Port Scanning with NMap

Estimated time needed: 20 minutes

In this project you will install NMap in Kali Linux and run port scanning.

Learning Objectives

After completing this lab:

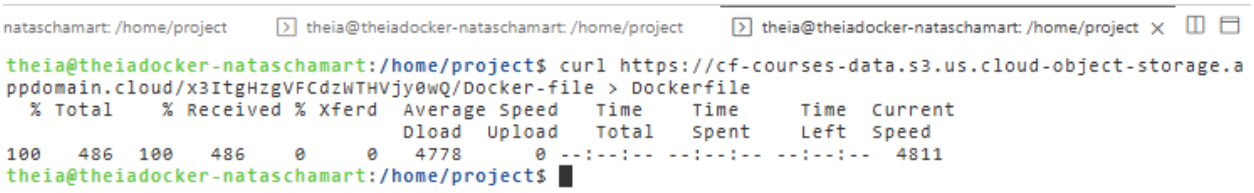
- Install NMap on Linux system
- Run port scan to check for vulnerabilities

I encountered issues launching the Kali Docker container due to mismatch between the lab instructions and the Dockerfile provided. Although the image built successfully, the `docker run` command did not drop me into the interactive shell as expected. Instead, it re-executed the last `RUN` instruction from the Dockerfile, causing the terminal to display build step logs (e.g. `[5/7] RUN apt-get install...`) and preventing me from typing commands. This happened because the Dockerfile lacked a proper `CMD` instruction to default to a Bash shell. The issue was resolved by opening a new terminal and manually starting the container with /bin/back specified, using `docker run -it kalilinux /bin/bash`, which gave me access to the intended Kali Linux environment for continuing the lab exercises.

Set up Kali Linux environment

1. Open a new terminal.
2. In the new terminal that opens up, run the following command to obtain a docker image of Kali Linux with all the required commands preinstalled.

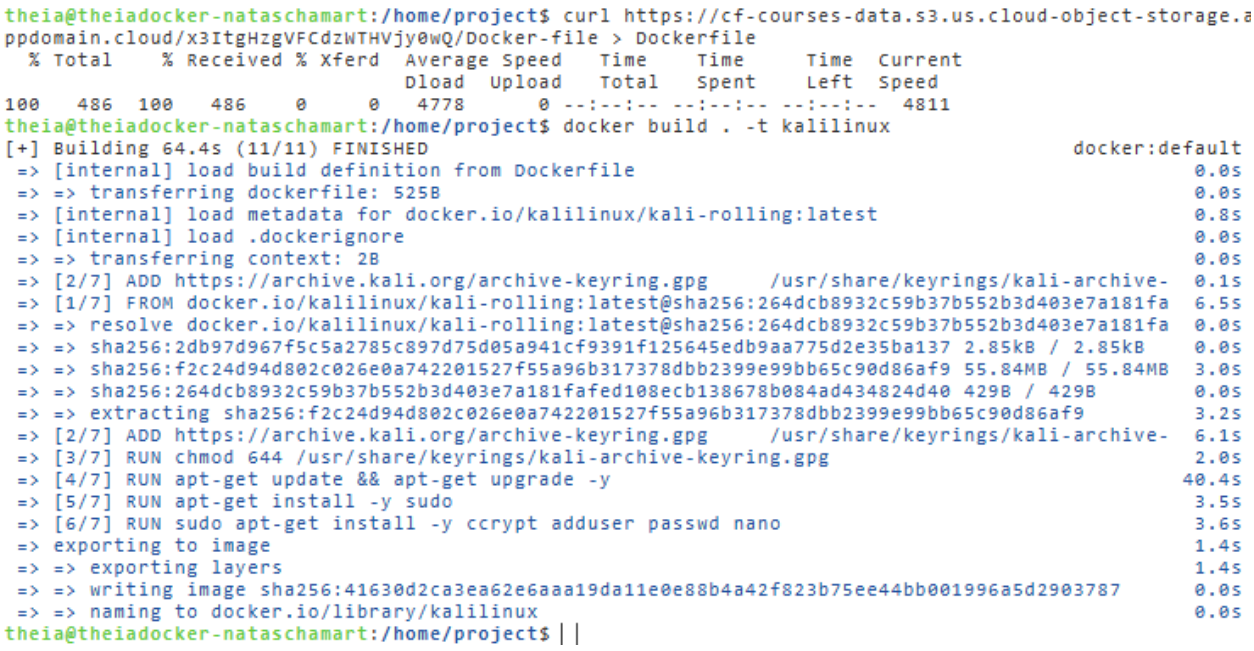
```
1. 1
1. curl https://cf-courses-data.s3.us.cloud-object-
   storage.appdomain.cloud/x3ItgHzgVFCdzWTHVjy0wQ/Docker-file > Dockerfile
Copied!Wrap Toggled!Executed!
```



