Practical – 2

Information Gathering using NMAP framework and study about port scanning.

NAME

Nmap - Network exploration tool and security / port scanner

SYNOPSIS

nmap [Scan Type...] [Options] {target specification}

DESCRIPTION

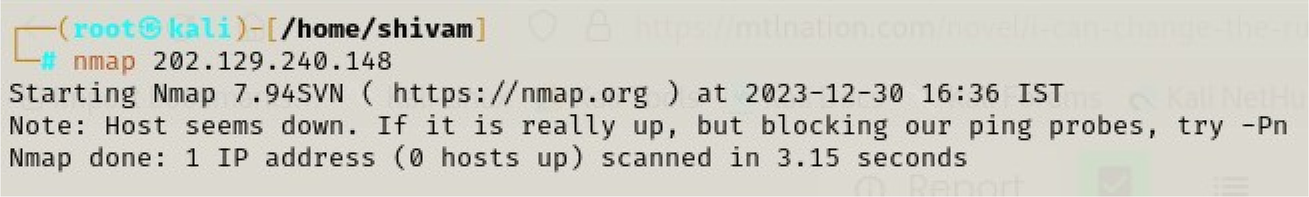
Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the“ interesting ports table”. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

1: Scan a single host or an IP address (IPv4)

# Nmap 202.192.240.148

Scans host IPv4 address

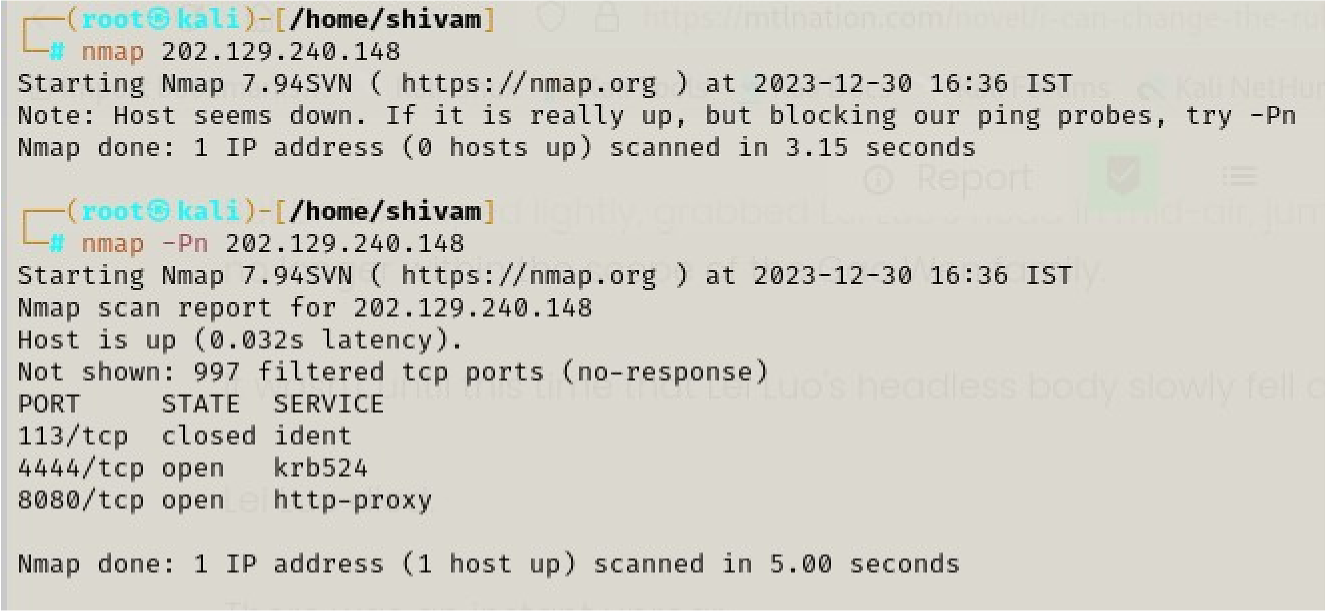


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:36 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds
```

2) Disabeling Host Discovery using “-Pn”

# Nmap -Pn 202.192.240.148

Disable host discovery. Port scan only.

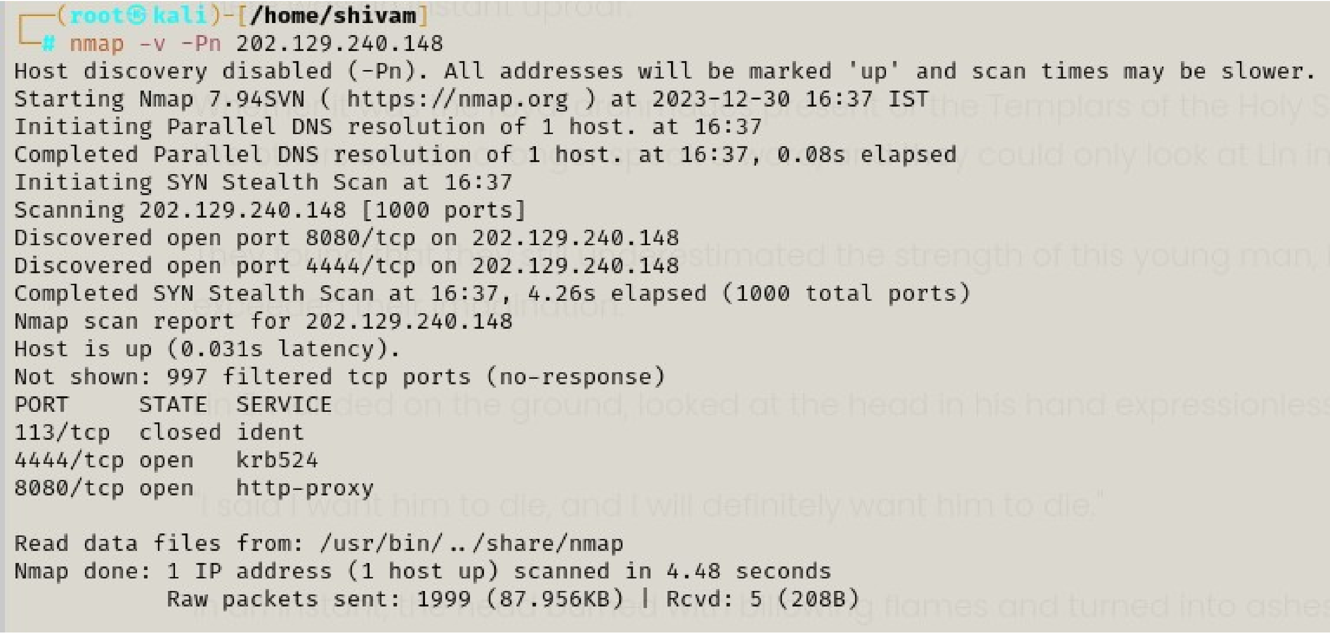


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:36 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

┌──(root㉿kali)-[/home/shivam]
└─# nmap -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:36 IST
Nmap scan report for 202.129.240.148
Host is up (0.032s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
```

3. Scan using “-v” option.

# Nmap -v 202.192.240.148

Increase the verbosity level (use -vv or more for greater effect)

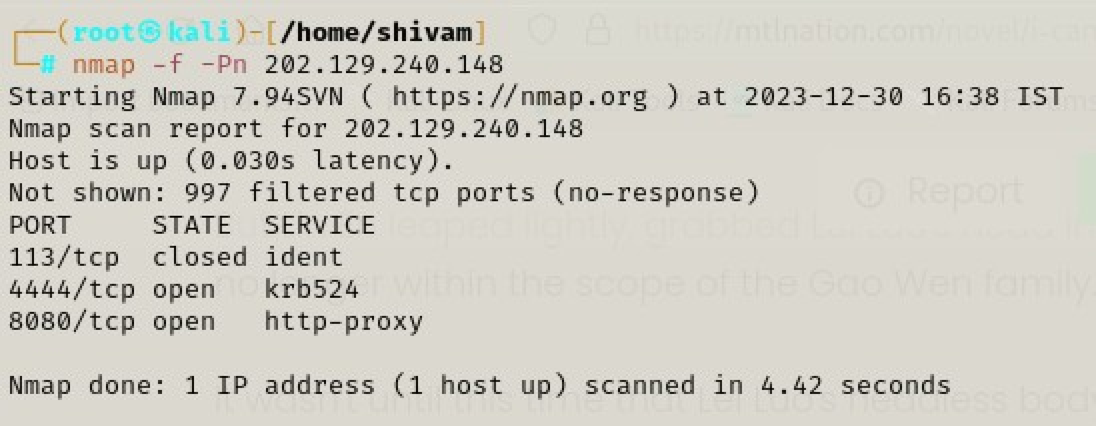


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -v -Pn 202.129.240.148
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:37 IST
Initiating Parallel DNS resolution of 1 host. at 16:37
Completed Parallel DNS resolution of 1 host. at 16:37, 0.08s elapsed
Initiating SYN Stealth Scan at 16:37
Scanning 202.129.240.148 [1000 ports]
Discovered open port 8080/tcp on 202.129.240.148
Discovered open port 4444/tcp on 202.129.240.148
Completed SYN Stealth Scan at 16:37, 4.26s elapsed (1000 total ports)
Nmap scan report for 202.129.240.148
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
           Raw packets sent: 1999 (87.956KB) | Rcvd: 5 (208B)
```

4. Scan using “-f” option.

# Nmap -f 202.192.240.148

Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing.

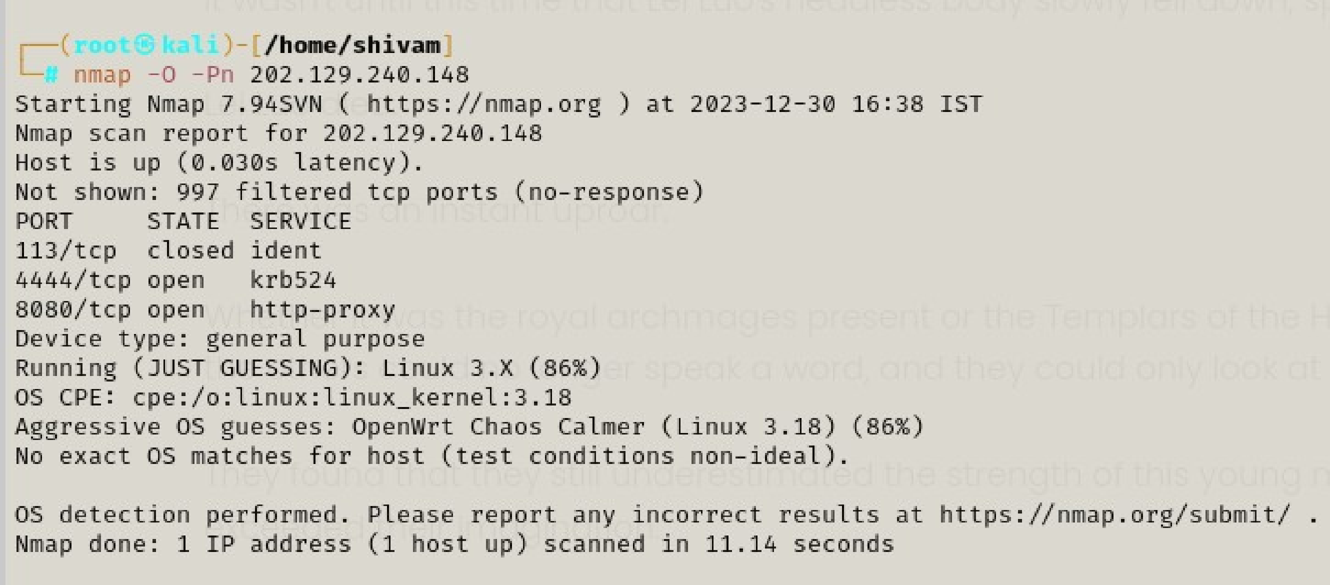


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -f -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:38 IST
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```

5 Enabling Os Detection using “-O’

# Nmap -O 202.192.240.148

Remote OS detection using TCP/IP stack fingerprinting

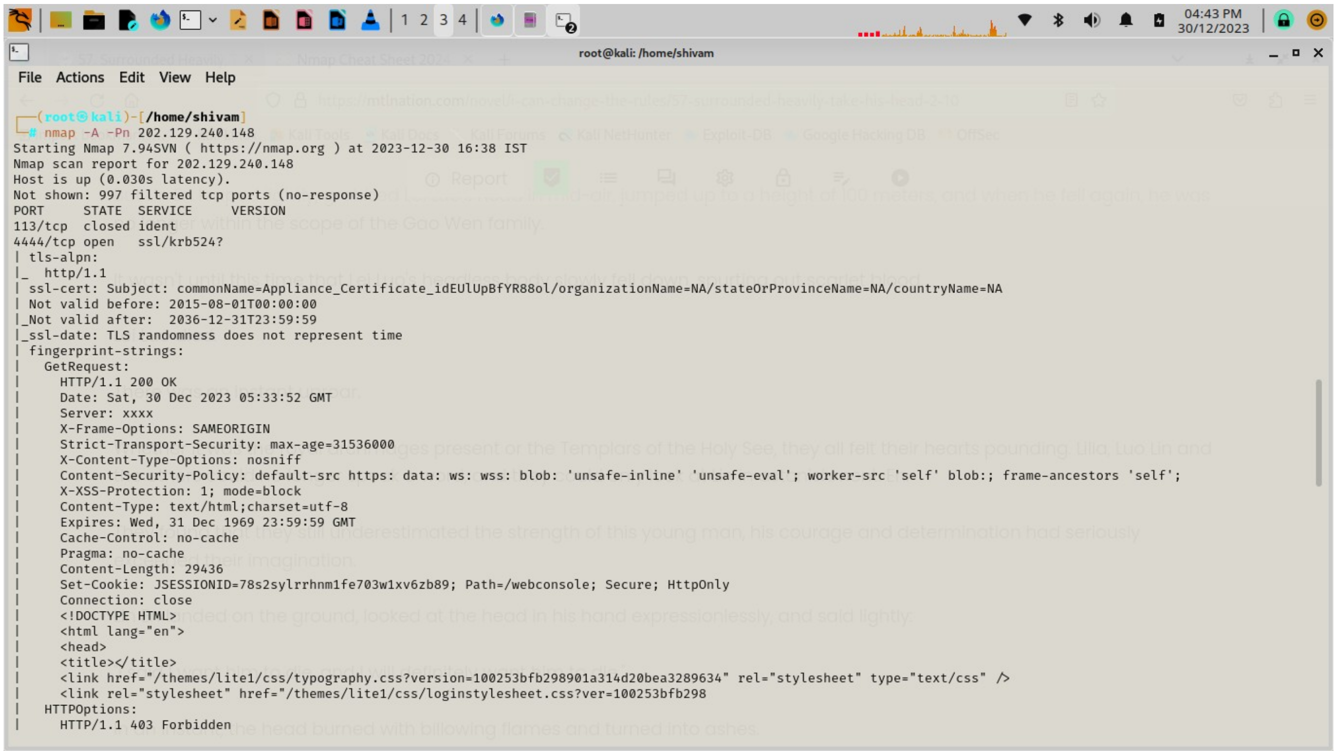


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -O -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:38 IST
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.18
Aggressive OS guesses: OpenWrt Chaos Calmer (Linux 3.18) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.14 seconds
```

