CSE3501-Information Security Analysis and Audit

Lab 9+10

Lab FAT

Submitted by: Alokam Nikhitha

Reg No:19BCE2555

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INNFORMATION SECURTY AUDIT AND ANALYSIS

Sl. No	Components	Marks
1.	AIM & PSEUDO CODE	10
2.	PROGRAM & OUTPUT	20+10
3.	QUIZ	10

1. Use the following commands; observe the response from your system. Discuss in detail the results you have observed using the following commands.
   a) nmap -v -A www.example.com
   b) nmap -v -sn w.x.y.z/16 a.b.c.d/8
   c) nmap -v -iR M -Pn -p N
   d) nmap w.x.y.z/24 -exclude w.x.y.z
   e) nmap -sF w.x.y.z
2. Use the ports s20, 53 and try to access router filters and access control Lists.
3. Is it possible to Spoof source address? Demonstrate.

1)

AIM

To run the Nmap commands and observe the detailed results

PROGRAM & OUTPUT:

A) nmap –v –A www.google.com

Zenmap

Scan Tools Profile Help

Target: nmap | Profile: Intense scan | Scan | Cancel

Command: nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap - -

Hosts | Services

OS ◂ Host

www.google.com (

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

nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap www.google.com - - | Details

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-07 10:21 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:21
Completed NSE at 10:21, 0.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:21
Completed NSE at 10:21, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:21
Completed NSE at 10:21, 0.00s elapsed
Failed to resolve "nmap".
Warning: Hostname www.google.com resolves to 2 IPs. Using 142.250.195.100.
Failed to resolve "-".
Failed to resolve "-".
Initiating Ping Scan at 10:21
Scanning www.google.com (142.250.195.100) [4 ports]
Completed Ping Scan at 10:21, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:21
Completed Parallel DNS resolution of 1 host. at 10:21, 0.01s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Failed to resolve "-".
Initiating SYN Stealth Scan at 10:21
Scanning www.google.com (142.250.195.100) [1000 ports]
Discovered open port 80/tcp on 142.250.195.100
Discovered open port 443/tcp on 142.250.195.100
Completed SYN Stealth Scan at 10:22, 9.93s elapsed (1000 total ports)
Initiating Service scan at 10:22
Scanning 2 services on www.google.com (142.250.195.100)
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em;
border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{ background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</
style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #ffffff; color: #000000; \}\nh1 \{ font-family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</
style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em;
```

Filter Hosts

Type here to search | 30°C | ENG IN | 10:26 AM 12/7/2021

Zenmap

Scan Tools Profile Help

Target: nmap | Profile: Intense scan | Scan | Cancel

Command: nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap - -

Hosts | Services

OS ◂ Host

www.google.com (

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

nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap www.google.com - - | Details

```
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em;
border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{ background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</
style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #ffffff; color: #000000; \}\nh1 \{ font-family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</
style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em;
border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{ background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</
style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-
color: #ffffff; color: #000000; \}\nh1 \{ font-family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</
style>'
Service scan Timing: About 50.00% done; ETC: 10:24 (0:00:59 remaining)
Completed Service scan at 10:23, 68.38s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.google.com (142.250.195.100)
Retrying OS detection (try #2) against www.google.com (142.250.195.100)
Initiating Traceroute at 10:23
Completed Traceroute at 10:23, 0.12s elapsed
Initiating Parallel DNS resolution of 14 hosts. at 10:23
Completed Parallel DNS resolution of 14 hosts. at 10:23, 0.15s elapsed
DNS resolution of 14 IPs took 0.15s. Mode: Async [#: 2, OK: 1, NX: 13, DR: 0, SF: 0, TR: 14, CN: 0]
NSE: Script scanning 142.250.195.100.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 10.03s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 3.72s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Nmap scan report for www.google.com (142.250.195.100)
Host is up, received syn-ack ttl 54 (0.038s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:824::2004
rDNS record for 142.250.195.100: maa03s39-in-f4.1e100.net
Scanned at 2021-12-07 10:21:58 India Standard Time for 98s
```

Filter Hosts

Type here to search | 30°C | ENG IN | 10:27 AM 12/7/2021

Zenmap

Scan Tools Profile Help

Target: nmap -v -A www.google.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap -v -A www.google.com - -

Hosts | Services

OS ◂ Host

www.google.com (

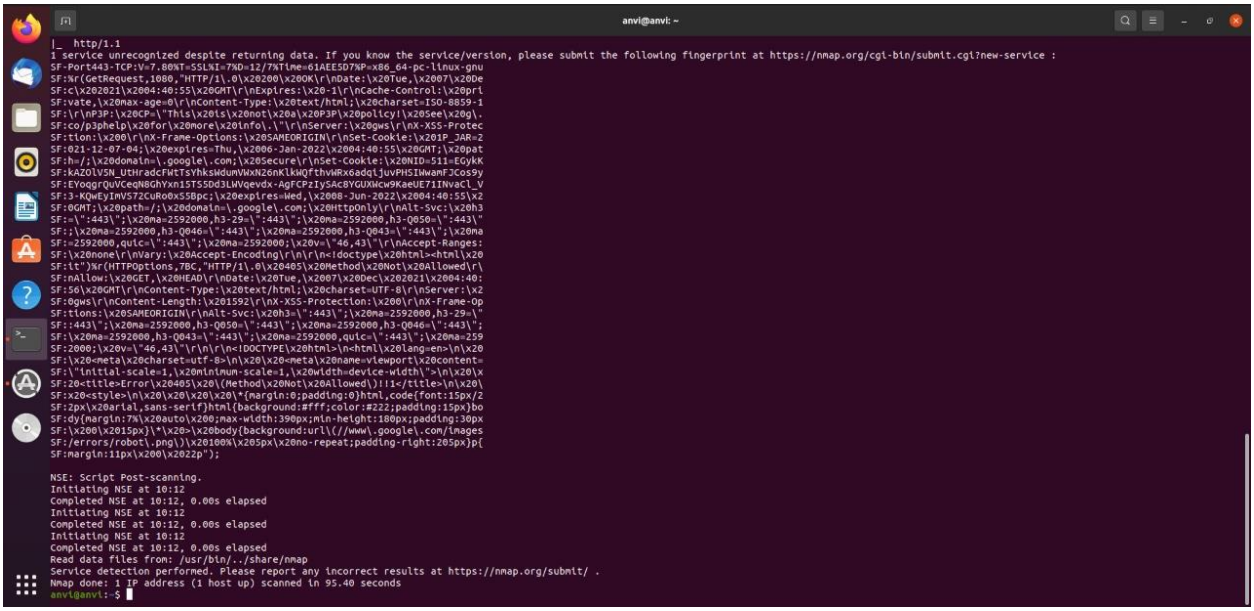
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap www.google.com - - Details

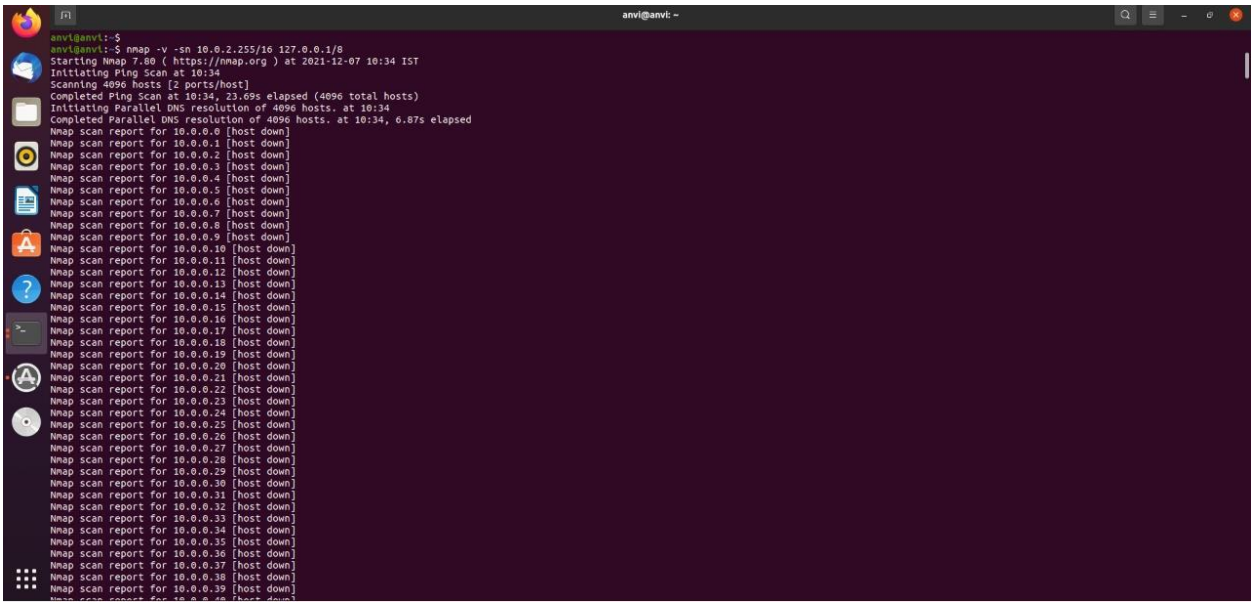
```
Uptime guess: 0.000 days (since Tue Dec  7 10:23:20 2021)
Network Distance: 15 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   4.00 ms  reliance.reliance (192.168.29.1)
2   7.00 ms  10.0.136.1
3   11.00 ms 172.31.2.120
4   14.00 ms 192.168.59.126
5   21.00 ms 172.26.74.70
6   20.00 ms 172.26.75.131
7   27.00 ms 192.168.60.228
8   31.00 ms 192.168.60.233
9   35.00 ms 172.31.2.65
10  39.00 ms 74.125.51.166
11  39.00 ms 216.239.43.133
12  35.00 ms 142.251.55.71
13  45.00 ms 72.14.232.51
14  39.00 ms 108.170.253.97
15  31.00 ms maa03s39-in-f4.1e100.net (142.250.195.100)

