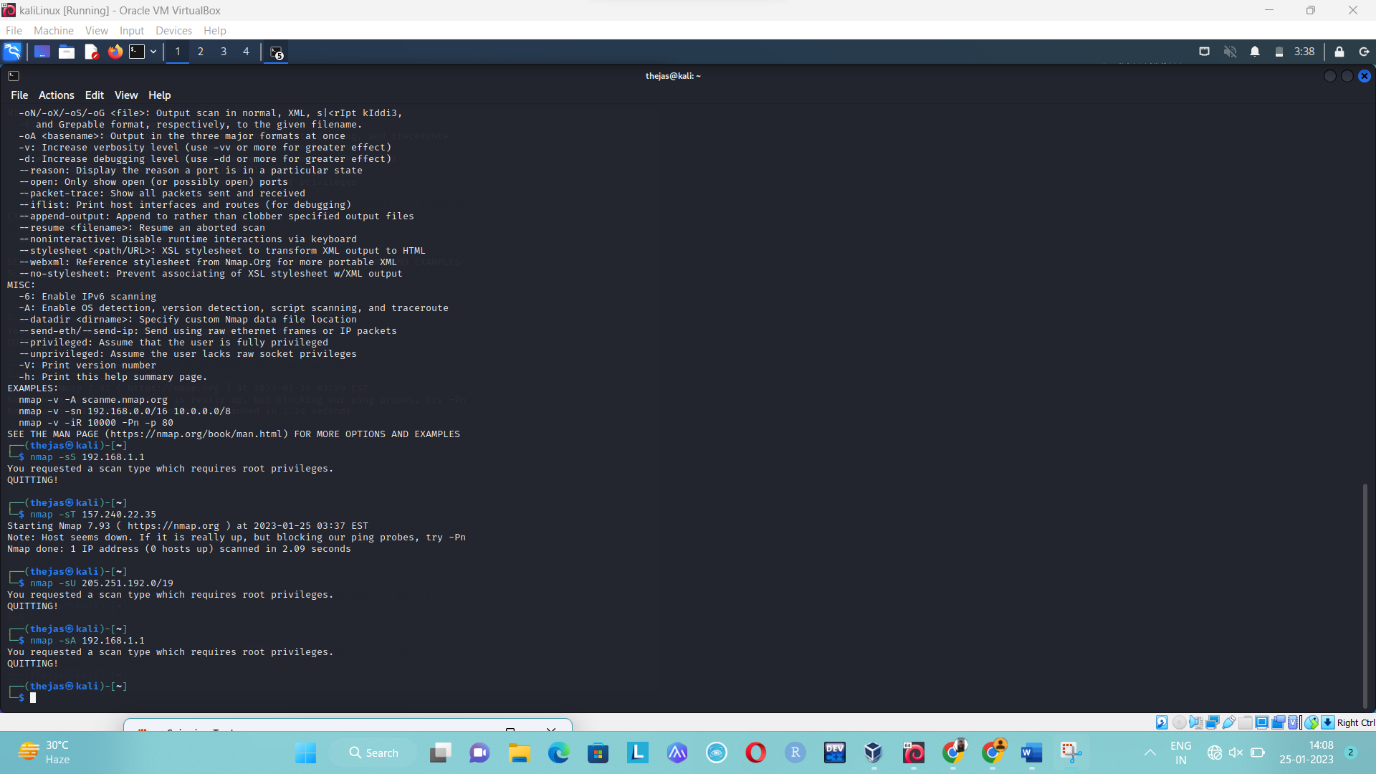
***Exp 1***

**Scanning Techniques**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-sS** | **TCP syn port scan** | **nmap -sS 192.168.1.1** |
| **-sT** | **TCP connect port scan** | **nmap -sT 192.168.1.1** |
| **–sU** | **UDP port scan** | **nmap –sU 192.168.1.1** |
| **–sA** | **nmap –sA 192.168.1.1** |  |



|  |  |  |
| --- | --- | --- |
| -Pn | only port scan | nmap -Pn192.168.1.1 |
| -sn | only host discover | nmap -sn192.168.1.1 |
| -PR | arp discovery on a local network | nmap -PR192.168.1.1 |
| -n | disable DNS resolution | nmap -n 192.168.1.1 |



