
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.43.178 are filtered

Nmap scan report for 192.168.43.179
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.43.179 are filtered

Nmap scan report for 192.168.43.180
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.43.180 are filtered

Nmap scan report for 192.168.43.181
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.181 are filtered

Nmap scan report for 192.168.43.182
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.43.182 are filtered

Nmap scan report for 192.168.43.183
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.183 are filtered

Nmap scan report for 192.168.43.184
Host is up (0.052s latency).
All 1000 scanned ports on 192.168.43.184 are filtered

Nmap scan report for 192.168.43.185
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.43.185 are filtered

Nmap scan report for 192.168.43.186
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.186 are filtered

Nmap scan report for 192.168.43.187
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.187 are filtered

Nmap scan report for 192.168.43.188
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.188 are filtered

Nmap scan report for 192.168.43.189
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.43.189 are filtered

Nmap scan report for 192.168.43.190
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.190 are filtered

Nmap scan report for 192.168.43.191
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.43.191 are filtered
```

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -sn 192.168.43.0/24				
<pre> Nmap scan report for 192.168.43.226 Host is up (0.021s latency). Nmap scan report for 192.168.43.227 Host is up (0.023s latency). Nmap scan report for 192.168.43.228 Host is up (0.021s latency). Nmap scan report for 192.168.43.229 Host is up (0.022s latency). Nmap scan report for 192.168.43.230 Host is up (0.023s latency). Nmap scan report for 192.168.43.231 Host is up (0.022s latency). Nmap scan report for 192.168.43.232 Host is up (0.023s latency). Nmap scan report for 192.168.43.233 Host is up (0.023s latency). Nmap scan report for 192.168.43.234 Host is up (0.022s latency). Nmap scan report for 192.168.43.235 Host is up (0.024s latency). Nmap scan report for 192.168.43.236 Host is up (0.024s latency). Nmap scan report for 192.168.43.237 Host is up (0.024s latency). Nmap scan report for 192.168.43.238 Host is up (0.027s latency). Nmap scan report for 192.168.43.239 Host is up (0.026s latency). Nmap scan report for 192.168.43.240 Host is up (0.025s latency). Nmap scan report for 192.168.43.241 Host is up (0.025s latency). Nmap scan report for 192.168.43.242 Host is up (0.029s latency). Nmap scan report for 192.168.43.243 Host is up (0.030s latency). Nmap scan report for 192.168.43.244 Host is up (0.029s