Failed to resolve "-".
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 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: 1 IP address (1 host up) scanned in 118.82 seconds
           Raw packets sent: 2108 (97.052KB) | Rcvd: 82 (4.938KB)
```

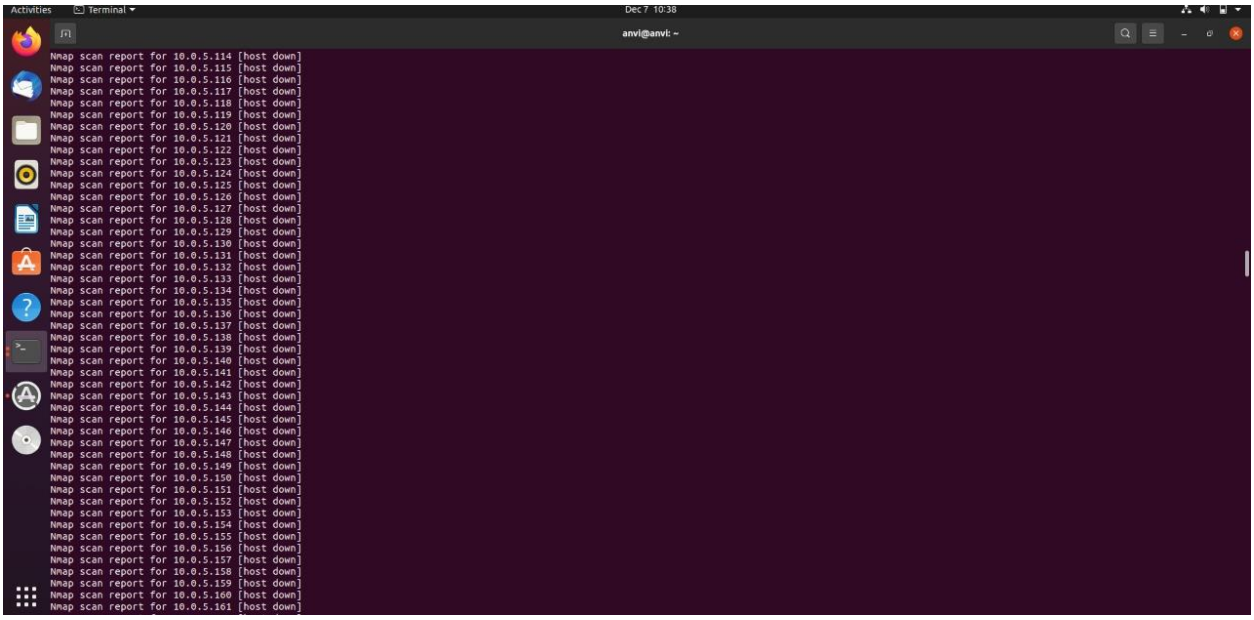
anvi@anvi: ~

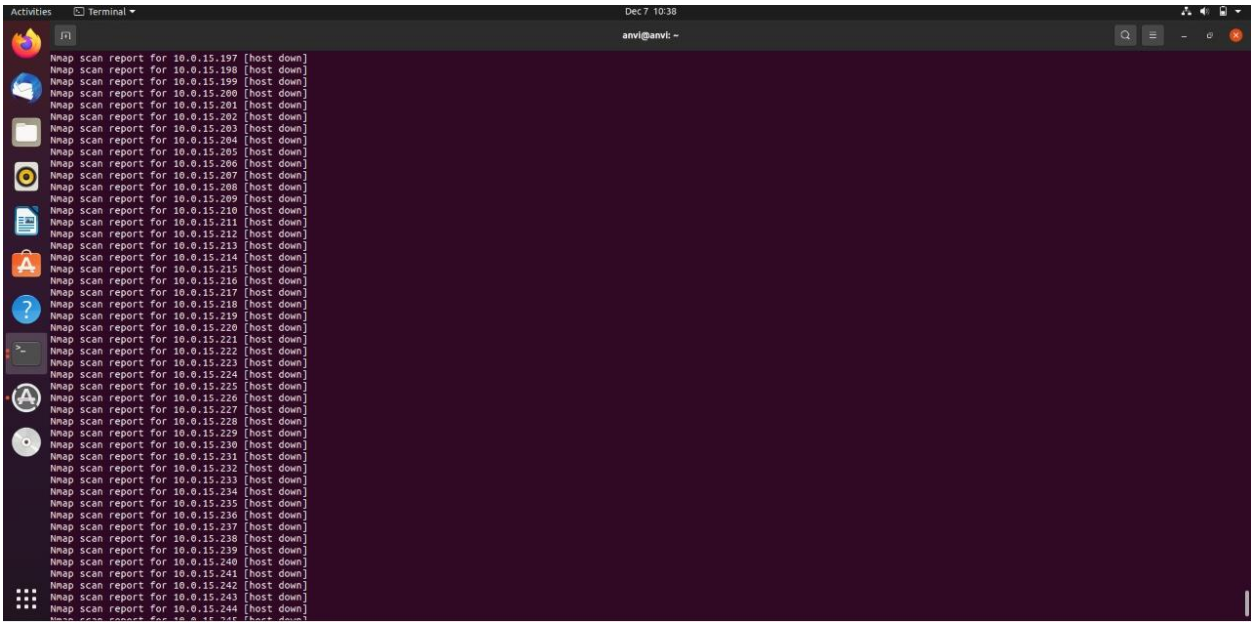
```
anvi@anvi:~$ nmap -v -A www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-07 10:10 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
Initiating Ping Scan at 10:10
Scanning www.google.com (142.250.193.164) [2 ports]
Completed Ping Scan at 10:10, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:10
Completed Parallel DNS resolution of 1 host. at 10:10, 0.01s elapsed
Initiating Connect Scan at 10:10
Scanning www.google.com (142.250.193.164) [1000 ports]
Discovered open port 443/tcp on 142.250.193.164
Discovered open port 80/tcp on 142.250.193.164
Completed Connect Scan at 10:10, 6.38s elapsed (1000 total ports)
Initiating Service scan at 10:10
Scanning 2 services on www.google.com (142.250.193.164)
Completed Service scan at 10:11, 68.87s elapsed (2 services on 1 host)
NSE: Script scanning 142.250.193.164.
Initiating NSE at 10:11
Completed NSE at 10:12, 15.21s elapsed
Initiating NSE at 10:12
Completed NSE at 10:12, 0.83s elapsed
Initiating NSE at 10:12
Completed NSE at 10:12, 0.00s elapsed
Nmap scan report for www.google.com (142.250.193.164)
Host is up (0.036s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:82d::2004
rDNS record for 142.250.193.164: maa05s26-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
|_http-favicon: Google
| http-methods:
|_  Supported Methods: GET HEAD
| http-robots.txt: 223 disallowed entries (15 shown)
| /search /sdch /groups /index.html? /? /?hl=*&