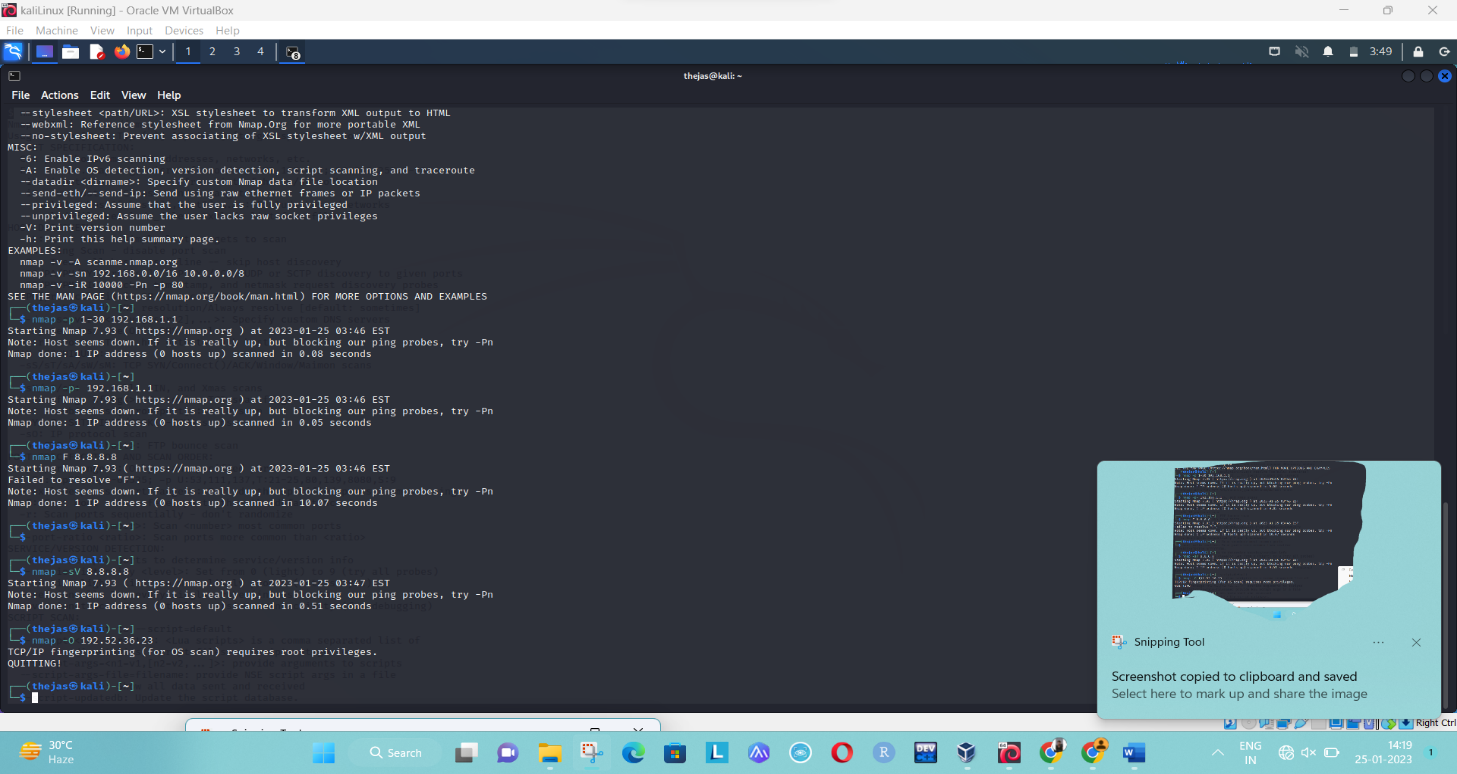
**Port Specification**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-p** | **specify a port or port range** | **nmap -p 1-30 192.168.1.1** |
| **-p-** | **scan all ports** | **nmap -p- 192.168.1.1** |
| **F** | **fast port scan** | **nmap -F 192.168.1.1** |

Step 5:-

***Service Version and OS Detection***

|  |  |  |
| --- | --- | --- |
| Flag | Use | Example |
| -sV | detect the version of services running | nmap -sV 192.168.1.1 |
| -A | aggressive scan | nmap -A 192.168.1.1 |
| -O | detect operating system of the target | nmap -O 192.168.1.1 |