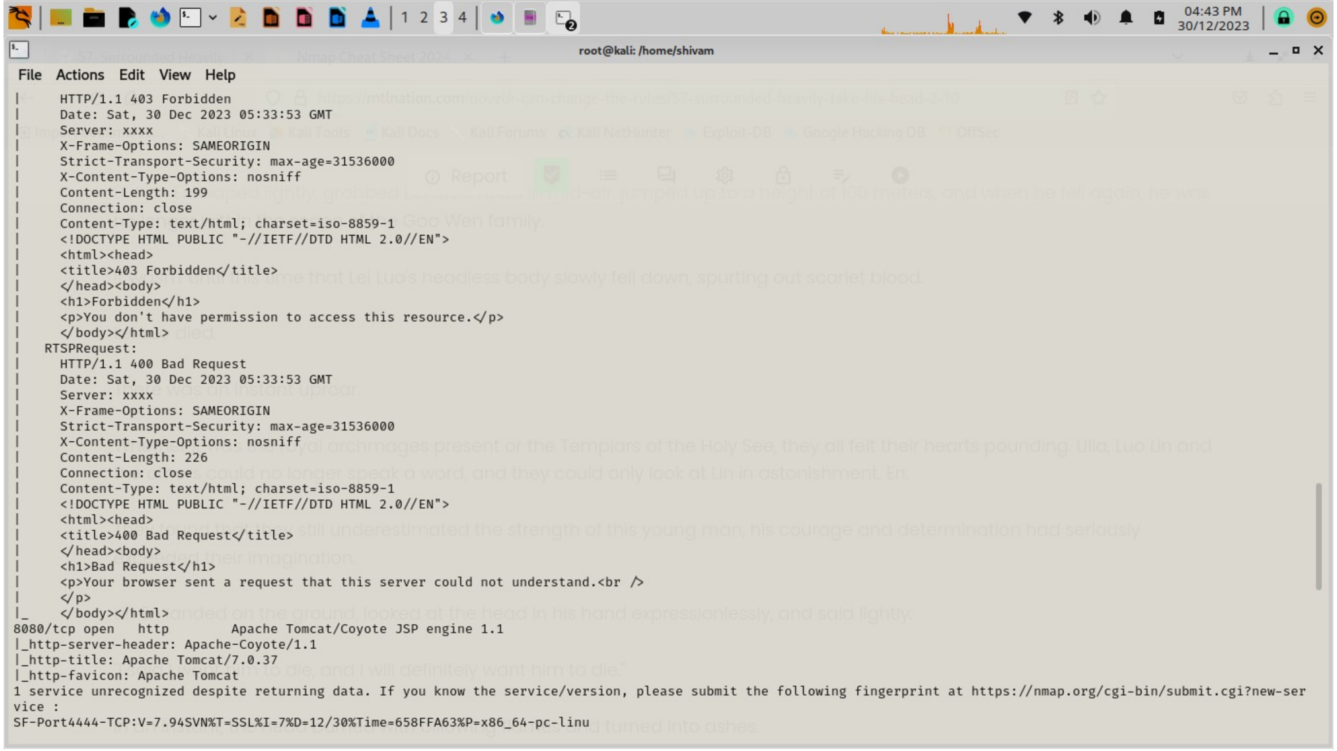
6) Scan OS information and Trace route.

# Nmap -A 202.192.240.148

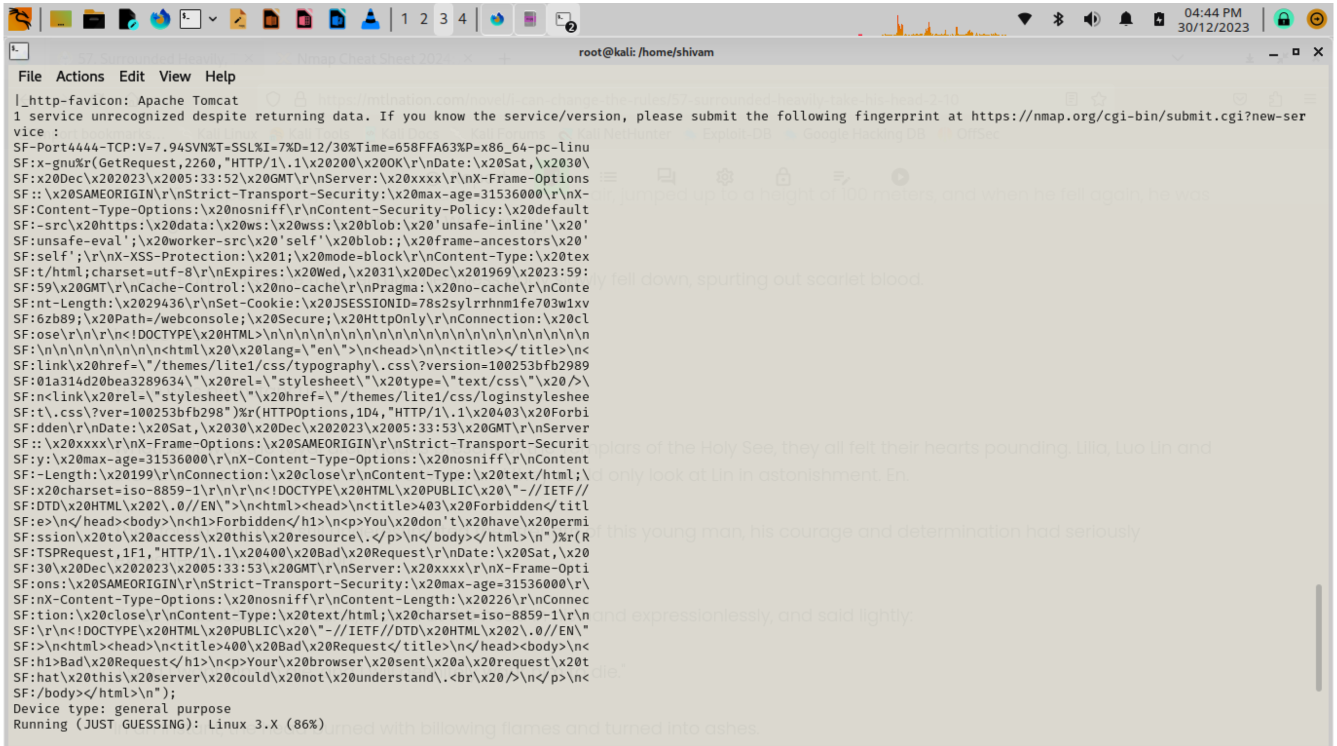
Enables OS detection, version detection, script scanning, and traceroute