latency). Nmap scan report for 192.168.43.245 Host is up (0.030s latency). Nmap scan report for 192.168.43.246 Host is up (0.025s latency). Nmap scan report for 192.168.43.247 Host is up (0.068s latency). Nmap scan report for 192.168.43.248 Host is up (0.068s latency). Nmap scan report for 192.168.43.249 Host is up (0.023s latency). Nmap scan report for 192.168.43.250 Host is up (0.022s latency). Nmap scan report for 192.168.43.251 Host is up (0.022s latency). Nmap scan report for 192.168.43.252 Host is up (0.024s latency). Nmap scan report for 192.168.43.253 Host is up (0.030s latency). Nmap scan report for 192.168.43.254 Host is up (0.020s latency). Nmap scan report for 192.168.43.255 Host is up (0.020s latency). Nmap done: 256 IP addresses (256 hosts up) scanned in 71.90 seconds </pre>				

Scan Multiple Servers using last octet of Ip address

Services

▼

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

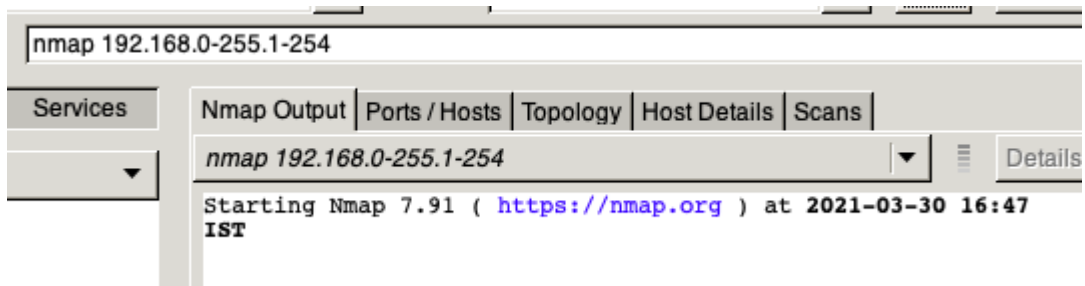
nmap 192.168.0-255.1-254

▼

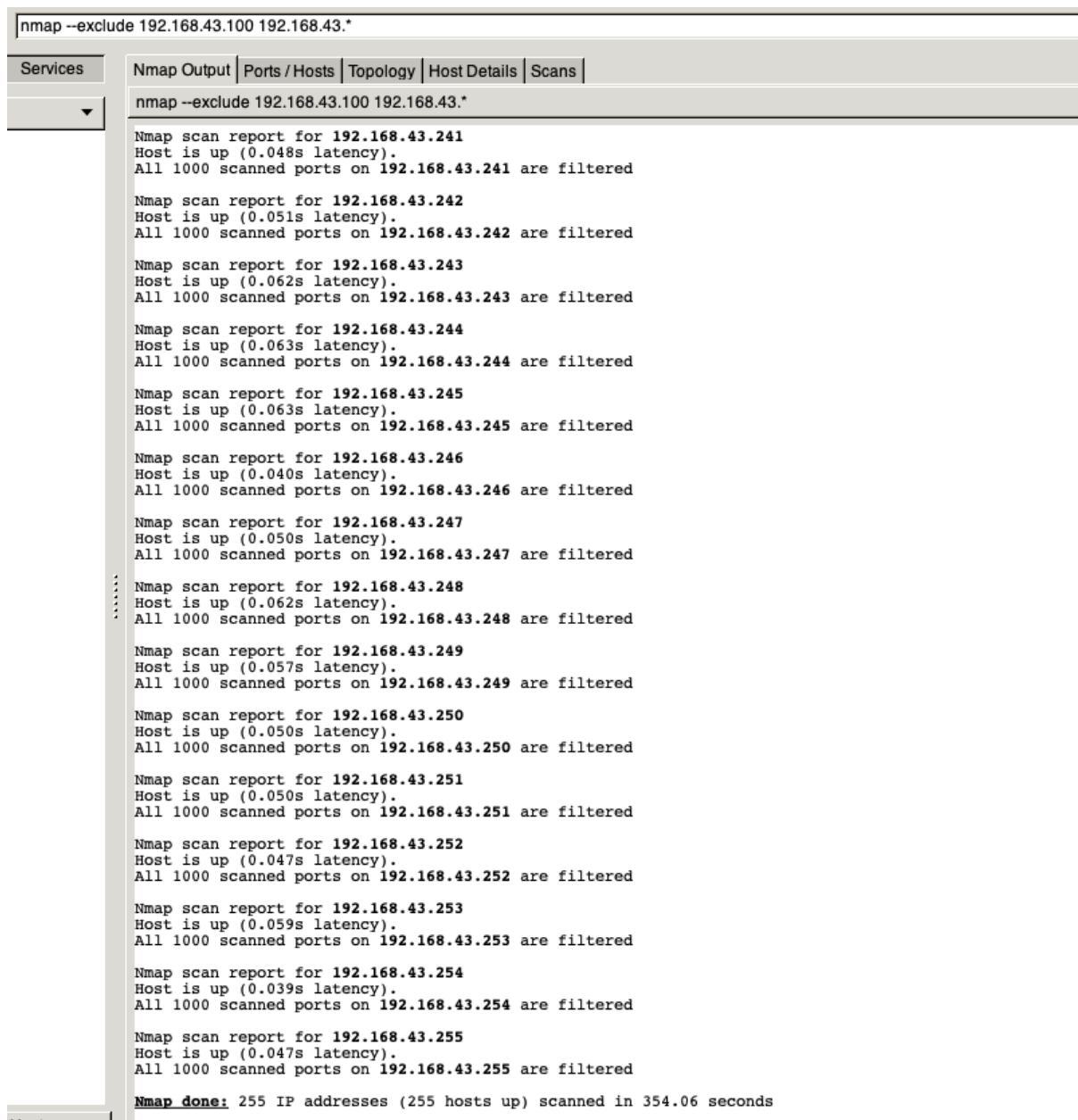
Details

Starting Nmap 7.91 (<https://nmap.org>) at 2021-03-30 16:44 IST

Scan an IP Address Range



Scan Network Excluding Remote Hosts



Scan OS information and Traceroute

Nmap Output | Ports / Hosts | Topology | Host Details | Scans |

nmap -A vtop.vitap.ac.in

http-title: HTTP Status 404 \xe2\x80\x93 Not Found
Requested resource was https://vtop.vitap.ac.in/vtop
ssl-cert: Subject: commonName=.vitap.ac.in
Subject Alternative Name: DNS:*.vitap.ac.in, DNS:vitap.ac.in
Not valid before: 2020-08-05T00:00:00
Not valid after: 2022-08-05T23:59:59
ssl-date: 2021-03-30T11:28:13+00:00; 0s from scanner time.

465/tcp closed smtps
993/tcp open tcpwrapped
995/tcp open tcpwrapped
8080/tcp closed http-proxy

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCPIP-v7.9180-SSLAI=74d3/3/3047Time=60630B2F4px86 64-apple-darwin
SF117.7.00r(GetRequest,EC,"HTTP/1.1\x20302\x20\r\nCache-Control:\x20Priva
SF1te\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2005:30:00\x20IST\r\nLocat
SF1ion:\x20https://vtop.vitap.ac.in/vtop\r\nContent-Type:\x20text/html;
SF1charset=UTF-8\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2030\x20Mar\x20
SF12021\x2011:27:43\x20GMT\r\nConnection:\x20close\r\n\r\n")&r(HTTPOptions
SF1,530,"HTTP/1.1\x20405\x20\r\nCache-Control:\x20private\r\nExpires:\x20
SF1Thu,\x2001\x20Jan\x201970\x2005:30:00\x20IST\r\nContent-Type:\x20text/h
SF1tml; charset=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x201108
SF1\r\nDate:\x20Tue,\x2030\x20Mar\x202021\x2011:27:43\x20GMT\r\nConnection
SF1:\x20close\r\n\r\n<doctype\x20html><html\x20lang=en><head<title>H
SF1HTTP\x20status\x20405\x20\x20\x20\x20\x20Method\x20Not\x20Allowed</title
SF1><style\x20type=text/css>h1\x20{font-family:Tahoma,Arial,sans-serif
SF1;color:white;background-color:#525D76;font-size:22px;}\x20h2\x20{font-f