Exp 7

facebook.com

whois information

[Whois](https://who.is/whois/facebook.com) [DNS Records](https://who.is/dns/facebook.com) [Diagnostics](https://who.is/tools/facebook.com)

cache expires in 13 hours, 39 minutes and 7 seconds  
[refresh](https://who.is/whois/facebook.com?forceRefresh=beb3004639204177239d348f877fad59583fd90eb01de1b09821e10ae72ce6e4)

Registrar Info

Name

RegistrarSafe, LLC

Whois Server

whois.registrarsafe.com

Referral URL

https://www.registrarsafe.com

Status

clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited  
clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited  
clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited  
serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited  
serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited  
serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited

Important Dates

Expires On

2031-03-30

Registered On

1997-03-29

Updated On

2022-01-26

Name Servers

[A.NS.FACEBOOK.COM](https://who.is/nameserver/A.NS.FACEBOOK.COM)

[129.134.30.12](https://who.is/whois-ip/ip-address/129.134.30.12)

[B.NS.FACEBOOK.COM](https://who.is/nameserver/B.NS.FACEBOOK.COM)

[129.134.31.12](https://who.is/whois-ip/ip-address/129.134.31.12)

[C.NS.FACEBOOK.COM](https://who.is/nameserver/C.NS.FACEBOOK.COM)

[185.89.218.12](https://who.is/whois-ip/ip-address/185.89.218.12)

[D.NS.FACEBOOK.COM](https://who.is/nameserver/D.NS.FACEBOOK.COM)

[185.89.219.12](https://who.is/whois-ip/ip-address/185.89.219.12)

Similar Domains

[faceb%c3%b6ok.com](https://who.is/whois/faceb%c3%b6ok.com) | [faceb--k.com](https://who.is/whois/faceb--k.com) | [faceb--kbasedbiz.com](https://who.is/whois/faceb--kbasedbiz.com) | [faceb--l.com](https://who.is/whois/faceb--l.com) | [faceb-activate.com](https://who.is/whois/faceb-activate.com) | [faceb-color.co.cc](https://who.is/whois/faceb-color.co.cc) | [faceb-design.com](https://who.is/whois/faceb-design.com) | [faceb-error.com](https://who.is/whois/faceb-error.com) | [faceb-junkie.com](https://who.is/whois/faceb-junkie.com) | [faceb-ok.com](https://who.is/whois/faceb-ok.com) | [faceb-ook.com](https://who.is/whois/faceb-ook.com) | [faceb-renovation.com](https://who.is/whois/faceb-renovation.com) | [faceb-server.com](https://who.is/whois/faceb-server.com) | [faceb-survey.com](https://who.is/whois/faceb-survey.com) | [faceb.be](https://who.is/whois/faceb.be) | [faceb.biz](https://who.is/whois/faceb.biz) | [faceb.br](https://who.is/whois/faceb.br) | [faceb.cc](https://who.is/whois/faceb.cc) | [faceb.chat](https://who.is/whois/faceb.chat) | [faceb.co](https://who.is/whois/faceb.co) |

Registrar Data

We will display stored WHOIS data for up to 30 days.  
[refresh](https://who.is/whois/facebook.com?forceRefresh=beb3004639204177239d348f877fad59583fd90eb01de1b09821e10ae72ce6e4)  
  
[Make Private Now](https://who.is/whois/privacy/facebook.com)

**Registrant Contact Information:**

**Name**

Domain Admin

**Organization**

Meta Platforms, Inc.

**Address**

1601 Willow Rd

**City**

Menlo Park

**State / Province**

CA

**Postal Code**

94025

**Country**

US

**Phone**

+1.6505434800

**Email**



**Administrative Contact Information:**

**Name**

Domain Admin

**Organization**

Meta Platforms, Inc.

**Address**

1601 Willow Rd

**City**

Menlo Park

**State / Province**

CA

**Postal Code**

94025

**Country**

US

**Phone**

+1.6505434800

**Email**



**Technical Contact Information:**

**Name**

Domain Admin

**Organization**

Meta Platforms, Inc.