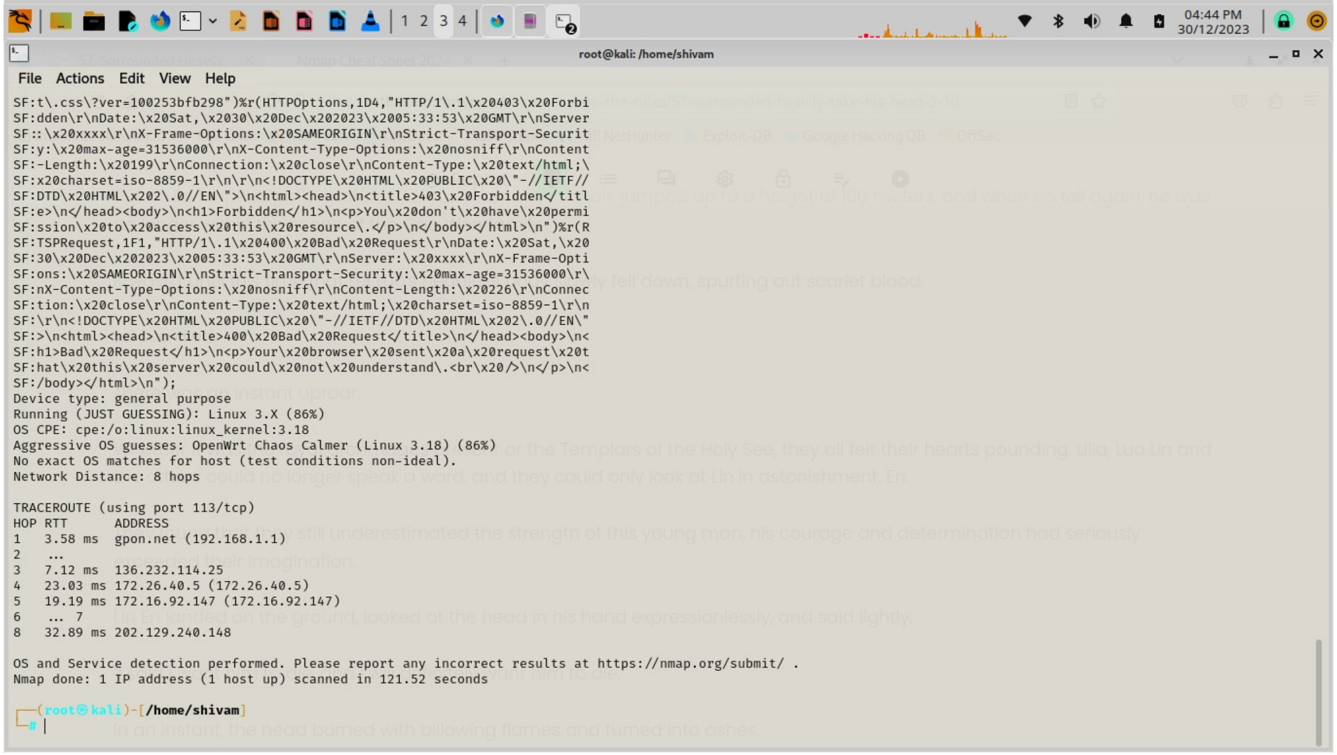
```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -A -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:38 IST
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
113/tcp  closed ident
4444/tcp open   ssl/krb524?
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=Appliance_Certificate_idEUlUpBfYR88ol/organizationName=NA/stateOrProvinceName=NA/countryName=NA
| Not valid before: 2015-08-01T00:00:00
|_Not valid after:  2036-12-31T23:59:59
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Sat, 30 Dec 2023 05:33:52 GMT
|     Server: xxxx
|     X-Frame-Options: SAMEORIGIN
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: default-src https: data: ws: wss: blob: 'unsafe-inline' 'unsafe-eval'; worker-src 'self' blob:; frame-ancestors 'self';
|     X-XSS-Protection: 1; mode=block
|     Content-Type: text/html;charset=utf-8
|     Expires: Wed, 31 Dec 1969 23:59:59 GMT
|     Cache-Control: no-cache
|     Pragma: no-cache
|     Content-Length: 29436
|     Set-Cookie: JSESSIONID=78s2sylrrhnm1fe703w1xv6zb89; Path=/webconsole; Secure; HttpOnly
|     Connection: close
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|     <title></title>
|     <link href="/themes/lite1/css/typography.css?version=100253bfb298901a314d20bea3289634" rel="stylesheet" type="text/css" />
|     <link rel="stylesheet" href="/themes/lite1/css/loginstylesheet.css?ver=100253bfb298
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
```



```
|     HTTP/1.1 403 Forbidden
|     Date: Sat, 30 Dec 2023 05:33:53 GMT
|     Server: xxxx
|     X-Frame-Options: SAMEORIGIN
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     Content-Length: 199
|     Connection: close
|     Content-Type: text/html; charset=iso-8859-1
|     <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
|     <html><head>
|     <title>403 Forbidden</title>
|     </head><body>
|     <h1>Forbidden</h1>
|     <p>You don't have permission to access this resource.</p>
|     </body></html>
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Sat, 30 Dec 2023 05:33:53 GMT
|     Server: xxxx
|     X-Frame-Options: SAMEORIGIN
|     Strict-Transport-Security: max-age=31536000
|     X-Content-Type-Options: nosniff
|     Content-Length: 226
|     Connection: close
|     Content-Type: text/html; charset=iso-8859-1
|     <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
|     <html><head>
|     <title>400 Bad Request</title>
|     </head><body>
|     <h1>Bad Request</h1>
|     <p>Your browser sent a request that this server could not understand.<br />
|     </p>
|_    </body></html>
8080/tcp open   http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.37
|_http-favicon: Apache Tomcat
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-ser
vice :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=7%D=12/30%Time=658FFA63%P=x86_64-pc-linu
```



```
|_http-favicon: Apache Tomcat
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-ser
vice :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=7%D=12/30%Time=658FFA63%P=x86_64-pc-linu
SF:x-gnu%r(GetRequest,2260,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sat,\x2030\
SF:x20Dec\x202023\x2005:33:52\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-
SF:Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20default
SF:-src\x20https:\x20data:\x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'
SF:unsafe-eval';\x20worker-src\x20'self'\x20blob:;\x20frame-ancestors\x20'
SF:self';\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Type:\x20tex
SF:t/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x20Dec\x201969\x2023:59:
SF:59\x20GMT\r\nCache-Control:\x20no-cache\r\nPragma:\x20no-cache\r\nConte
SF:nt-Length:\x2029436\r\nSet-Cookie:\x20JSESSIONID=78s2sylrrhnm1fe703w1xv
SF:6zb89;\x20Path=/webconsole;\x20Secure;\x20HttpOnly\r\nConnection:\x20cl
SF:ose\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n
SF:\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></title>\n<
SF:link\x20href=\"/themes/lite1/css/typography\.css\?version=100253bfb2989
SF:01a314d20bea3289634\"\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20/>\
SF:n<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/loginstyleshee
SF:t\.css\?ver=100253bfb298")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2005:33:53\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2005:33:53\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
SF:nX-Content-Type-Options:\x20nosniff\r\nContent-Length:\x20226\r\nConnec
SF:tion:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n
SF:\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\"
SF:>\n<html><head>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<
SF:h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20t
SF:hat\x20this\x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n<
SF:/body></html>\n");
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (86%)
```



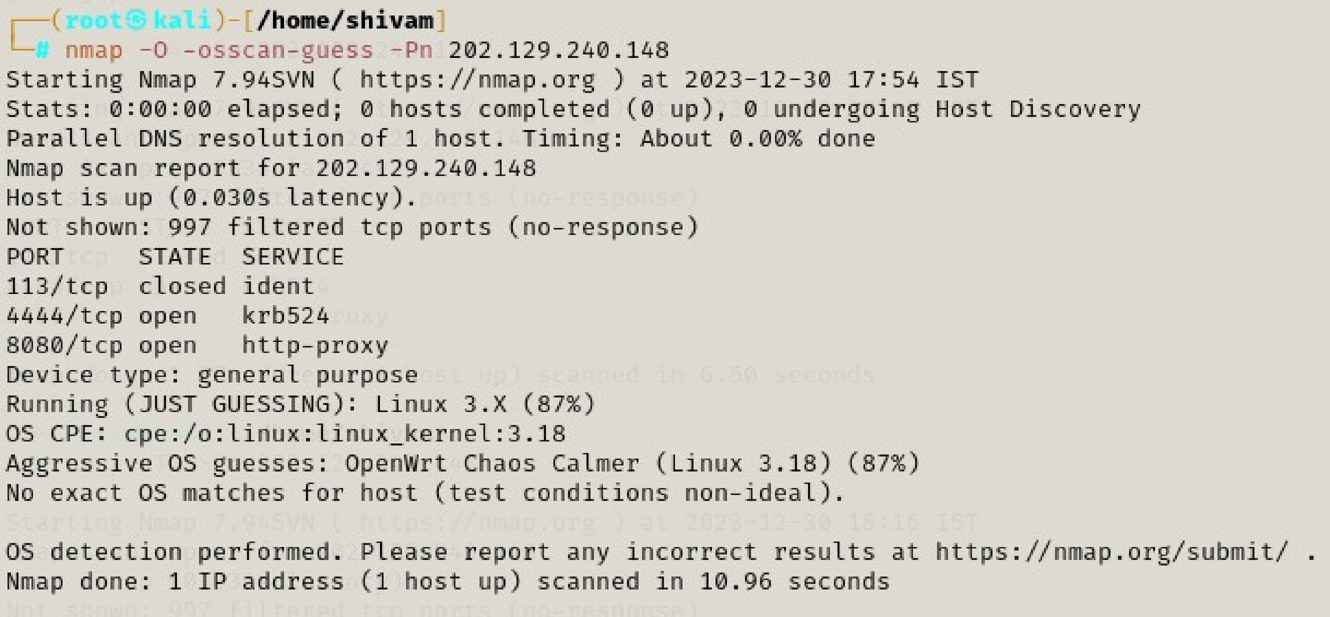
```
SF:t\.css\?ver=100253bfb298")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2005:33:53\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2005:33:53\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
SF:nX-Content-Type-Options:\x20nosniff\r\nContent-Length:\x20226\r\nConnec
SF:tion:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n
SF:\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\"
SF:>\n<html><head>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<
SF:h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20t
SF:hat\x20this\x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n<
SF:/body></html>\n");
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (86%)
```

```
OS CPE: cpe:/o:linux:linux_kernel:3.18
Aggressive OS guesses: OpenWrt Chaos Calmer (Linux 3.18) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   3.58 ms  gpon.net (192.168.1.1)
2   ...
3   7.12 ms  136.232.114.25
4   23.03 ms 172.26.40.5 (172.26.40.5)
5   19.19 ms 172.16.92.147 (172.16.92.147)
6   ... 7
8   32.89 ms 202.129.240.148

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 121.52 seconds

┌──(root㉿kali)-[/home/shivam]
└─# |
```

7) Aggressively Scan OS information

# Nmap -O -osscan-guess 202.192.240.148

Makes Nmap guess more aggressively

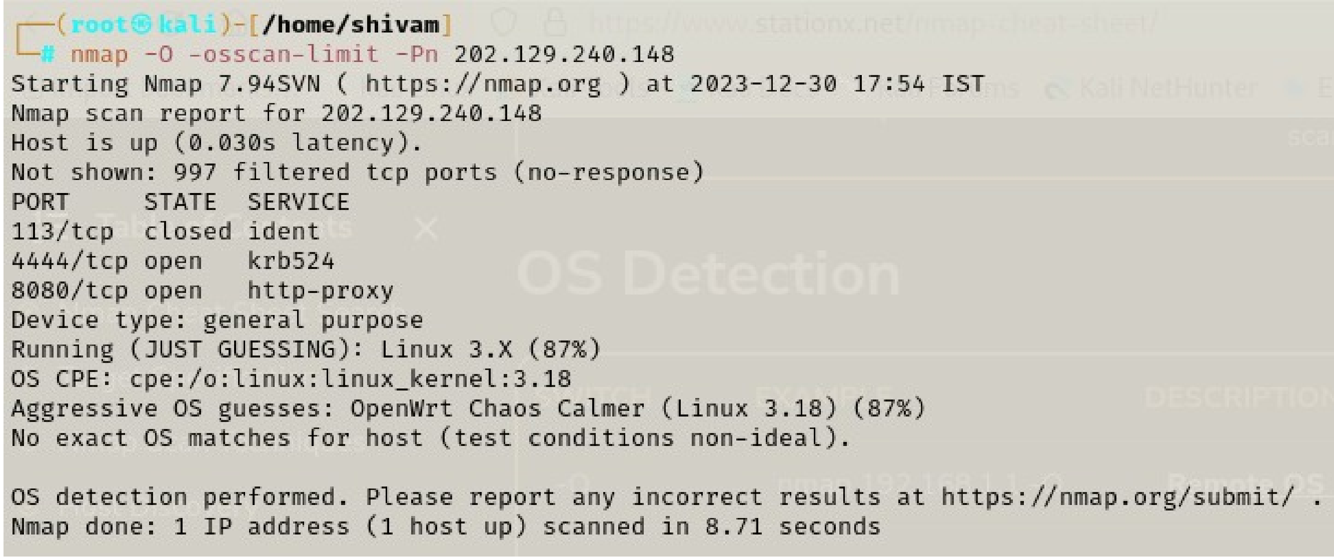


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -O -osscan-guess -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:54 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.18
Aggressive OS guesses: OpenWrt Chaos Calmer (Linux 3.18) (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.96 seconds
```

8) Scan OS information if at least one open and one closed port is detected

# Nmap -O -osscan-limit 202.192.240.148

If at least one open and one closed TCP port are not found it will not try OS detection against host

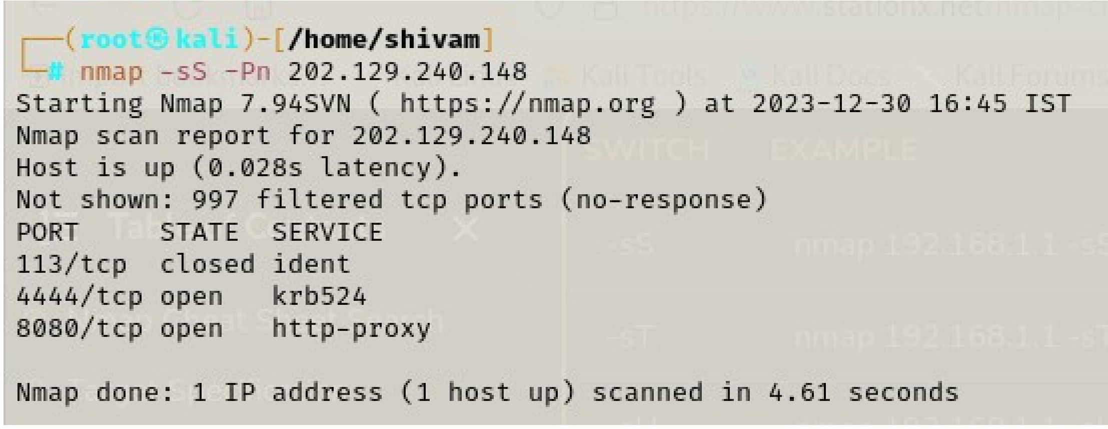


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -O -osscan-limit -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:54 IST
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.18
Aggressive OS guesses: OpenWrt Chaos Calmer (Linux 3.18) (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds
```