SF1amily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font
SF1-size:16px;}\x20h3\x20{font-family:Tahoma,Arial,sans-serif;color:white;
SF1;background-color:#525D76;font-size:14px;}\x20body\x20{font-family:Tahom
SF1s,Arial,sans-serif;color:black;background-color:white;}\x20b\x20{font-f
SF1amily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}\x2
SF1p\x20{font-family:Tahoma,Arial,sans-serif;background-color:white;color:black
SF1;font-size:12px;}\x20a\x20{color:black;}\x20a.name\x20{color:black;}\x
SF120b.in"&r(Four0Fourrequest,530,"HTTP/1.1\x20404\x20\r\nCache-Contro
SF1l:\x20private\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2005:30:00\x20I
SF1ST\r\nContent-Type:\x20text/html; charset=utf-8\r\nContent-Language:\x20
SF1en\r\nContent-Length:\x201108\r\nDate:\x20Tue,\x2030\x20Mar\x202021\x20
SF111:27:43\x20GMT\r\nConnection:\x20close\r\n\r\n<doctype\x20html><html
SF1\x20lang=en><head<title>HTTP\x20status\x20404\x20\x20\x20\x20\x20No
SF1t\x20Found</title><style\x20type=text/css>h1\x20{font-family:Tahoma
SF1,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
SF1\x20h2\x20{font-family:Tahoma,Arial,sans-serif;color:white;background-c
SF1olor:#525D76;font-size:16px;}\x20h3\x20{font-family:Tahoma,Arial,sans-s
SF1erif;color:white;background-color:#525D76;font-size:14px;}\x20body\x20{
SF1font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;
SF1}\x20b\x20{font-family:Tahoma,Arial,sans-serif;color:white;background-c
SF1olor:#525D76;}\x20p\x20{font-family:Tahoma,Arial,sans-serif;background:
SF1white;color:black;font-size:12px;}\x20a\x20{color:black;}\x20a.name\x2
SF10{color:black;}\x20b.in"&line\x20height";
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -ssu
No OS matches for host
Network Distance: 3 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 4.60 ms 192.168.55.1
2 24.29 ms 10.0.0.1
3 23.27 ms 117.213.200.8

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.40 seconds

Scan a Hst to Detect Firewall

Nmap Output | Ports / Hosts | Topology | Host Details | Scans |

nmap -sA 192.168.43.96

Starting Nmap 7.91 (https://nmap.org) at 2021-03-30 17:03 IST
Nmap scan report for 192.168.43.96
Host is up (0.028s latency).
Not shown: 998 unfiltered ports
PORT STATE SERVICE
179/tcp filtered bgp
646/tcp filtered ldp

Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds

Scan a Host to check its protected by Firewall

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -Pn 192.168.43.96				
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower. Starting Nmap 7.91 (https://nmap.org) at 2021-03-30 17:03 IST Nmap scan report for 192.168.43.96 Host is up. All 1000 scanned ports on 192.168.43.96 are filtered Nmap done: 1 IP address (1 host up) scanned in 202.49 seconds				

11. Find out Live hosts in a Network