**Address**

1601 Willow Rd

**City**

Menlo Park

**State / Province**

CA

**Postal Code**

94025

**Country**

US

**Phone**

+1.6505434800

**Email**



Information Updated: 2023-01-24 19:20:17

DNS Records for facebook.com

| **Hostname** | **Type** | **TTL** | **Priority** | **Content** |
| --- | --- | --- | --- | --- |
| facebook.com | SOA | 3340 |  | a.ns.facebook.com dns@facebook.com 3191226929 14400 1800 604800 300 |
| facebook.com | NS | 21600 |  | d.ns.facebook.com |
| facebook.com | NS | 21600 |  | c.ns.facebook.com |
| facebook.com | NS | 21600 |  | a.ns.facebook.com |
| facebook.com | NS | 21600 |  | b.ns.facebook.com |
| facebook.com | A | 300 |  | 31.13.66.35 |
| facebook.com | AAAA | 300 |  | 2a03:2880:f103:83:face:b00c:0:25de |
| facebook.com | MX | 1369 | 10 | smtpin.vvv.facebook.com |
| www.facebook.com | A | 3 |  | 31.13.71.36 |
| www.facebook.com | AAAA | 60 |  | 2a03:2880:f103:83:face:b00c:0:25de |
| www.facebook.com | CNAME | 3595 |  | star-mini.c10r.facebook.com |

PING facebook.com (31.13.66.35) 56(84) bytes of data.

64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp\_seq=1 ttl=46 time=1.77 ms

64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp\_seq=2 ttl=46 time=1.47 ms

64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp\_seq=3 ttl=46 time=1.62 ms

64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp\_seq=4 ttl=46 time=1.45 ms

64 bytes from edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35): icmp\_seq=5 ttl=46 time=1.53 ms

--- facebook.com ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4006ms

rtt min/avg/max/mdev = 1.455/1.573/1.772/0.120 ms

Traceroute

traceroute to facebook.com (31.13.66.35), 30 hops max, 60 byte packets

1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.822 ms 0.808 ms 0.827 ms

2 216.182.239.215 (216.182.239.215) 18.814 ms 216.182.226.38 (216.182.226.38) 12.743 ms 216.182.238.143 (216.182.238.143) 22.043 ms

3 100.66.37.218 (100.66.37.218) 5.943 ms 100.65.83.160 (100.65.83.160) 5.793 ms 100.66.37.106 (100.66.37.106) 54.567 ms

4 100.66.15.84 (100.66.15.84) 15.496 ms 100.66.15.76 (100.66.15.76) 17.162 ms 100.66.60.246 (100.66.60.246) 10.471 ms

5 241.0.4.196 (241.0.4.196) 1.285 ms 241.0.4.210 (241.0.4.210) 1.338 ms 241.0.4.203 (241.0.4.203) 1.394 ms

6 241.0.4.202 (241.0.4.202) 1.432 ms 241.0.4.220 (241.0.4.220) 4.761 ms 240.0.40.18 (240.0.40.18) 4.751 ms

7 240.0.40.28 (240.0.40.28) 4.981 ms 240.0.40.19 (240.0.40.19) 4.668 ms 240.0.40.25 (240.0.40.25) 9.053 ms

8 240.0.40.19 (240.0.40.19) 8.894 ms 240.0.40.17 (240.0.40.17) 8.874 ms 240.0.40.29 (240.0.40.29) 5.122 ms

9 52.93.28.179 (52.93.28.179) 5.621 ms 52.93.28.195 (52.93.28.195) 6.427 ms 52.93.28.181 (52.93.28.181) 5.527 ms

10 100.100.4.42 (100.100.4.42) 5.968 ms 100.100.4.36 (100.100.4.36) 11.082 ms 100.100.4.46 (100.100.4.46) 6.759 ms

11 99.82.178.41 (99.82.178.41) 2.212 ms 99.82.178.39 (99.82.178.39) 2.151 ms 99.82.178.41 (99.82.178.41) 2.160 ms

12 po105.psw04.iad3.tfbnw.net (157.240.41.1) 1.569 ms po105.psw02.iad3.tfbnw.net (157.240.40.239) 1.521 ms 99.82.178.41 (99.82.178.41) 2.267 ms

13 157.240.38.235 (157.240.38.235) 1.479 ms 157.240.38.187 (157.240.38.187) 1.746 ms 157.240.38.117 (157.240.38.117) 1.500 ms

14 edge-star-mini-shv-01-iad3.facebook.com (31.13.66.35) 1.438 ms 1.584 ms 157.240.38.243 (157.240.38.243) 1.698 ms

*Exp 8*

Microsoft Windows [Version 10.0.22621.1105]

(c) Microsoft Corporation. All rights reserved.