9) Scan TCP SYN Port

# Nmap -sS 202.192.240.148

TCP SYN port scan (Default)

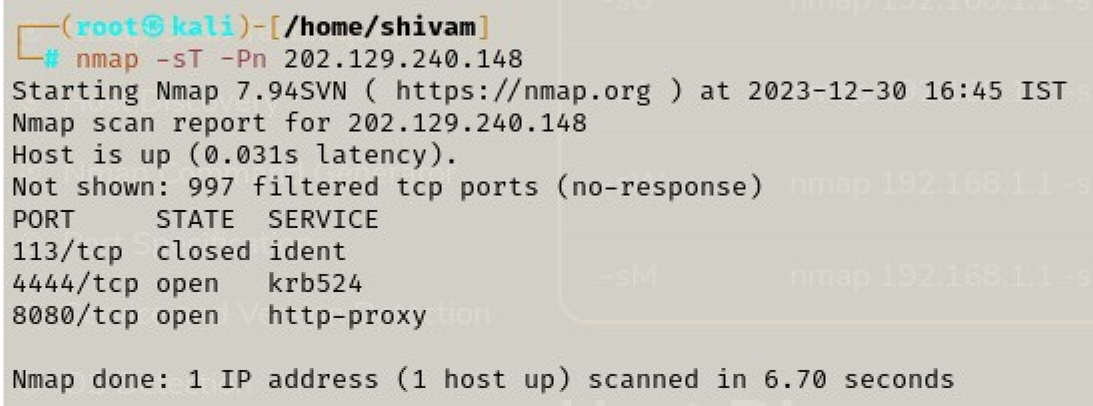


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sS -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:45 IST
Nmap scan report for 202.129.240.148
Host is up (0.028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds
```

10) TCP Port Scan

# Nmap -sT 202.192.240.148

TCP connect port scan (Default without root privilege)

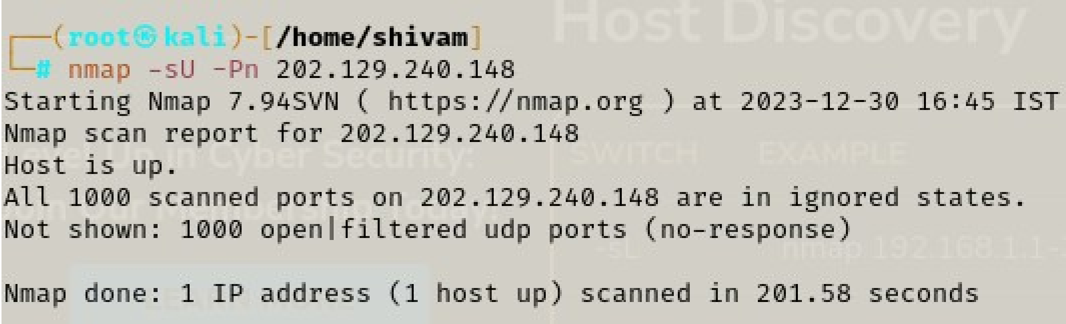


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sT -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:45 IST
Nmap scan report for 202.129.240.148
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
```

11) UDP Port Scan

# Nmap -sU 202.192.240.148

UDP port scan

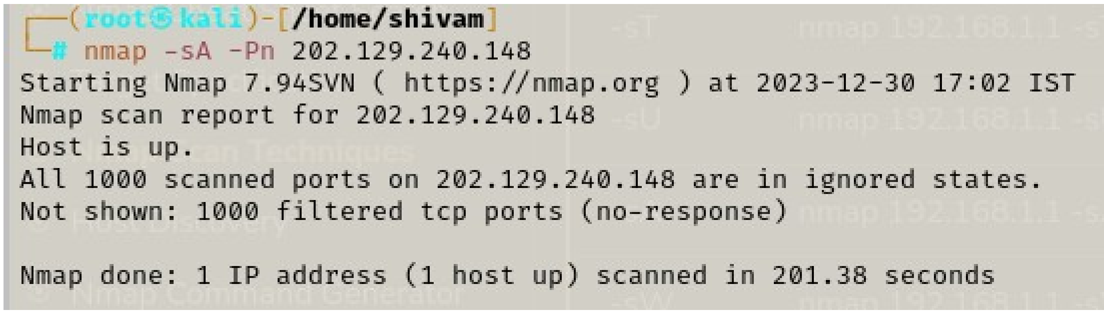


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sU -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:45 IST
Nmap scan report for 202.129.240.148
Host is up.
All 1000 scanned ports on 202.129.240.148 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.58 seconds
```

12) TCP ACK Port Scan

# Nmap -sA 202.192.240.148

TCP ACK port scan

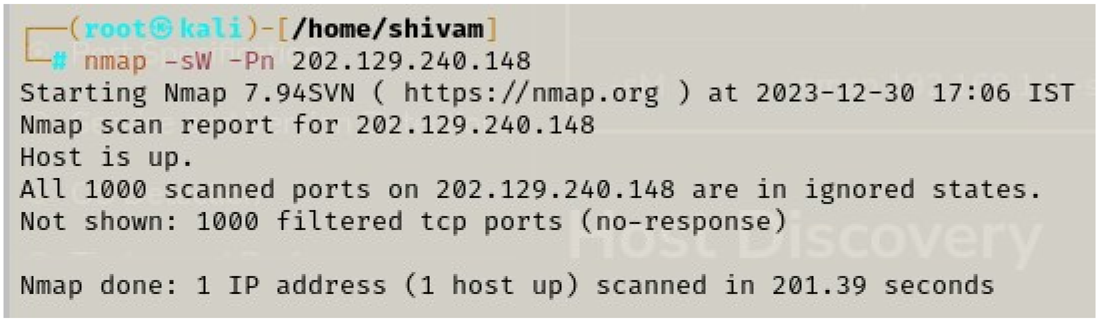


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sA -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:02 IST
Nmap scan report for 202.129.240.148
Host is up.
All 1000 scanned ports on 202.129.240.148 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.38 seconds
```

13) TCP Window Port Scan

# Nmap -sW 202.192.240.148

TCP Window port scan

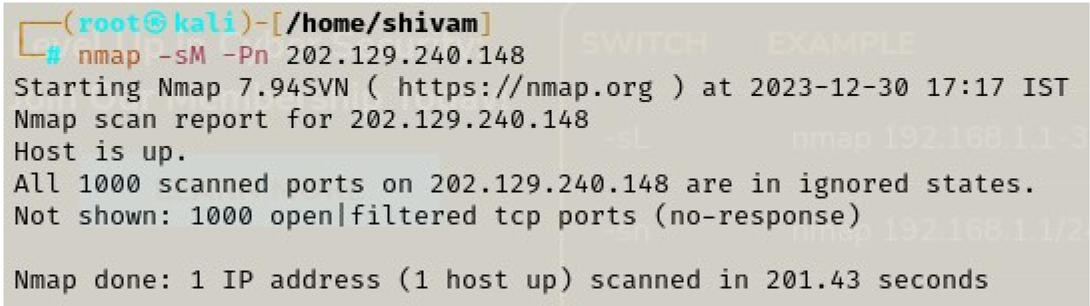


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sW -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:06 IST
Nmap scan report for 202.129.240.148
Host is up.
All 1000 scanned ports on 202.129.240.148 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.39 seconds
```

14) TCP Maimon port scan

# Nmap -sM 202.192.240.148

TCP Maimon port scan

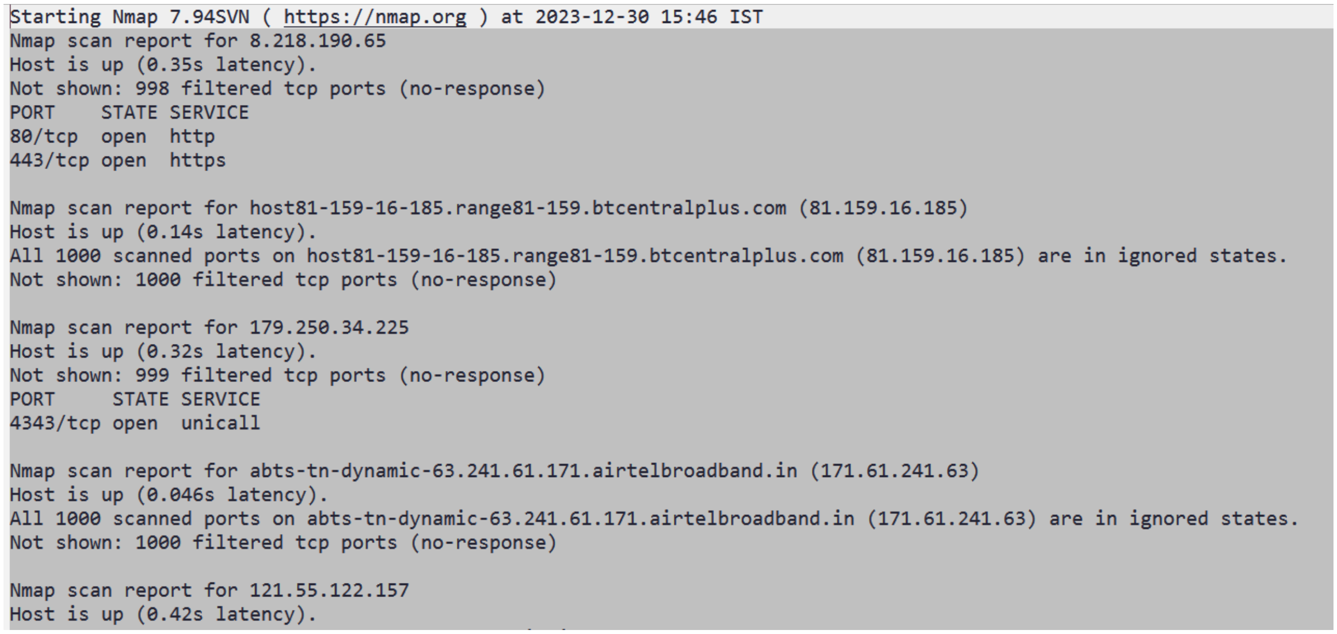


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sM -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:17 IST
Nmap scan report for 202.129.240.148
Host is up.
All 1000 scanned ports on 202.129.240.148 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.43 seconds
```

15) Random Host Scan

15) Nmap -iR 0

Scan random hosts

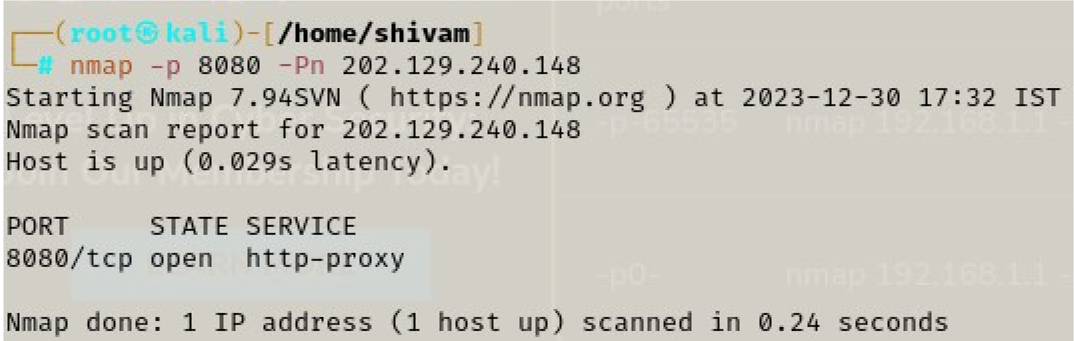


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 15:46 IST
Nmap scan report for 8.218.190.65
Host is up (0.35s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for host81-159-16-185.range81-159.btcentralplus.com (81.159.16.185)
Host is up (0.14s latency).
All 1000 scanned ports on host81-159-16-185.range81-159.btcentralplus.com (81.159.16.185) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 179.250.34.225
Host is up (0.32s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
4343/tcp open  unicall