3. Build the `Dockerfile` in the current directory.

```
1. 1
1. docker build . -t kalilinux
```

Copied!Wrap Toggled!Executed!



4. Run the Kali Linux from the docker image that was just built with an interactive shell.

```
1. 1
1. docker run --tty --interactive  kalilinux
```

Copied!Wrap Toggled!Executed!

This starts an interactive virtual Kali Linux environment. Any files you create in this environment will exist until you are in the virtual environment.

```
[+] Building 64.4s (11/11) FINISHED                                                                    docker:default
 => [internal] load build definition from Dockerfile                                                            0.0s
 => => transferring dockerfile: 525B                                                                            0.0s
 => [internal] load metadata for docker.io/kalilinux/kali-rolling:latest                                        0.8s
 => [internal] load .dockerignore                                                                               0.0s
 => => transferring context: 2B                                                                                 0.0s
 => [2/7] ADD https://archive.kali.org/archive-keyring.gpg     /usr/share/keyrings/kali-archive-                0.1s
 => [1/7] FROM docker.io/kalilinux/kali-rolling:latest@sha256:264dcb8932c59b37b552b3d403e7a181fa                 6.5s
 => => resolve docker.io/kalilinux/kali-rolling:latest@sha256:264dcb8932c59b37b552b3d403e7a181fa                 0.0s
 => => sha256:2db97d967f5c5a2785c897d75d05a941cf9391f125645edb9aa775d2e35ba137 2.85kB / 2.85kB                   0.0s
 => => sha256:f2c24d94d802c026e0a742201527f55a96b317378dbb2399e99bb65c90d86af9 55.84MB / 55.84MB                 3.0s
 => => sha256:264dcb8932c59b37b552b3d403e7a181fafed108ecb138678b084ad434824d40 429B / 429B                      0.0s
 => => extracting sha256:f2c24d94d802c026e0a742201527f55a96b317378dbb2399e99bb65c90d86af9                       3.2s
 => [2/7] ADD https://archive.kali.org/archive-keyring.gpg     /usr/share/keyrings/kali-archive-                6.1s
 => [3/7] RUN chmod 644 /usr/share/keyrings/kali-archive-keyring.gpg                                            2.0s
 => [4/7] RUN apt-get update && apt-get upgrade -y                                                             40.4s
 => [5/7] RUN apt-get install -y sudo                                                                           3.5s
 => [6/7] RUN sudo apt-get install -y ccrypt adduser passwd nano                                                3.6s
 => exporting to image                                                                                          1.4s
 => => exporting layers                                                                                         1.4s
 => => writing image sha256:41630d2ca3ea62e6aaa19da11e0e88b4a42f823b75ee44bb001996a5d2903787                    0.0s
 => => naming to docker.io/library/kalilinux                                                                    0.0s
theia@theiadocker-nataschamart:/home/project$ docker run --tty --interactive  kalilinux
┌──(root㉿1fa7483d997c)-[/]
└─# [5/7] RUN apt-get install -y sudo                                                                          3.5s
 => [6/7] RUN sudo apt-get install -y ccrypt adduser passwd nano                                                3.2s
 => => # Setting up adduser (3.152) ...
 => => # Selecting previously unselected package libncursesw6:amd64.
 => => # (Reading database ... 5630 files and directories currently installed.)
 => => # Preparing to unpack .../libncursesw6_6.5+20250216-2_amd64.deb ...
 => => # Unpacking libncursesw6:amd64 (6.5+20250216-2) ...
 => => # Selecting previously unselected package nano.
```