|_/?hl=*&*&gws_rd=ssl /imgres /u/ /preferences /setprefs /default /m? /m/ /wml?
|_http-server-header: gws
|_http-title: Google
443/tcp open  ssl/https  gws
| fingerprint-strings:
|   GetRequest:
```

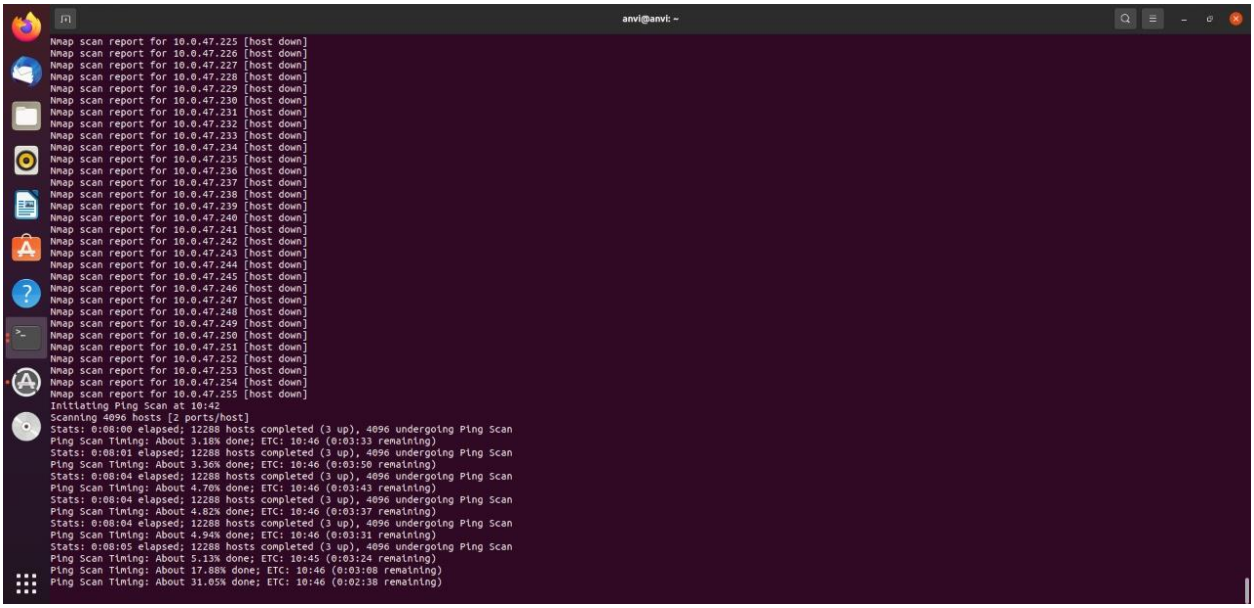


b)nmap –v –sn 10.0.2.255/16 127.0.0.1/8

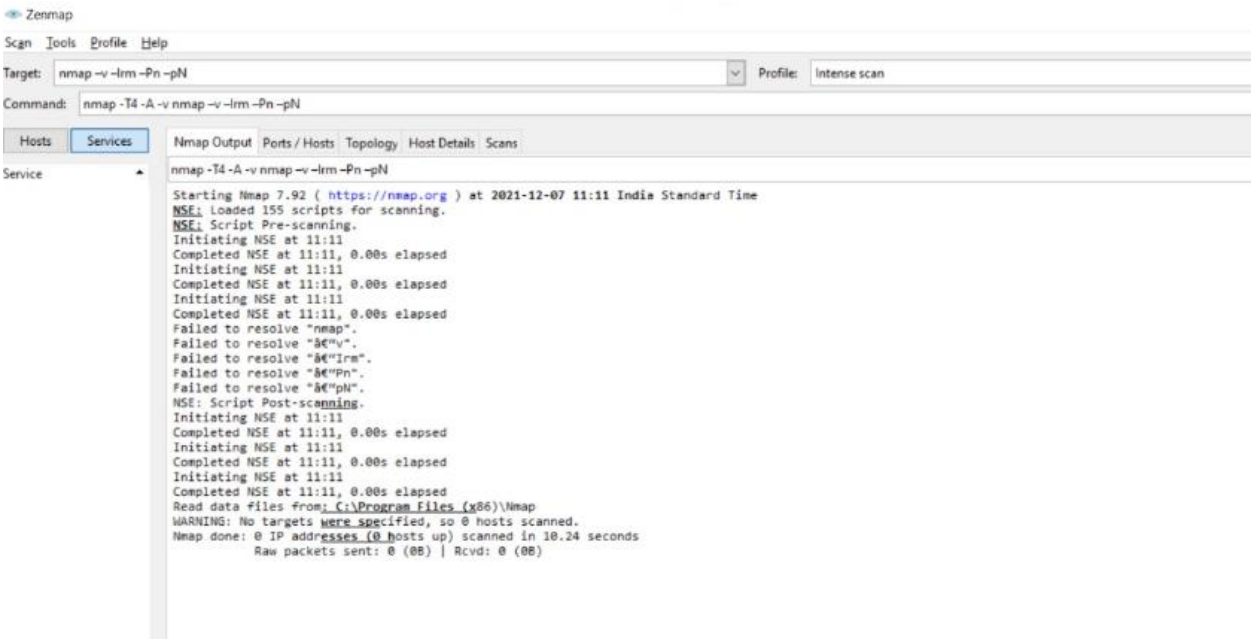



Activities
Terminal
Dec 7 10:38
anvi@anvi: ~
Nmap scan report for 10.0.5.114 [host down]
Nmap scan report for 10.0.5.115 [host down]
Nmap scan report for 10.0.5.116 [host down]
Nmap scan report for 10.0.5.117 [host down]
Nmap scan report for 10.0.5.118 [host down]
Nmap scan report for 10.0.5.119 [host down]
Nmap scan report for 10.0.5.120 [host down]
Nmap scan report for 10.0.5.121 [host down]
Nmap scan report for 10.0.5.122 [host down]
Nmap scan report for 10.0.5.123 [host down]
Nmap scan report for 10.0.5.124 [host down]
Nmap scan report for 10.0.5.125 [host down]
Nmap scan report for 10.0.5.126 [host down]
Nmap scan report for 10.0.5.127 [host down]
Nmap scan report for 10.0.5.128 [host down]
Nmap scan report for 10.0.5.129 [host down]
Nmap scan report for 10.0.5.130 [host down]
Nmap scan report for 10.0.5.131 [host down]
Nmap scan report for 10.0.5.132 [host down]
Nmap scan report for 10.0.5.133 [host down]
Nmap scan report for 10.0.5.134 [host down]
Nmap scan report for 10.0.5.135 [host down]
Nmap scan report for 10.0.5.136 [host down]
Nmap scan report for 10.0.5.137 [host down]
Nmap scan report for 10.0.5.138 [host down]
Nmap scan report for 10.0.5.139 [host down]
Nmap scan report for 10.0.5.140 [host down]
Nmap scan report for 10.0.5.141 [host down]
Nmap scan report for 10.0.5.142 [host down]
Nmap scan report for 10.0.5.143 [host down]
Nmap scan report for 10.0.5.144 [host down]
Nmap scan report for 10.0.5.145 [host down]