Nmap scan report for abts-tn-dynamic-63.241.61.171.airtelbroadband.in (171.61.241.63)
Host is up (0.046s latency).
All 1000 scanned ports on abts-tn-dynamic-63.241.61.171.airtelbroadband.in (171.61.241.63) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 121.55.122.157
Host is up (0.42s latency).
```

16) Scan A Single Port

# Nmap -p 8080 -Pn 202.192.240.148

Port scan for port x

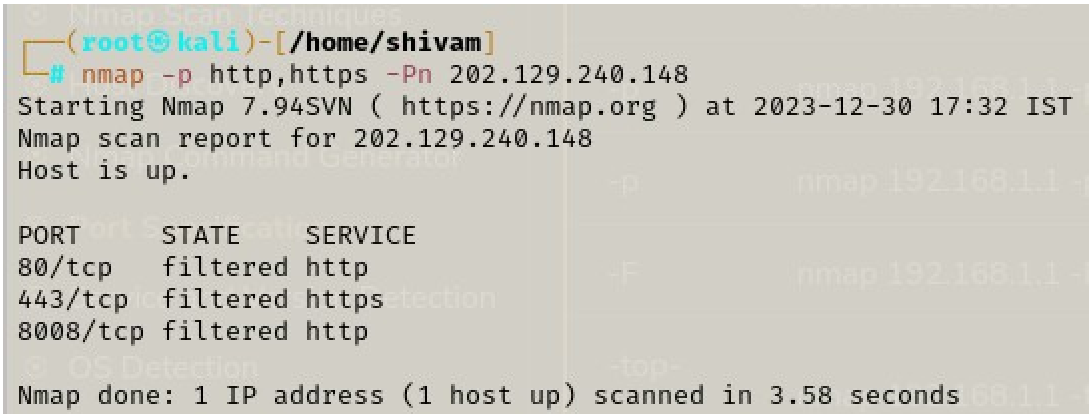


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p 8080 -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:32 IST
Nmap scan report for 202.129.240.148
Host is up (0.029s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

17) Port Scan for specific services

# Nmap -p http,https 202.192.240.148

Port scan from service name

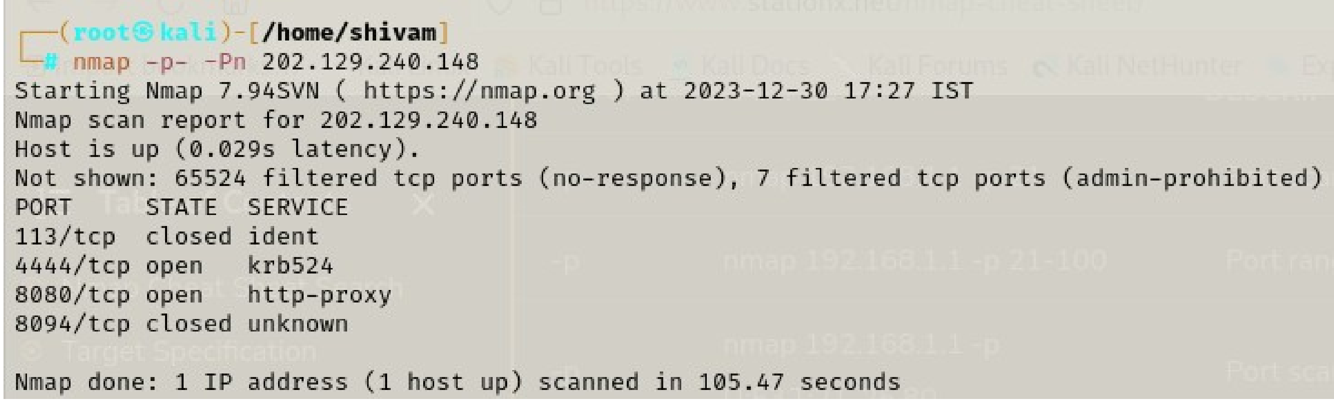


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p http,https -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:32 IST
Nmap scan report for 202.129.240.148
Host is up.

PORT     STATE    SERVICE
80/tcp   filtered http
443/tcp  filtered https
8008/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
```

18) All Port Scan

# Nmap -p- 202.192.240.148

Port scan all ports

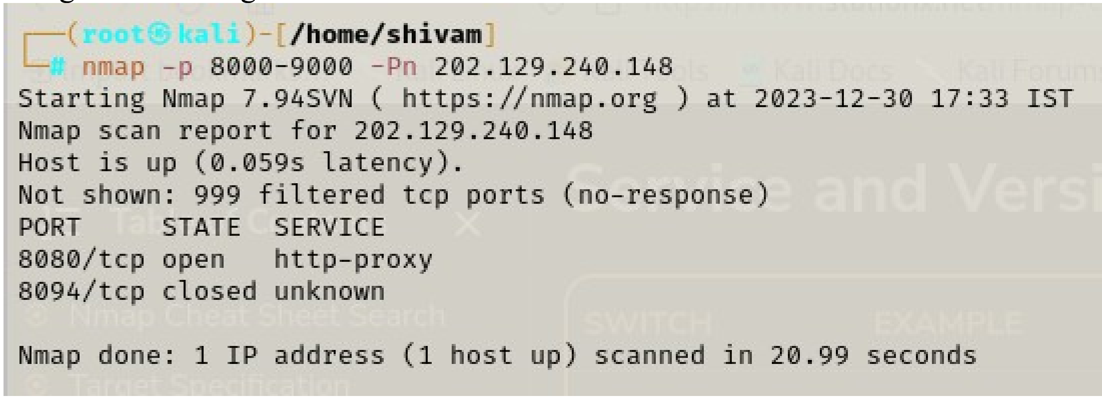


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p- -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:27 IST
Nmap scan report for 202.129.240.148
Host is up (0.029s latency).
Not shown: 65524 filtered tcp ports (no-response), 7 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
8094/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 105.47 seconds
```

19) Port Scan in Range

# Nmap -p 8000-9000 202.192.240.148

Port scan for given Port range

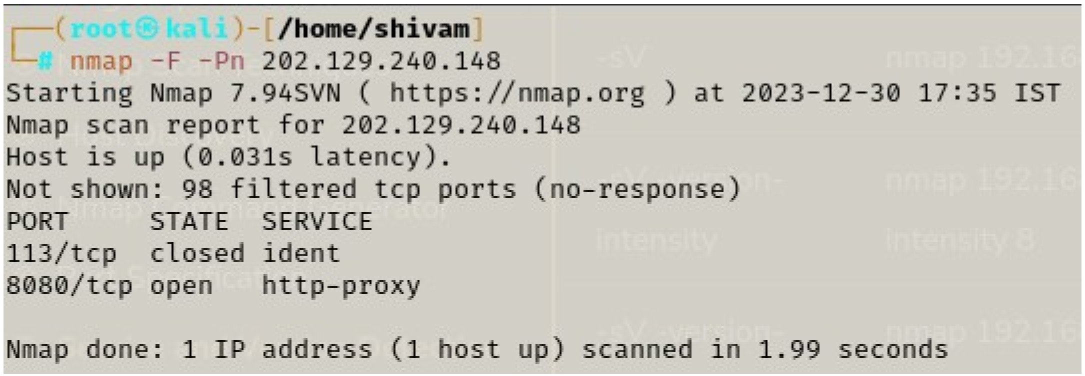


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p 8000-9000 -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:33 IST
Nmap scan report for 202.129.240.148
Host is up (0.059s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE  SERVICE
8080/tcp open   http-proxy
8094/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 20.99 seconds
```

20) Fast port scan

# Nmap -F 202.192.240.148

Fast port scan (100 ports)

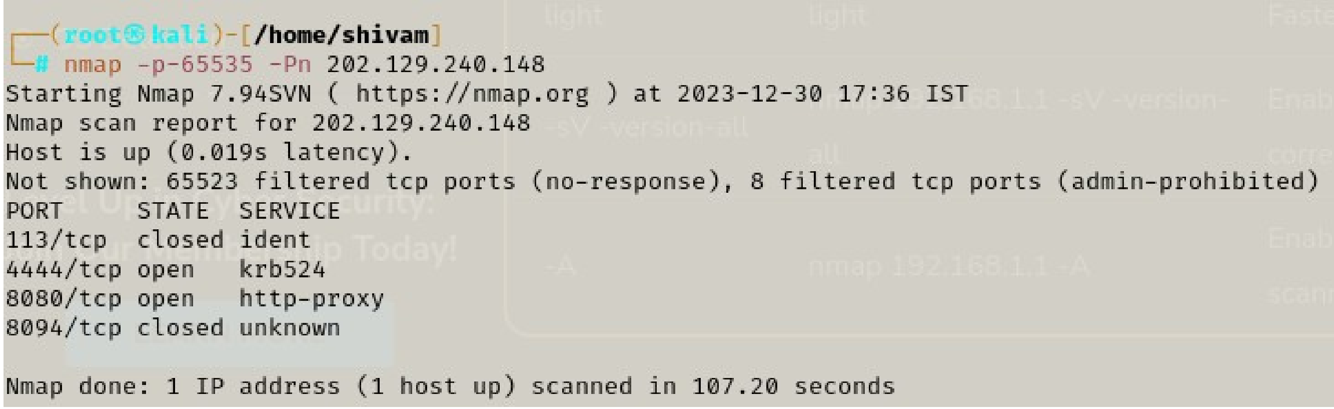


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -F -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:35 IST
Nmap scan report for 202.129.240.148
Host is up (0.031s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds
```

21) Scan all ports starting from port 1

# Nmap -p-65535 202.192.240.148

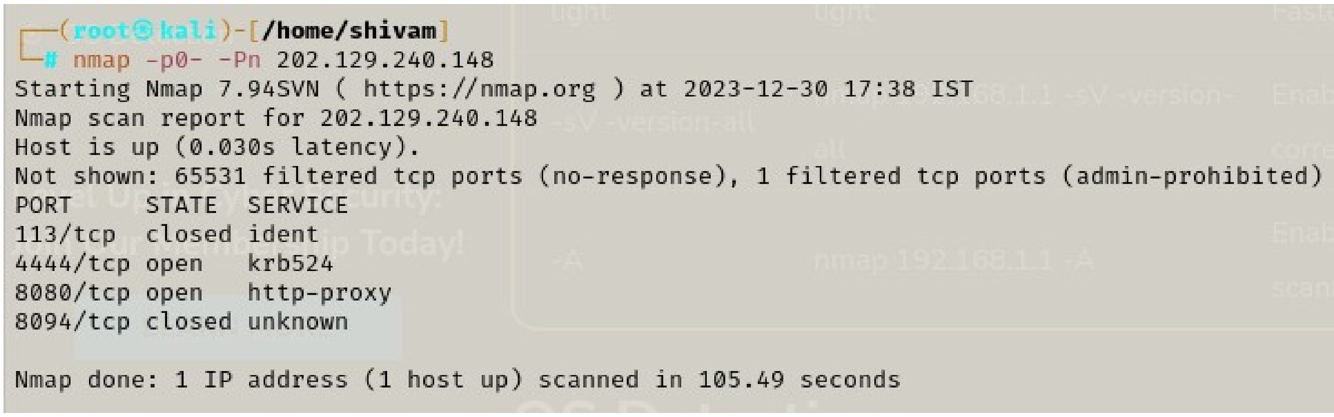
Leaving off initial port in range makes the scan start at port 1