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -sn 192.168.43.*				
Nmap scan report for 192.168.43.226 Host is up (0.029s latency). Nmap scan report for 192.168.43.227 Host is up (0.030s latency). Nmap scan report for 192.168.43.228 Host is up (0.030s latency). Nmap scan report for 192.168.43.229 Host is up (0.030s latency). Nmap scan report for 192.168.43.230 Host is up (0.029s latency). Nmap scan report for 192.168.43.231 Host is up (0.029s latency). Nmap scan report for 192.168.43.232 Host is up (0.029s latency). Nmap scan report for 192.168.43.233 Host is up (0.020s latency). Nmap scan report for 192.168.43.234 Host is up (0.023s latency). Nmap scan report for 192.168.43.235 Host is up (0.025s latency). Nmap scan report for 192.168.43.236 Host is up (0.025s latency). Nmap scan report for 192.168.43.237 Host is up (0.025s latency). Nmap scan report for 192.168.43.238 Host is up (0.026s latency). Nmap scan report for 192.168.43.239 Host is up (0.026s latency). Nmap scan report for 192.168.43.240 Host is up (0.027s latency). Nmap scan report for 192.168.43.241 Host is up (0.032s latency). Nmap scan report for 192.168.43.242 Host is up (0.032s latency). Nmap scan report for 192.168.43.243 Host is up (0.027s latency). Nmap scan report for 192.168.43.244 Host is up (0.028s latency). Nmap scan report for 192.168.43.245 Host is up (0.033s latency). Nmap scan report for 192.168.43.246 Host is up (0.034s latency). Nmap scan report for 192.168.43.247 Host is up (0.023s latency). Nmap scan report for 192.168.43.248 Host is up (0.023s latency). Nmap scan report for 192.168.43.249 Host is up (0.020s latency). Nmap scan report for 192.168.43.250 Host is up (0.020s latency). Nmap scan report for 192.168.43.251 Host is up (0.029s latency). Nmap scan report for 192.168.43.252 Host is up (0.029s latency). Nmap scan report for 192.168.43.253 Host is up (0.030s latency). Nmap scan report for 192.168.43.254 Host is up (0.021s latency). Nmap scan report for 192.168.43.255 Host is up (0.029s latency). Nmap done: 256 IP addresses (256 hosts up) scanned in 75.54 seconds				

Perform a Fast Scan

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -F 192.168.43.96				
Starting Nmap 7.91 (https://nmap.org) at 2021-03-30 17:10 IST Nmap scan report for 192.168.43.96 Host is up (0.022s latency). All 100 scanned ports on 192.168.43.96 are filtered Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds				

Scan Ports Consecutively

nmap -r 192.168.43.96					
Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
▼	nmap -r 192.168.43.96				
	Starting Nmap 7.91 (https://nmap.org) at 2021-03-30 17:13 IST Nmap scan report for 192.168.43.96 Host is up (0.022s latency). All 1000 scanned ports on 192.168.43.96 are filtered Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds				

Print Host interfaces and Routes