Nmap scan report for 10.0.5.146 [host down]
Nmap scan report for 10.0.5.147 [host down]
Nmap scan report for 10.0.5.148 [host down]
Nmap scan report for 10.0.5.149 [host down]
Nmap scan report for 10.0.5.150 [host down]
Nmap scan report for 10.0.5.151 [host down]
Nmap scan report for 10.0.5.152 [host down]
Nmap scan report for 10.0.5.153 [host down]
Nmap scan report for 10.0.5.154 [host down]
Nmap scan report for 10.0.5.155 [host down]
Nmap scan report for 10.0.5.156 [host down]
Nmap scan report for 10.0.5.157 [host down]
Nmap scan report for 10.0.5.158 [host down]
Nmap scan report for 10.0.5.159 [host down]
Nmap scan report for 10.0.5.160 [host down]
Nmap scan report for 10.0.5.161 [host down]


Activities
Terminal
Dec 7 10:38
anvi@anvi: ~
Nmap scan report for 10.0.15.197 [host down]
Nmap scan report for 10.0.15.198 [host down]
Nmap scan report for 10.0.15.199 [host down]
Nmap scan report for 10.0.15.200 [host down]
Nmap scan report for 10.0.15.201 [host down]
Nmap scan report for 10.0.15.202 [host down]
Nmap scan report for 10.0.15.203 [host down]
Nmap scan report for 10.0.15.204 [host down]
Nmap scan report for 10.0.15.205 [host down]
Nmap scan report for 10.0.15.206 [host down]
Nmap scan report for 10.0.15.207 [host down]
Nmap scan report for 10.0.15.208 [host down]
Nmap scan report for 10.0.15.209 [host down]
Nmap scan report for 10.0.15.210 [host down]
Nmap scan report for 10.0.15.211 [host down]
Nmap scan report for 10.0.15.212 [host down]
Nmap scan report for 10.0.15.213 [host down]
Nmap scan report for 10.0.15.214 [host down]
Nmap scan report for 10.0.15.215 [host down]
Nmap scan report for 10.0.15.216 [host down]
Nmap scan report for 10.0.15.217 [host down]
Nmap scan report for 10.0.15.218 [host down]