```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p-65535 -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:36 IST
Nmap scan report for 202.129.240.148
Host is up (0.019s latency).
Not shown: 65523 filtered tcp ports (no-response), 8 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
8094/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 107.20 seconds
```

22) Scan all ports leaving of end ports

#Nmap -p0- 202.192.240.148
Leaving off end port in range makes the scan go through to port 65535

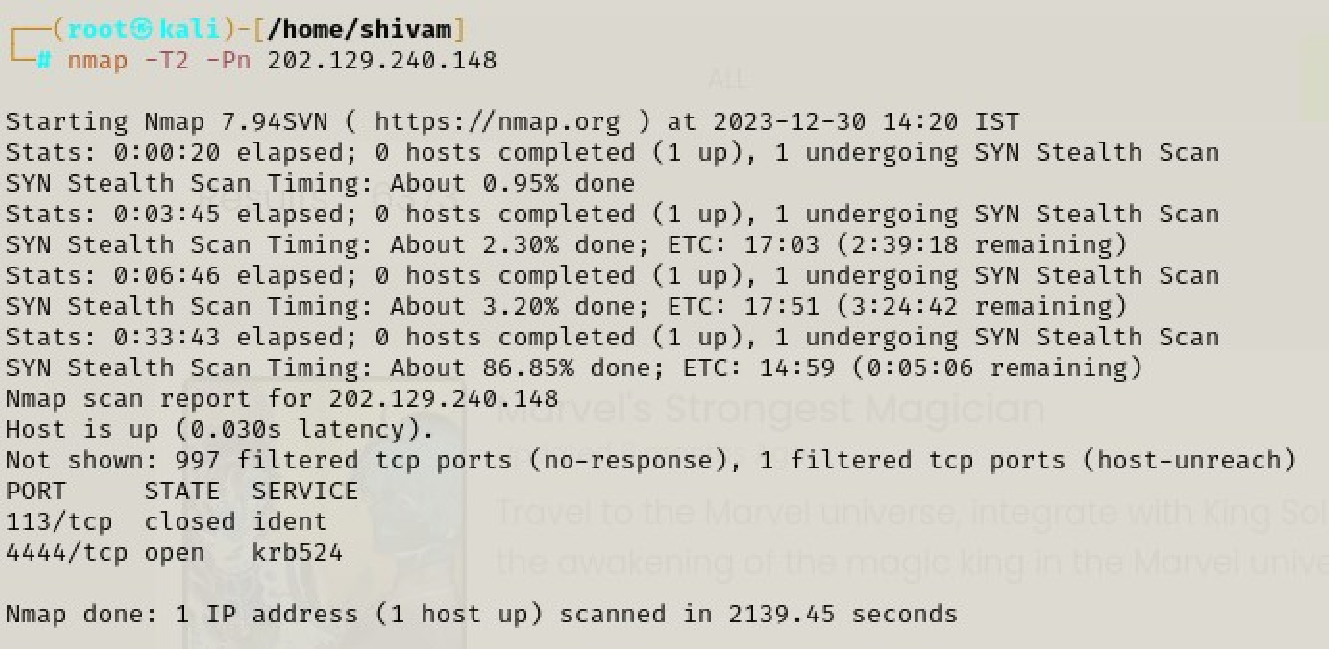


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -p0- -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:38 IST
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 65531 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy
8094/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 105.49 seconds
```

22) Polite Scan

# Nmap -T2 202.192.240.148

Polite (2) slows down the scan to use less bandwidth and use less target machine resources

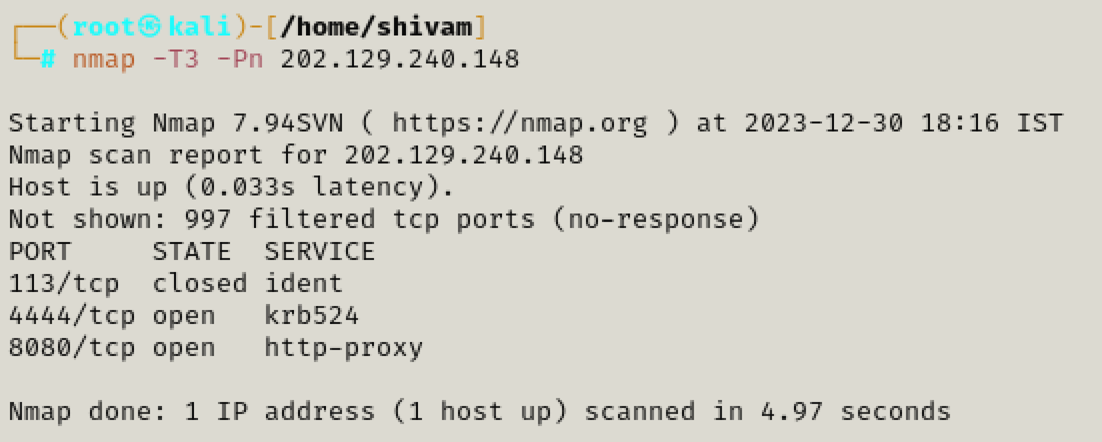


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -T2 -Pn 202.129.240.148

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 14:20 IST
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.95% done
Stats: 0:03:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.30% done; ETC: 17:03 (2:39:18 remaining)
Stats: 0:06:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.20% done; ETC: 17:51 (3:24:42 remaining)
Stats: 0:33:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.85% done; ETC: 14:59 (0:05:06 remaining)
Nmap scan report for 202.129.240.148
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524

Nmap done: 1 IP address (1 host up) scanned in 2139.45 seconds
```

24) Normal Scan

# Nmap -T3 202.192.240.148

Normal (3) which is default speed

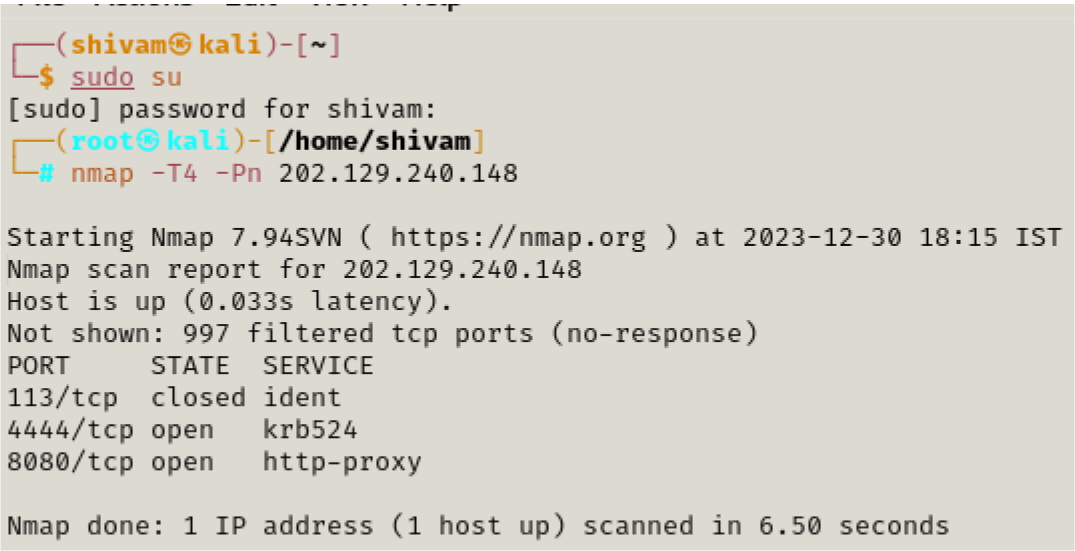


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -T3 -Pn 202.129.240.148

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 18:16 IST
Nmap scan report for 202.129.240.148
Host is up (0.033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
```

25) Aggressive Speed Scan

# Nmap -T4 202.192.240.148

Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network

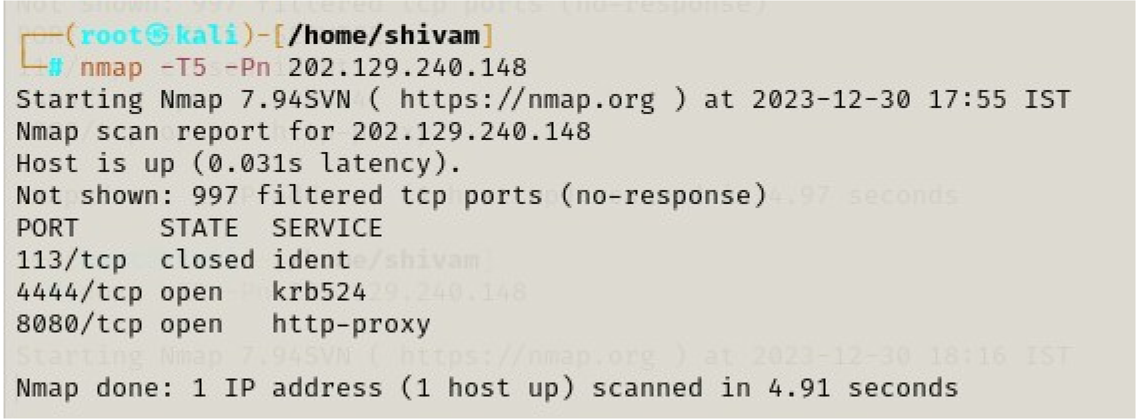


```
┌──(shivam㉿kali)-[~]
└─$ sudo su
[sudo] password for shivam:
┌──(root㉿kali)-[/home/shivam]
└─# nmap -T4 -Pn 202.129.240.148

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 18:15 IST
Nmap scan report for 202.129.240.148
Host is up (0.033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds
```