C:\Users\theja>tracert saveetha.com

Tracing route to saveetha.com [198.185.159.144]

over a maximum of 30 hops:

1 \* General failure.

Trace complete.

C:\Users\theja> tracert facebook.com

Tracing route to facebook.com [2a03:2880:f137:182:face:b00c:0:25de]

over a maximum of 30 hops:

1 1049 ms 8 ms 6 ms 2409:4072:604:b1dc::89

2 \* \* \* Request timed out.

3 48 ms 52 ms 44 ms 2405:200:363:161:a::2

4 47 ms \* 49 ms 2405:200:801:900::1483

5 53 ms 60 ms \* 2405:200:801:900::12f8

6 29 ms 34 ms \* 2405:200:801:900::128f

7 75 ms \* 118 ms ae0.pr02.maa2.tfbnw.net [2620:0:1cff:dead:beee::992]

8 \* 53 ms 36 ms ae0.pr02.maa2.tfbnw.net [2620:0:1cff:dead:beee::992]

9 \* \* \* Request timed out.

10 90 ms 36 ms 37 ms po5.msw1an.02.maa2.tfbnw.net [2a03:2880:f037:ffff::2eb]

11 \* \* \* Request timed out.

12 \* \* 52 ms edge-star-mini6-shv-02-maa2.facebook.com [2a03:2880:f137:182:face:b00c:0:25de]

Trace complete.

C:\Users\theja> tracert saveetha.com

Tracing route to saveetha.com [198.185.159.144]

over a maximum of 30 hops:

1 5 ms 4 ms 2 ms 192.168.137.210

2 \* \* \* Request timed out.

3 \* \* \* Request timed out.

4 \* \* \* Request timed out.

5 \* 48 ms \* 192.168.71.142

6 \* \* \* Request timed out.

7 \* \* \* Request timed out.

8 \* \* 126 ms 192.168.68.136

9 \* \* \* Request timed out.

10 \* \* \* Request timed out.

11 \* \* \* Request timed out.

12 \* \* \* Request timed out.

13 \* \* \* Request timed out.

14 \* 78 ms 80 ms 103.198.140.249

15 83 ms \* \* snge-b3-link.ip.twelve99.net [62.115.11.246]

16 \* \* \* Request timed out.

17 552 ms \* \* po110.bs-a.sech-sin.netarch.akamai.com [23.57.106.243]

18 \* \* \* Request timed out.

19 281 ms 352 ms 295 ms ae120.access-a.sech-sin.netarch.akamai.com [23.57.106.249]

20 357 ms \* 322 ms 93.191.172.102

21 297 ms 379 ms 321 ms a72-52-39-154.deploy.static.akamaitechnologies.com [72.52.39.154]

22 425 ms 463 ms \* 198.185.159.144

23 \* 474 ms \* 198.185.159.144

24 574 ms \* 418 ms 198.185.159.144

u

Trace complete.

C:\Users\theja> ping 172.18.64.1

Pinging 172.18.64.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.18.64.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\theja>netstat

Active Connections

Proto Local

Address Foreign Address State

TCP 127.0.0.1:49669 LAPTOP-0G0G6ED2:49670 ESTABLISHED

TCP 127.0.0.1:49670 LAPTOP-0G0G6ED2:49669 ESTABLISHED

TCP 127.0.0.1:49671 LAPTOP-0G0G6ED2:49672 ESTABLISHED

TCP 127.0.0.1:49672 LAPTOP-0G0G6ED2:49671 ESTABLISHED

TCP 127.0.0.1:62383 LAPTOP-0G0G6ED2:62384 ESTABLISHED

TCP 127.0.0.1:62384 LAPTOP-0G0G6ED2:62383 ESTABLISHED

TCP 127.0.0.1:62387 LAPTOP-0G0G6ED2:62388 ESTABLISHED

TCP 127.0.0.1:62388 LAPTOP-0G0G6ED2:62387 ESTABLISHED

C:\Users\theja>netstat

Active Connections