Nmap scan report for 10.0.15.219 [host down]
Nmap scan report for 10.0.15.220 [host down]
Nmap scan report for 10.0.15.221 [host down]
Nmap scan report for 10.0.15.222 [host down]
Nmap scan report for 10.0.15.223 [host down]
Nmap scan report for 10.0.15.224 [host down]
Nmap scan report for 10.0.15.225 [host down]
Nmap scan report for 10.0.15.226 [host down]
Nmap scan report for 10.0.15.227 [host down]
Nmap scan report for 10.0.15.228 [host down]
Nmap scan report for 10.0.15.229 [host down]
Nmap scan report for 10.0.15.230 [host down]
Nmap scan report for 10.0.15.231 [host down]
Nmap scan report for 10.0.15.232 [host down]
Nmap scan report for 10.0.15.233 [host down]
Nmap scan report for 10.0.15.234 [host down]
Nmap scan report for 10.0.15.235 [host down]
Nmap scan report for 10.0.15.236 [host down]
Nmap scan report for 10.0.15.237 [host down]
Nmap scan report for 10.0.15.238 [host down]
Nmap scan report for 10.0.15.239 [host down]
Nmap scan report for 10.0.15.240 [host down]
Nmap scan report for 10.0.15.241 [host down]
Nmap scan report for 10.0.15.242 [host down]
Nmap scan report for 10.0.15.243 [host down]
Nmap scan report for 10.0.15.244 [host down]

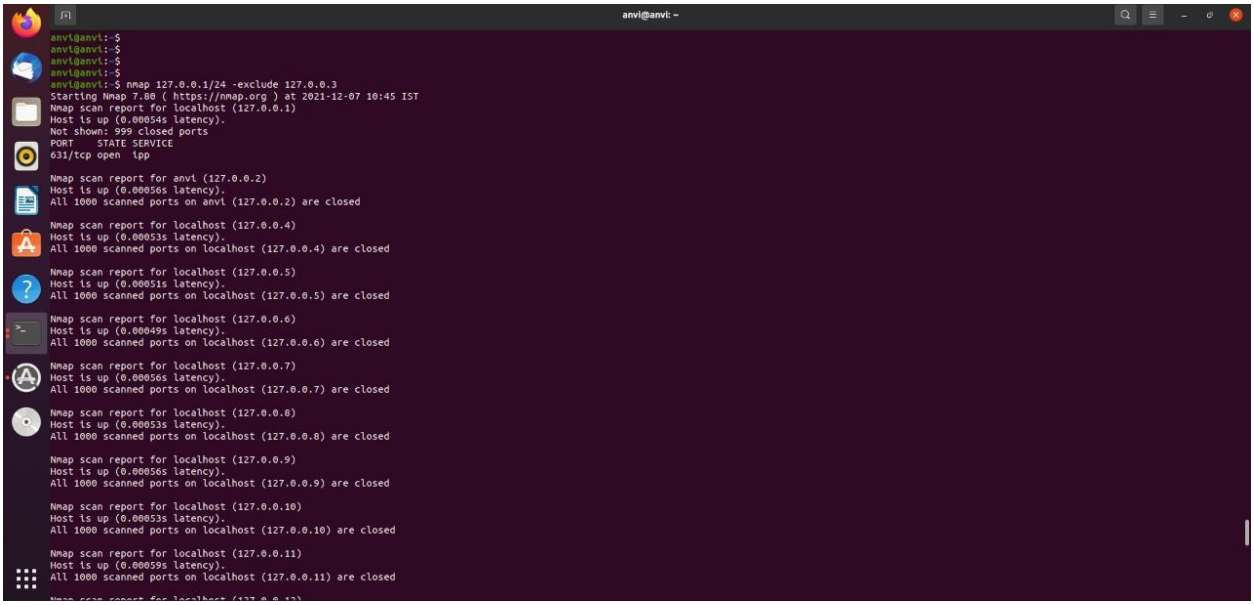


c) nmap -v -iR M -Pn -p N

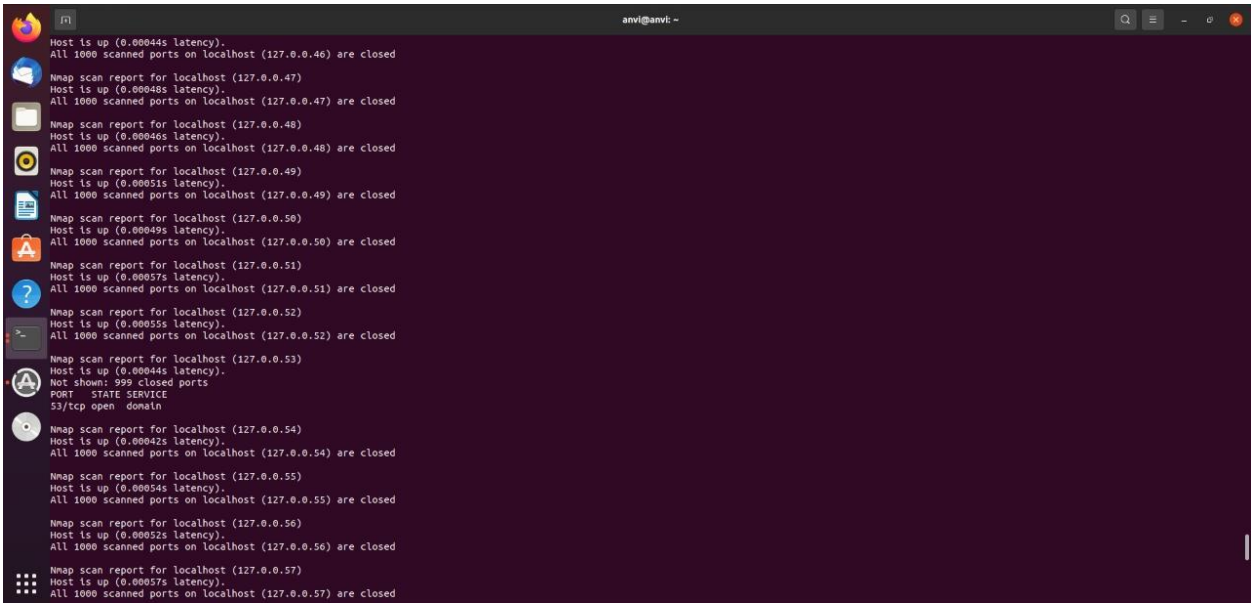


d)nmap 127.0.0.1/24 -exclude 127.0.0.3

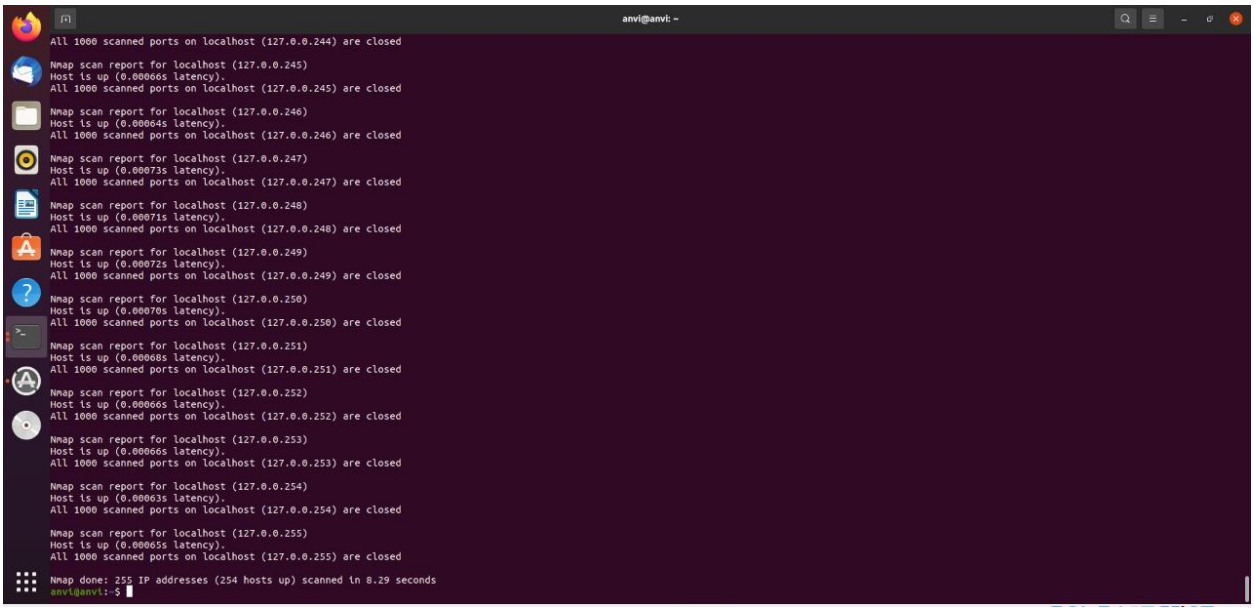
Here we excluded 127.0.0.3 port from series can see in the image below



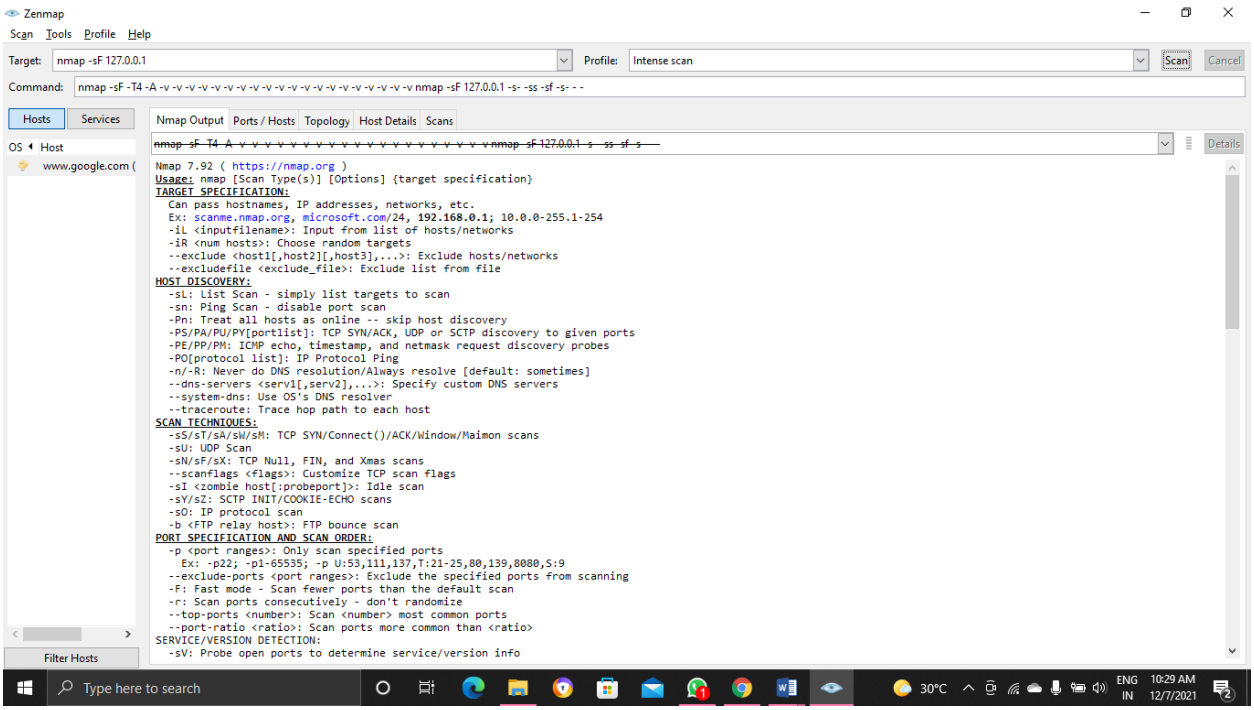
```
anvi@anvi: ~
anvi@anvi:~$
anvi@anvi:~$
anvi@anvi:~$
anvi@anvi:~$
anvi@anvi:~$ nmap 127.0.0.1/24 -exclude 127.0.0.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-07 10:45 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00054s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp

Nmap scan report for anvi (127.0.0.2)
Host is up (0.00056s latency).
All 1000 scanned ports on anvi (127.0.0.2) are closed

Nmap scan report for localhost (127.0.0.4)
Host is up (0.00053s latency).
All 1000 scanned ports on localhost (127.0.0.4) are closed

Nmap scan report for localhost (127.0.0.5)
Host is up (0.00051s latency).
All 1000 scanned ports on localhost (127.0.0.5) are closed

Nmap scan report for localhost (127.0.0.6)
Host is up (0.00049s latency).
All 1000 scanned ports on localhost (127.0.0.6) are closed

Nmap scan report for localhost (127.0.0.7)
Host is up (0.00056s latency).
All 1000 scanned ports on localhost (127.0.0.7) are closed

Nmap scan report for localhost (127.0.0.8)
Host is up (0.00053s latency).
All 1000 scanned ports on localhost (127.0.0.8) are closed

Nmap scan report for localhost (127.0.0.9)
Host is up (0.00056s latency).
All 1000 scanned ports on localhost (127.0.0.9) are closed

Nmap scan report for localhost (127.0.0.10)
Host is up (0.00053s latency).
All 1000 scanned ports on localhost (127.0.0.10) are closed

Nmap scan report for localhost (127.0.0.11)
Host is up (0.00059s latency).
All 1000 scanned ports on localhost (127.0.0.11) are closed
```



```
anvi@anvi: ~
Host is up (0.00044s latency).
All 1000 scanned ports on localhost (127.0.0.46) are closed

Nmap scan report for localhost (127.0.0.47)
Host is up (0.00048s latency).
All 1000 scanned ports on localhost (127.0.0.47) are closed