26) Insane Speed Scan

# Nmap -T5 202.192.240.148

Insane (5) speeds scan; assumes you are on an extraordinarily fast network

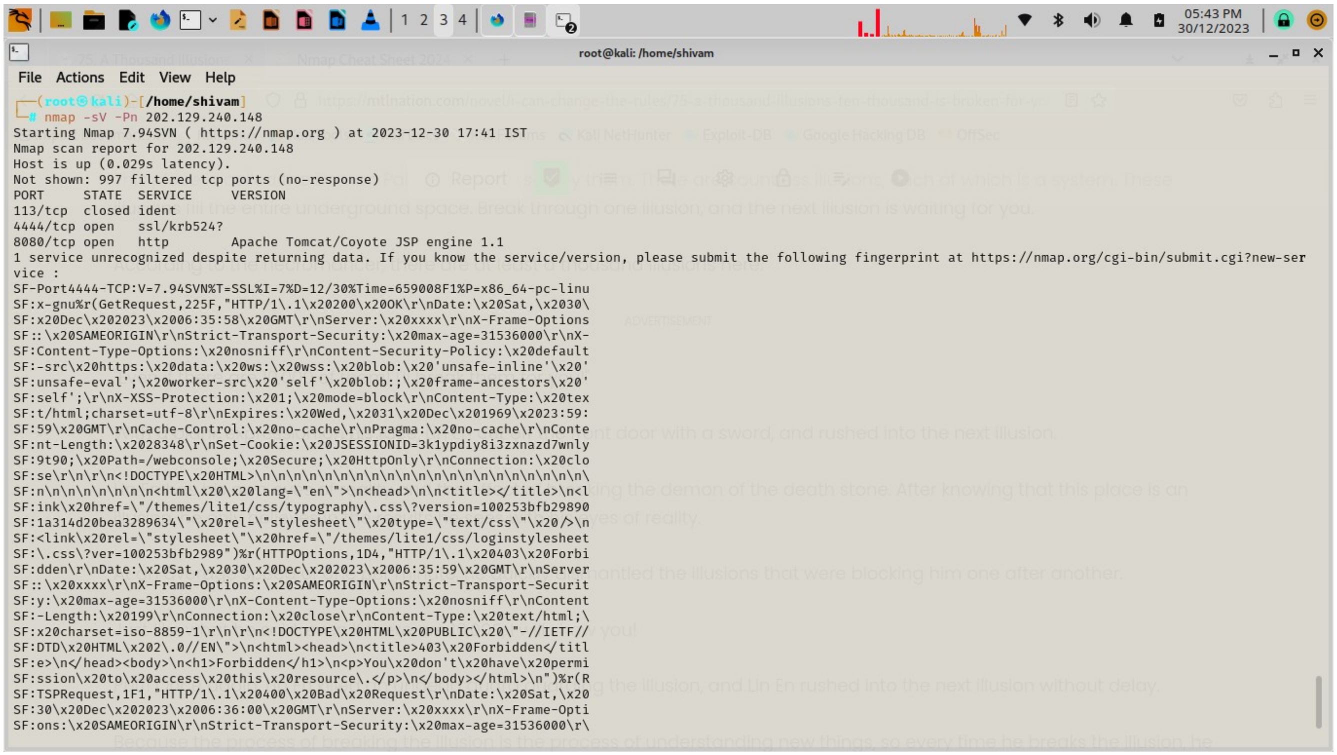


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -T5 -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:55 IST
Nmap scan report for 202.129.240.148
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
```

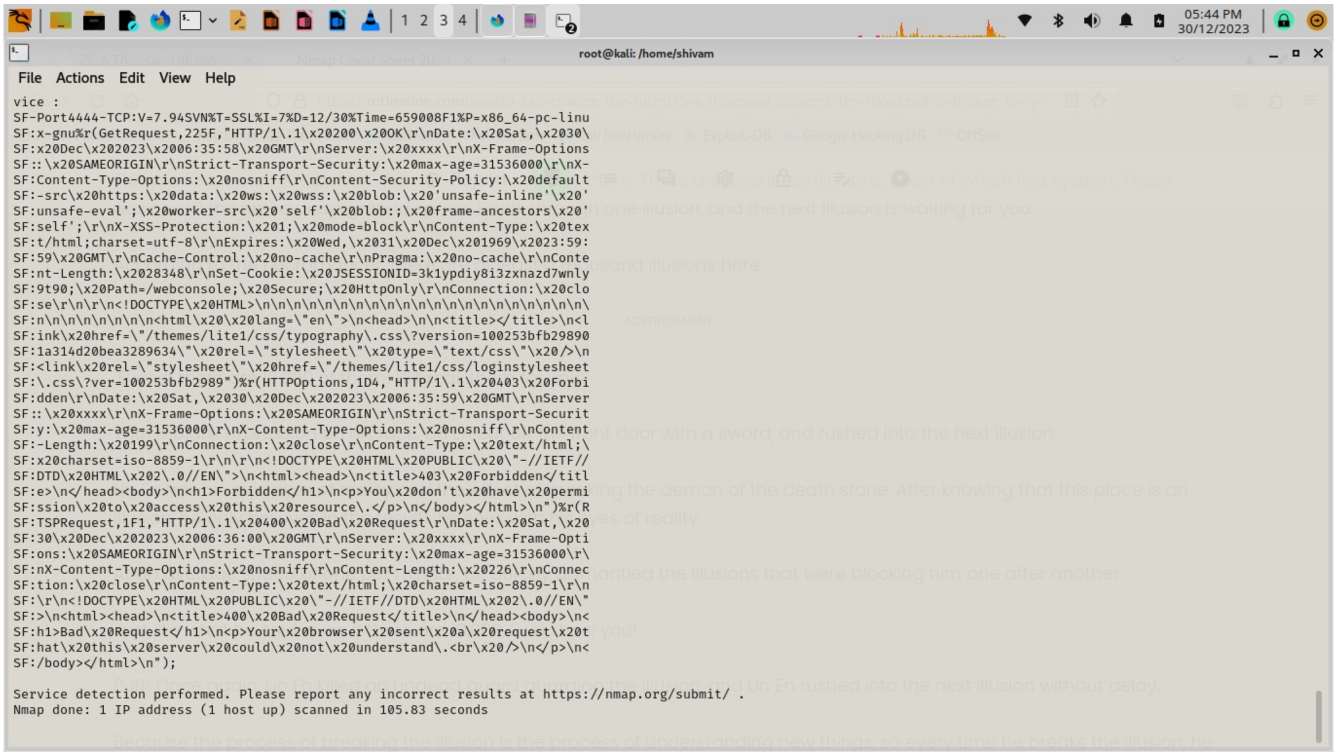
27) Service Version Scanning

# Nmap -sV 202.192.240.148

Attempts to determine the version of the service running on port



```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sV -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:41 IST
Nmap scan report for 202.129.240.148
Host is up (0.029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE      VERSION
113/tcp  closed ident
4444/tcp open   ssl/krb524?
8080/tcp open   http         Apache Tomcat/Coyote JSP engine 1.1
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-ser
vice :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=7%D=12/30%Time=659008F1%P=x86_64-pc-linu
SF:x-gnu%r(GetRequest,225F,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sat,\x2030\
SF:x20Dec\x202023\x2006:35:58\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-
SF:Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20default
SF:-src\x20https:\x20data:\x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'
SF:unsafe-eval';\x20worker-src\x20'self'\x20blob:;\x20frame-ancestors\x20'
SF:self';\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Type:\x20tex
SF:t/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x20Dec\x201969\x2023:59:
SF:59\x20GMT\r\nCache-Control:\x20no-cache\r\nPragma:\x20no-cache\r\nConte
SF:nt-Length:\x2028348\r\nSet-Cookie:\x20JSESSIONID=3k1ypdiy8i3zxnazd7wnly
SF:9t90;\x20Path=/webconsole;\x20Secure;\x20HttpOnly\r\nConnection:\x20clo
SF:se\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\
SF:n\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></title>\n<l
SF:ink\x20href=\"/themes/lite1/css/typography\.css\?version=100253bfb29890
SF:1a314d20bea3289634\"\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20/>\n
SF:<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/loginstylesheet
SF:\.css\?ver=100253bfb2989")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2006:35:59\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2006:36:00\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
```



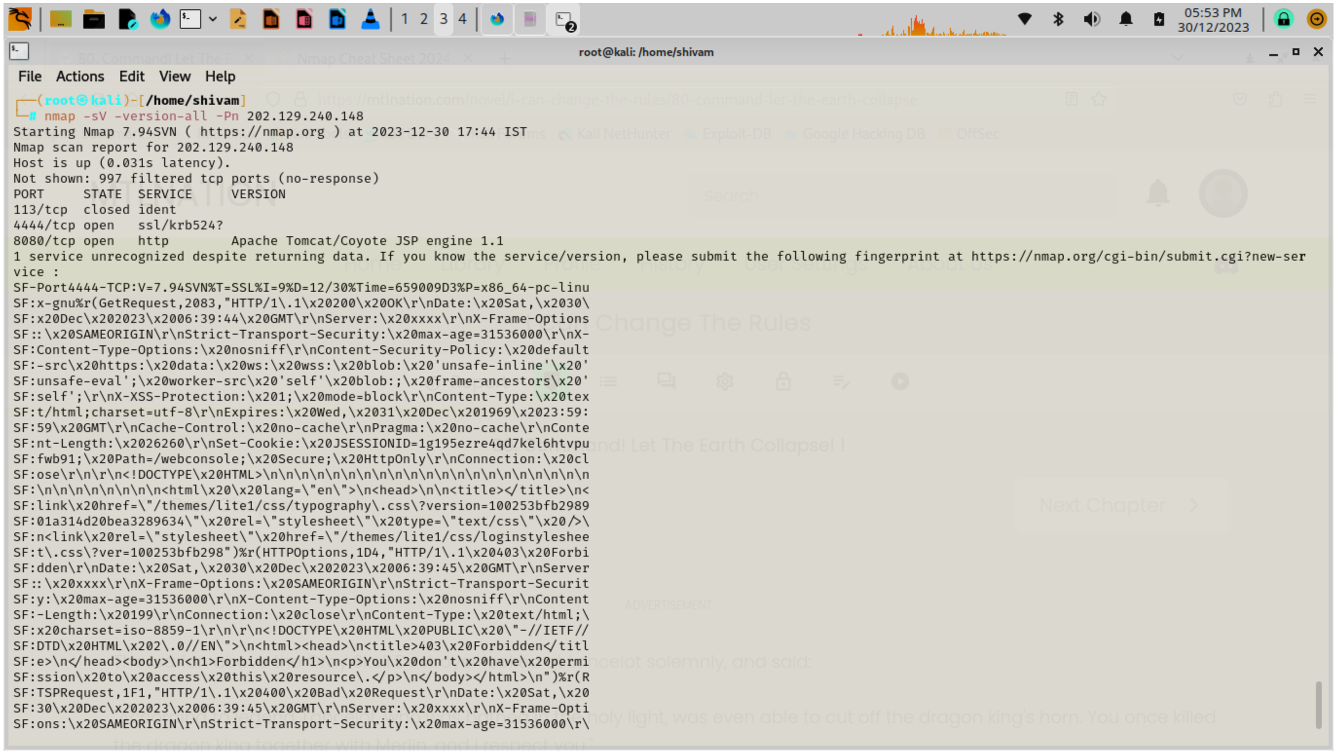
```
vice :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=7%D=12/30%Time=659008F1%P=x86_64-pc-linu
SF:x-gnu%r(GetRequest,225F,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sat,\x2030\
SF:x20Dec\x202023\x2006:35:58\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-
SF:Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20default
SF:-src\x20https:\x20data:\x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'
SF:unsafe-eval';\x20worker-src\x20'self'\x20blob:;\x20frame-ancestors\x20'
SF:self';\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Type:\x20tex
SF:t/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x20Dec\x201969\x2023:59:
SF:59\x20GMT\r\nCache-Control:\x20no-cache\r\nPragma:\x20no-cache\r\nConte
SF:nt-Length:\x2028348\r\nSet-Cookie:\x20JSESSIONID=3k1ypdiy8i3zxnazd7wnly
SF:9t90;\x20Path=/webconsole;\x20Secure;\x20HttpOnly\r\nConnection:\x20clo
SF:se\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\
SF:n\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></title>\n<l
SF:ink\x20href=\"/themes/lite1/css/typography\.css\?version=100253bfb29890
SF:1a314d20bea3289634\"\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20/>\n
SF:<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/loginstylesheet
SF:\.css\?ver=100253bfb2989")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2006:35:59\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2006:36:00\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
```

```
SF:nX-Content-Type-Options:\x20nosniff\r\nContent-Length:\x20226\r\nConnec
SF:tion:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n
SF:\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\"
SF:>\n<html><head>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<
SF:h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20t
SF:hat\x20this\x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n<
SF:/body></html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.83 seconds
```

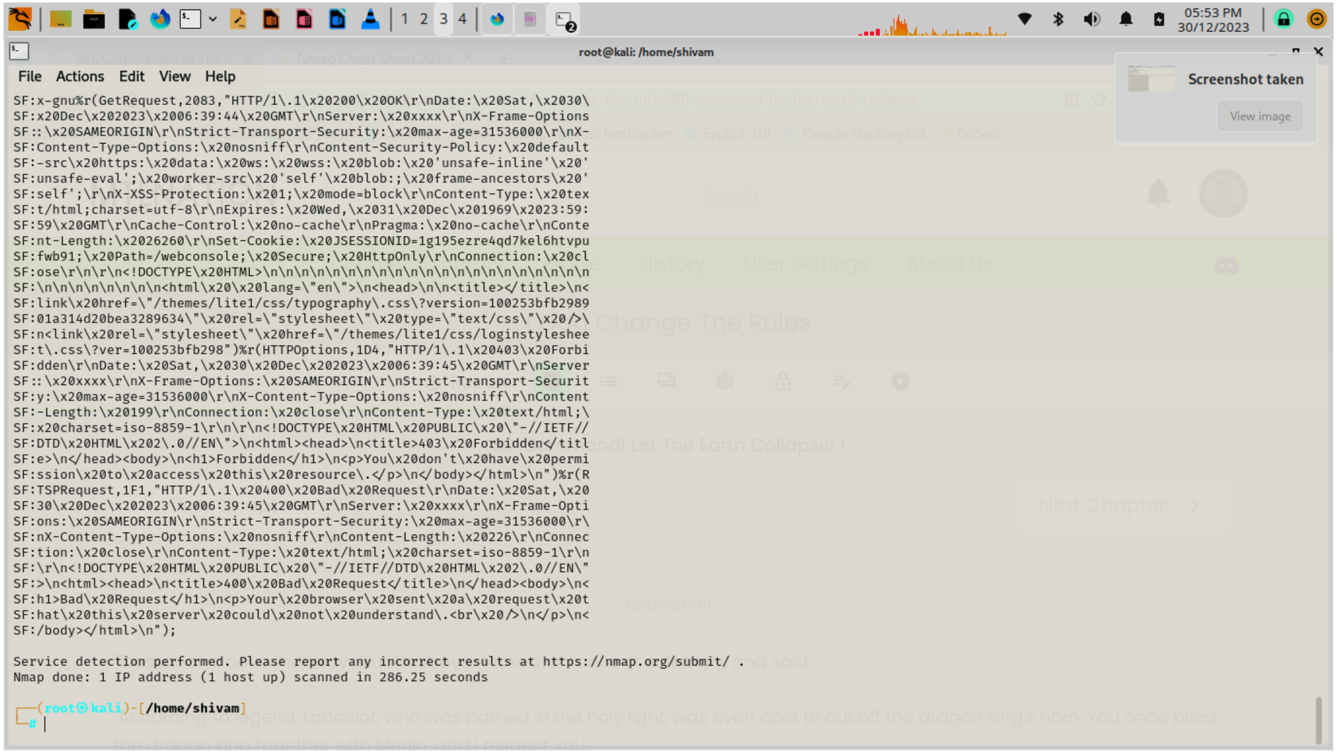
28) High Accuracy Service Version Scanning

# Nmap -sV -version-all 202.192.240.148

Enable intensity level 9. Higher possibility of correctness. Slower