```
nmap --iflist

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 17:14 IST
*****INTERFACES*****
DEV      (SHORT)  IP/MASK      TYPE      UP      MTU      MAC
lo0      (lo0)    127.0.0.1/8  loopback  up      16384
lo0      (lo0)    ::1/128      loopback  up      16384
lo0      (lo0)    fe80::1/128  loopback  up      16384
gif0     (gif0)    (none)/0     point2point down 1280
stf0     (stf0)    (none)/0     other     down 1280
XHC20    (XHC20)   (none)/0     other     down 0
en0      (en0)    192.168.55.102/24 ethernet  up      1500    98:46:0A:9C:14:F6
en0      (en0)    fe80::1857:4cac:db0b:6ae6/128 ethernet  up      1500    98:46:0A:9C:14:F6
p2p0     (p2p0)   (none)/0     ethernet  up      2304    0A:46:0A:9C:14:F6
awdl0    (awdl0)   (none)/0     ethernet  up      1484    AE:E1:48:D2:C0:14
awdl0    (awdl0)   fe80::ace1:48ff:fed2:c014/128 ethernet  up      1484    AE:E1:48:D2:C0:14
en1      (en1)    (none)/0     ethernet  up      1500    9A:00:19:73:8E:E0
bridge0  (bridge0) (none)/0     point2point up      1500    9A:00:19:73:8E:E0
utun0    (utun0)   (none)/0     point2point up      2000
utun0    (utun0)   fe80::44ed:882:35ea:946c/128 point2point up      2000

*****ROUTES*****
DST/MASK      DEV      METRIC  GATEWAY
216.58.203.46/32 en0      0       192.168.55.1
216.58.203.133/32 en0      0       192.168.55.1
17.57.145.138/32 en0      0       192.168.55.1
172.217.166.163/32 en0      0       192.168.55.1
127.0.0.1/32 lo0      0       127.0.0.1
142.250.67.142/32 en0      0       192.168.55.1
142.250.67.170/32 en0      0       192.168.55.1
142.250.77.46/32 en0      0       192.168.55.1
142.250.182.238/32 en0      0       192.168.55.1
142.250.183.10/32 en0      0       192.168.55.1
157.240.23.53/32 en0      0       192.168.55.1
172.217.26.238/32 en0      0       192.168.55.1
74.125.68.189/32 en0      0       192.168.55.1
172.217.166.170/32 en0      0       192.168.55.1
172.217.174.74/32 en0      0       192.168.55.1
192.168.55.1/32 en0      0
192.168.55.102/32 en0      0
74.125.24.189/32 en0      0       192.168.55.1
255.255.255.255/32 en0      0
192.168.55.0/24 en0      0
169.254.0.0/16 en0      0
127.0.0.0/8 lo0      0       127.0.0.1
224.0.0.0/4 en0      0
0.0.0.0/0 en0      0       192.168.55.1
fe80:a::44ed:882:35ea:946c/128 lo0      0
::1/128 lo0      0       ::1
fe80:1::1/128 lo0      0
fe80:1::/64 lo0      0       fe80:1::1
fe80:5::/64 en0      0
fe80:7::/64 awdl0    0
fe80:a::/64 utun0    0       fe80:a::44ed:882:35ea:946c
ff01:1::/32 lo0      0       ::1
ff02:a::/32 utun0    0       fe80:a::44ed:882:35ea:946c
ff02:7::/32 awdl0    0
ff01:7::/32 awdl0    0
ff01:a::/32 utun0    0       fe80:a::44ed:882:35ea:946c
ff02:1::/32 lo0      0       ::1
ff01:5::/32 en0      0
ff02:5::/32 en0      0
::/0 en0      0       fe80:5::1
::/0 utun0    0       fe80:a::
```

Find Host Services version Numbers

```
nmap -sV 192.168.43.96

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 17:18 IST
Nmap scan report for 192.168.43.96
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.43.96 are filtered

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```