Nmap scan report for localhost (127.0.0.48)
Host is up (0.00046s latency).
All 1000 scanned ports on localhost (127.0.0.48) are closed

Nmap scan report for localhost (127.0.0.49)
Host is up (0.00051s latency).
All 1000 scanned ports on localhost (127.0.0.49) are closed

Nmap scan report for localhost (127.0.0.50)
Host is up (0.00049s latency).
All 1000 scanned ports on localhost (127.0.0.50) are closed

Nmap scan report for localhost (127.0.0.51)
Host is up (0.00057s latency).
All 1000 scanned ports on localhost (127.0.0.51) are closed

Nmap scan report for localhost (127.0.0.52)
Host is up (0.00055s latency).
All 1000 scanned ports on localhost (127.0.0.52) are closed

Nmap scan report for localhost (127.0.0.53)
Host is up (0.00044s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
53/tcp open  domain

Nmap scan report for localhost (127.0.0.54)
Host is up (0.00042s latency).
All 1000 scanned ports on localhost (127.0.0.54) are closed

Nmap scan report for localhost (127.0.0.55)
Host is up (0.00054s latency).
All 1000 scanned ports on localhost (127.0.0.55) are closed

Nmap scan report for localhost (127.0.0.56)
Host is up (0.00052s latency).
All 1000 scanned ports on localhost (127.0.0.56) are closed

Nmap scan report for localhost (127.0.0.57)
Host is up (0.00057s latency).
All 1000 scanned ports on localhost (127.0.0.57) are closed
```



e)nmap -sF 127.0.0.1



Zenmap

Scan Tools Profile Help

Target: nmap -sF 127.0.0.1 Profile: Intense scan Scan Cancel

Command: nmap -sF -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap -sF 127.0.0.1 -s- -ss -sf -s- - -

Hosts Services

OS ◂ Host

www.google.com (

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

~~nmap -sF -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap -sF 127.0.0.1 -s- -ss -sf -s-~~

Details

```
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
```

Type here to search 30°C ENG IN 10:30 AM 12/7/2021

Zenmap

Scan Tools Profile Help

Target: nmap -sF 127.0.0.1 Profile: Intense scan Scan Cancel

Command: nmap -sF -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap -sF 127.0.0.1 -s- -ss -sf -s- - -

Hosts Services

OS ◂ Host

www.google.com (

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

~~nmap -sF -T4 -A -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v -v nmap -sF 127.0.0.1 -s- -ss -sf -s-~~

Details

```
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype - not supported
```

Type here to search 30°C ENG IN 10:30 AM 12/7/2021

2)

Aim and Psuedocode:

To access router filters and access control Lists with ports s20 and 53

Psuedo code:

- **To view a policy access control list, click a domain's name from the Domains pane in the Policy**
- **Administration window and select the Access Control Rules tab. In the Search Results table, click the view access control lists icon .**
- **The View Access Control Lists window opens.**
- **Multiple View Access Control Lists windows can be opened to allow you to compare lists for different object types and life cycle states.**

to acess file connected to router :Click Start > All Programs > Accessories > Run.

Type \\ IP address of the router (default is 192.168.0.1)
Example- \\192.168.0.1.
Click OK.
If you are prompted to enter a Username and Password, enter the credentials that you use to log in to the router's web-based configuration utility.

Program and Output

```
R0(config-line)#no exec-tim
R0(config-line)#no exec-timeout
R0(config-line)#
R0(config-line)#
R0(config-line)#int fa0/0
R0(config-if)#ip addre
R0(config-if)#ip address 172.16.1.1 255.255.255.252
R0(config-if)#int lo0
R0(config-if)#ip addr
R0(config-if)#ip address 192.168.10.1 255.255.255.0
R0(config-if)#int lo1
R0(config-if)#ip addr
R0(config-if)#ip address 192.168.20.1 255.255.255.0
R0(config-if)#router rip
R0(config-if)#router rip
R0(config-router)#ver
R0(config-router)#version 2
R0(config-router)#no au
R0(config-router)#no auto-summary
R0(config-router)#network
R0(config-router)#network 172.16.0.0
R0(config-router)#netowrk 192.168.10.0
                      ^
% Invalid input detected at '^' marker.

R0(config-router)#network 192.168.10.
% Incomplete command.
```

```
R0(config-router)#netowrk 192.168.10.0
                      ^
% Invalid input detected at '^' marker.

R0(config-router)#network 192.168.10.
% Incomplete command.

R0(config-router)#network 192.168.10.0
R0(config-router)#network 192.168.20.0
R0(config-router)#end
R0#show ip
*Mar  1 00:05:32.091: %SYS-5-CONFIG_I: Configured from console by consolepro
R0#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    Loopback0             2     2
    Loopback1             2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
    192.168.20.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

3)

Aim & Psuedocode:

Our aim is to check if Spoofing of Source Address is possible or not. If possible we have to demonstrate.

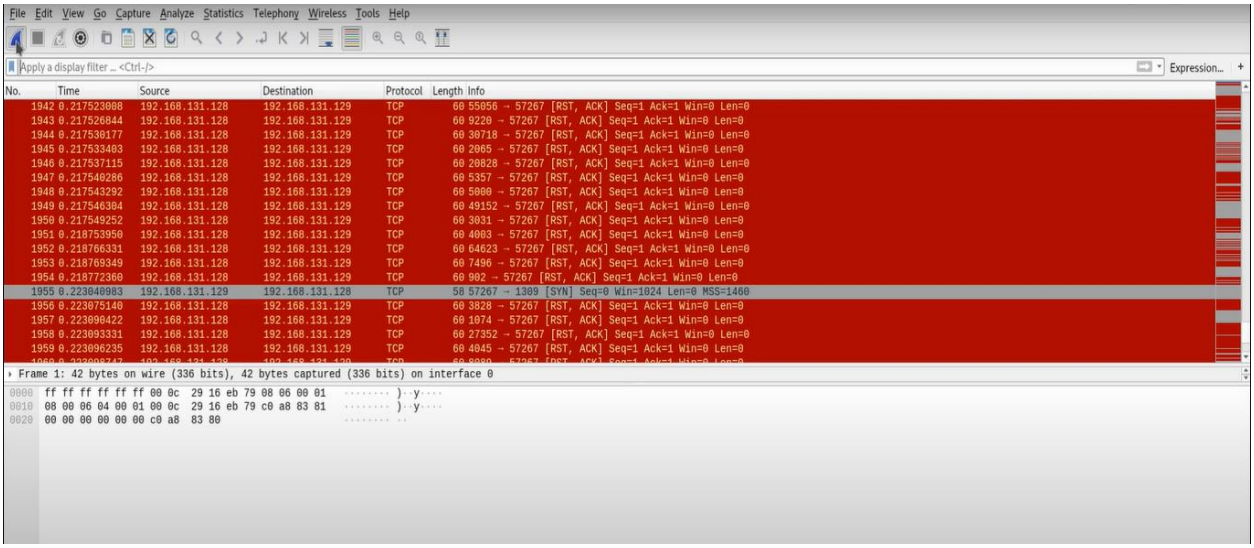
IP address spoofing, or IP spoofing, is the forging of a source IP address field in IP packets with the purpose of concealing the identity of the sender or impersonating another computing system. Fundamentally, source IP spoofing is possible because Internet global routing is based on the destination IP address.