```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -sV -version-all -Pn 202.129.240.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 17:44 IST
Nmap scan report for 202.129.240.148
Host is up (0.031s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE  SERVICE    VERSION
113/tcp   closed ident
4444/tcp  open   ssl/krb524?
8080/tcp  open   http       Apache Tomcat/Coyote JSP engine 1.1
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-ser
vice :
SF-Port4444-TCP:V=7.94SVN%T=SSL%I=9%D=12/30%Time=659009D3%P=x86_64-pc-linu
SF:x-gnu%r(GetRequest,2083,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sat,\x2030\
SF:x20Dec\x202023\x2006:39:44\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-
SF:Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20default
SF:-src\x20https:\x20data:\x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'
SF:unsafe-eval';\x20worker-src\x20'self'\x20blob:;\x20frame-ancestors\x20'
SF:self';\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Type:\x20tex
SF:t/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x20Dec\x201969\x2023:59:
SF:59\x20GMT\r\nCache-Control:\x20no-cache\r\nPragma:\x20no-cache\r\nConte
SF:nt-Length:\x2026260\r\nSet-Cookie:\x20JSESSIONID=1g195ezre4qd7kel6htvpu
SF:fwb91;\x20Path=/webconsole;\x20Secure;\x20HttpOnly\r\nConnection:\x20cl
SF:ose\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n
SF:\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></title>\n<
SF:link\x20href=\"/themes/lite1/css/typography\.css\?version=100253bfb2989
SF:01a314d20bea3289634\"\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20/>\
SF:n<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/loginstyleshee
SF:t\.css\?ver=100253bfb298")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2006:39:45\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2006:39:45\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
```

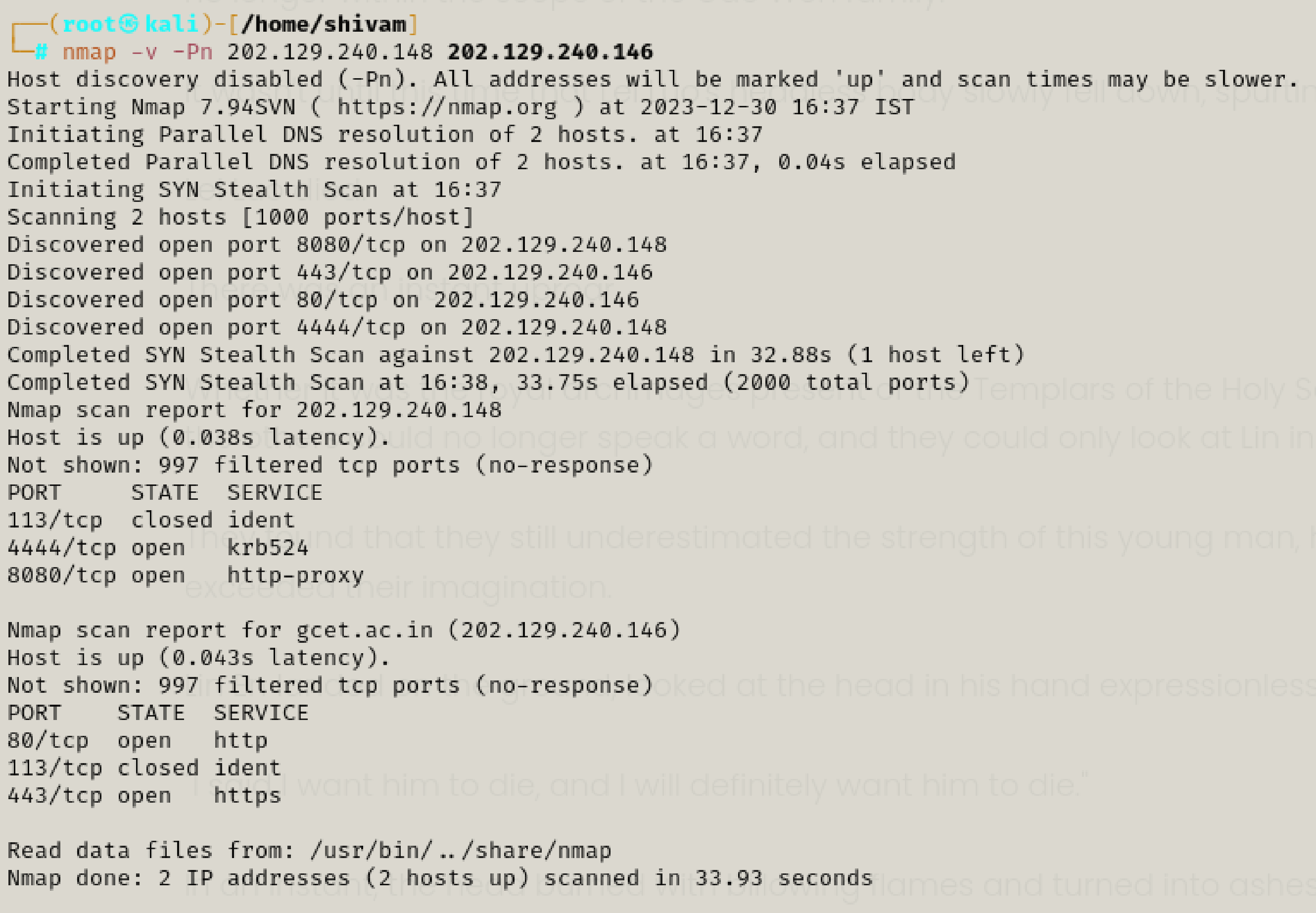


```
SF:x-gnu%r(GetRequest,2083,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sat,\x2030\
SF:x20Dec\x202023\x2006:39:44\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-
SF:Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20default
SF:-src\x20https:\x20data:\x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'
SF:unsafe-eval';\x20worker-src\x20'self'\x20blob:;\x20frame-ancestors\x20'
SF:self';\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Type:\x20tex
SF:t/html;charset=utf-8\r\nExpires:\x20Wed,\x2031\x20Dec\x201969\x2023:59:
SF:59\x20GMT\r\nCache-Control:\x20no-cache\r\nPragma:\x20no-cache\r\nConte
SF:nt-Length:\x2026260\r\nSet-Cookie:\x20JSESSIONID=1g195ezre4qd7kel6htvpu
SF:fwb91;\x20Path=/webconsole;\x20Secure;\x20HttpOnly\r\nConnection:\x20cl
SF:ose\r\n\r\n<!DOCTYPE\x20HTML>\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n
SF:\n\n\n\n\n\n\n\n<html\x20\x20lang=\"en\">\n<head>\n\n<title></title>\n<
SF:link\x20href=\"/themes/lite1/css/typography\.css\?version=100253bfb2989
SF:01a314d20bea3289634\"\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20/>\
SF:n<link\x20rel=\"stylesheet\"\x20href=\"/themes/lite1/css/loginstyleshee
SF:t\.css\?ver=100253bfb298")%r(HTTPOptions,1D4,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nDate:\x20Sat,\x2030\x20Dec\x202023\x2006:39:45\x20GMT\r\nServer
SF::\x20xxxx\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Securit
SF:y:\x20max-age=31536000\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Length:\x20199\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\
SF:x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//
SF:DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>403\x20Forbidden</titl
SF:e>\n</head><body>\n<h1>Forbidden</h1>\n<p>You\x20don't\x20have\x20permi
SF:ssion\x20to\x20access\x20this\x20resource\.</p>\n</body></html>\n")%r(R
SF:TSPRequest,1F1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x20
SF:30\x20Dec\x202023\x2006:39:45\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Opti
SF:ons:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\
SF:nX-Content-Type-Options:\x20nosniff\r\nContent-Length:\x20226\r\nConnec
SF:tion:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n
SF:\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\"
SF:>\n<html><head>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<
SF:h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20t
SF:hat\x20this\x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n<
SF:/body></html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 286.25 seconds

┌──(root㉿kali)-[/home/shivam]
└─# |
```

29) Scan Multiple Hosts.

# nmap -v 202.192.240.148 202.192.240.146

scans multiple ip addresses

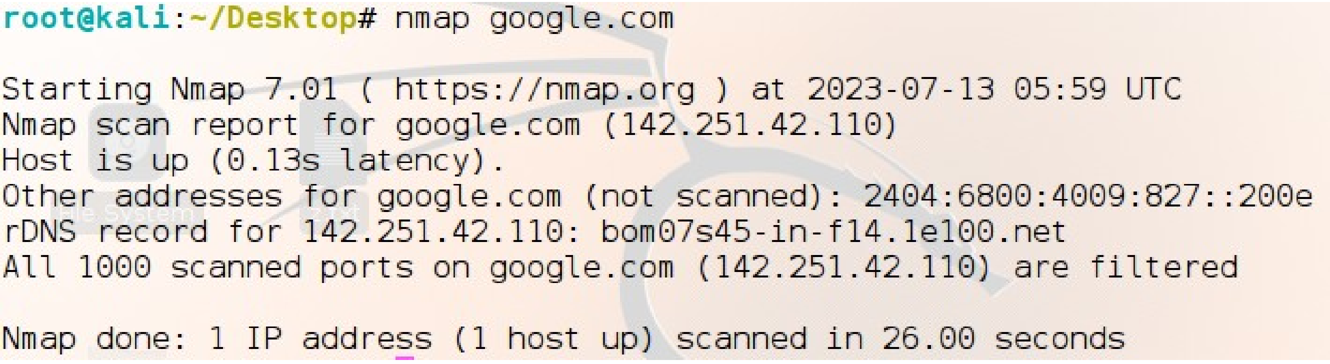


```
┌──(root㉿kali)-[/home/shivam]
└─# nmap -v -Pn 202.129.240.148 202.129.240.146
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 16:37 IST
Initiating Parallel DNS resolution of 2 hosts. at 16:37
Completed Parallel DNS resolution of 2 hosts. at 16:37, 0.04s elapsed
Initiating SYN Stealth Scan at 16:37
Scanning 2 hosts [1000 ports/host]
Discovered open port 8080/tcp on 202.129.240.148
Discovered open port 443/tcp on 202.129.240.146
Discovered open port 80/tcp on 202.129.240.146
Discovered open port 4444/tcp on 202.129.240.148
Completed SYN Stealth Scan against 202.129.240.148 in 32.88s (1 host left)
Completed SYN Stealth Scan at 16:38, 33.75s elapsed (2000 total ports)
Nmap scan report for 202.129.240.148
Host is up (0.038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
113/tcp  closed ident
4444/tcp open   krb524
8080/tcp open   http-proxy

Nmap scan report for gcet.ac.in (202.129.240.146)
Host is up (0.043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Read data files from: /usr/bin/../share/nmap
Nmap done: 2 IP addresses (2 hosts up) scanned in 33.93 seconds
```

30) Scanning host using Host’s name

# Nmap google.com

Scan a domain



```
root@kali:~/Desktop# nmap google.com

Starting Nmap 7.01 ( https://nmap.org ) at 2023-07-13 05:59 UTC
Nmap scan report for google.com (142.251.42.110)
Host is up (0.13s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:827::200e
rDNS record for 142.251.42.110: bom07s45-in-f14.1e100.net
All 1000 scanned ports on google.com (142.251.42.110) are filtered

Nmap done: 1 IP address (1 host up) scanned in 26.00 seconds
```

Important Terminologies

1) TCP SYN Scan

- The TCP SYN scan -- a variant of the traditional SYN scan -- is commonly used. It is a quick and efficient scan, not restricted by firewalls since it never completes the full TCP connection. For this reason, TCP SYN scanning is also commonly referred to as *half-open scanning* and can indicate open, filtered and closed port states.
- It works by sending a SYN packet in an attempt to open a connection. A SYN/ACK response indicates an open TCP port, whereas an RST response indicates a closed port. If no response is received or if an Internet Control Message Protocol (ICMP) unreachable error is received, it indicates a filtered state.
- On rare occasions, a SYN packet may be returned without the ACK flag, indicating an open port and the presence of a TCP three-way handshake.
- Syn Scan - SYN scanning is a tactic that a malicious hacker can use to determine the state of a communications port without establishing a full connection.

2) TCP FIN Scan

- A **FIN scan** is when an attacker sends a packet with only the FIN flag enabled. If an attacker sends the FIN packet to the target, it means the attacker is requesting the connection be terminate but there was no established connection to close. This would confuse the target. If the target does not respond, it means the port is open. If the target replies with an RST packet, the port on the target is closed

3) Port Scan

- Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.
- This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.
- The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user’s device.
- After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.