Yes we can spoof IP address

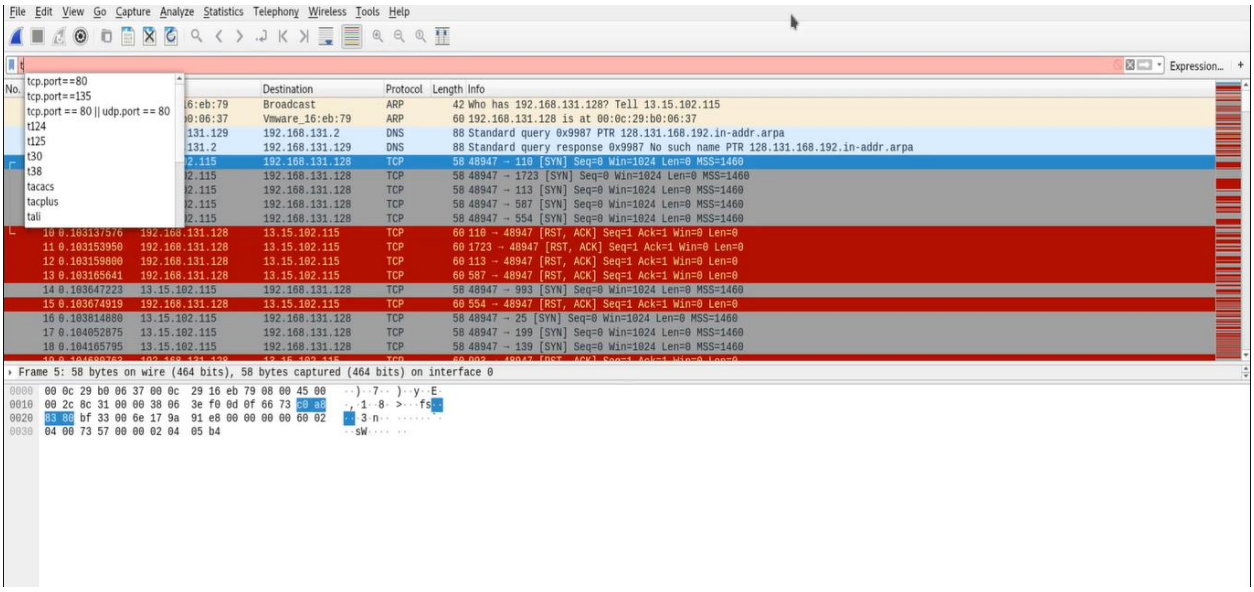
The most common forms of spoofing are:

- **DNS server spoofing** – Modifies a DNS server in order to redirect a domain name to a different IP address. It's typically used to spread viruses.
- **ARP spoofing** – Links a perpetrator's MAC address to a legitimate IP address through spoofed ARP messages. It's typically used in denial of service (DoS) and man-in-the-middle assaults.
- **IP address spoofing** – Disguises an attacker's origin IP. It's typically used in DoS assaults.

Program and Output:



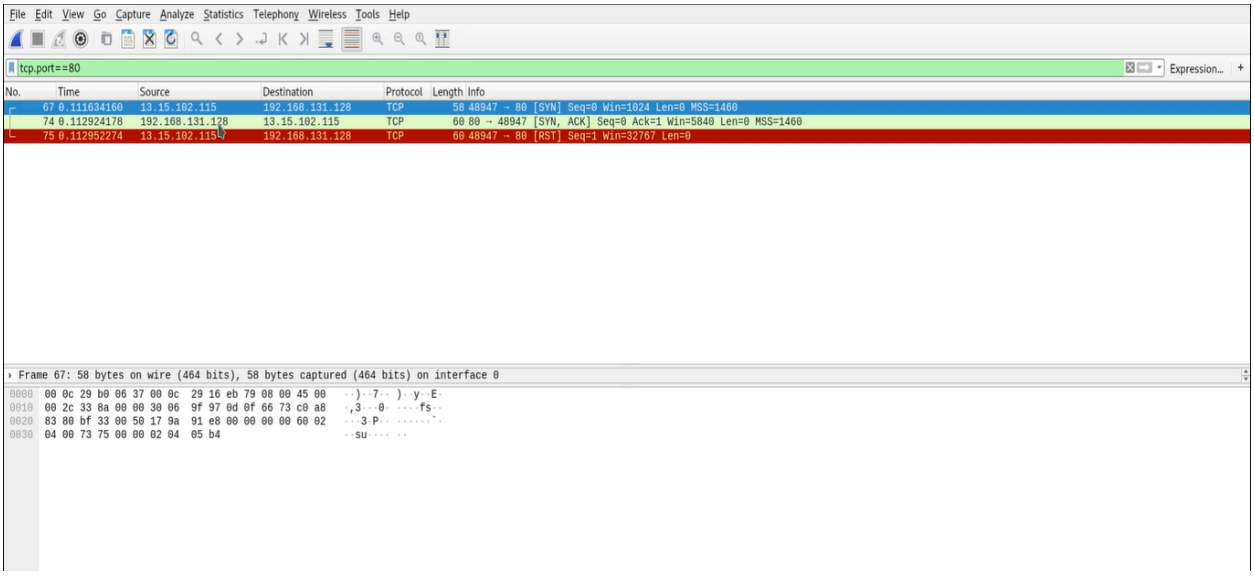
These are list of various IP sources



We are considering a particular IP address among all these for spoofing.

```
#nmap -e eth0 -S 13.15.102.115 192.168.131.128
WARNING: If -S is being used to fake your source address, you may also have to u
se -e <interface> and -Pn .  If you are using it to specify your real source add
ress, you can ignore this warning.
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-26 23:21 IST
NSOCK ERROR [0.1270s] mksock_bind_addr(): Bind to 13.15.102.115:0 failed (IOD #1
): Cannot assign requested address (99)
Nmap scan report for 192.168.131.128
Host is up (0.0036s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
```

Spoofing a particular IP address whose source addr is:13.15.102.115 and Destination addr :192.168.131.128



Considering IP sources whose tcp==80

We can see that there are 2 same Ip sources Request generated from Fake IP address in blue color line.