Install NMap

1. Run the following command to install NMap in Kali Linux.

```
1. 1
1. sudo apt-get install nmap
Copied!Wrap Toggled!
```

This will take a few second to complete the installation.

```
:hamart: /home/project   theia@theiadocker-nataschamart: /home/project   root@1fa7483d997c: /   root@9042d8b7f288: / ×
theia@theiadocker-nataschamart:/home/project$ docker run -it kalilinux /bin/bash
┌──(root㉿9042d8b7f288)-[/]
└─# sudo apt-get install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dbus dbus-bin dbus-daemon dbus-session-bus-common dbus-system-bus-common libblas3 libdbus-1-3
  libexpat1 liblinear4 liblua5.4-0 libpcap0.8t64 libssh2-1t64 nmap-common
Suggested packages:
  default-dbus-session-bus | dbus-session-bus liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  dbus dbus-bin dbus-daemon dbus-session-bus-common dbus-system-bus-common libblas3 libdbus-1-3
  libexpat1 liblinear4 liblua5.4-0 libpcap0.8t64 libssh2-1t64 nmap nmap-common
0 upgraded, 14 newly installed, 0 to remove and 8 not upgraded.
Need to get 7802 kB of archives.
After this operation, 31.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] ||
```

2. Run the following command in the terminal to scan `scanme.nmap.org`.

```
1. nmap scanme.nmap.org
```

Copied!Wrap Toggled!

The output would be as seen below.

```
┌──(root㉿0498317a5890)-[/]
└─# nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-15 00:33 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0083s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156 2600:3c01::ffff:ffff:fe18:bb2f 2600:3c01::ffff:ffff:fe18:bb2f
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE  SERVICE
53/tcp closed domain

Nmap done: 1 IP address (1 host up) scanned in 5.13 seconds
```

```
Setting up libdbus-1-3:amd64 (1.16.2-2) ...
Setting up nmap-common (7.95+dfsg-3kali1) ...
Setting up dbus-session-bus-common (1.16.2-2) ...
Setting up liblua5.4-0:amd64 (5.4.7-1+b2) ...
Setting up libpcap0.8t64:amd64 (1.10.5-2) ...
Setting up libssh2-1t64:amd64 (1.11.1-1) ...
Setting up dbus-system-bus-common (1.16.2-2) ...
Setting up dbus-bin (1.16.2-2) ...
Setting up dbus-daemon (1.16.2-2) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5+b2) ...
Setting up dbus (1.16.2-2) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of start.
Setting up nmap (7.95+dfsg-3kali1) ...
Processing triggers for libc-bin (2.41-9) ...

┌──(root㉿9042d8b7f288)-[/]
└─# nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 14:57 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.13s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156
Not shown: 858 closed tcp ports (reset), 138 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds

┌──(root㉿9042d8b7f288)-[/]
└─# ||
```

3. The default scan in nmap is SYN scan. It is a stealth scan to see if the target system has the ports specified in the command, open, closed or filtered. The SYN scan executes rapidly, capable of scanning thousands of ports within seconds on a high-speed network without hindrance from restrictive firewalls. To initiate a SYN scan using Nmap, the -sS option is utilized. `-sS` is commonly excluded when running Nmap as root or Administrator.

```
1. nmap -p22,113,139 scanme.nmap.org
```

Copied!Wrap Toggled!

```
Processing triggers for libc-bin (2.41-9) ...

┌──(root㉿9042d8b7f288)-[/]
└─# nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 14:57 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.13s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156
Not shown: 858 closed tcp ports (reset), 138 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds

┌──(root㉿9042d8b7f288)-[/]
└─# nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 14:58 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.029s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156

PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
139/tcp closed netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(root㉿9042d8b7f288)-[/]
└─# ||
```

4. Create a new user without root or admin privilige.

```
1. 1
1. useradd John
```

Copied!Wrap Toggled!

```
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(root㉿9042d8b7f288)-[/]
└─# useradd John
```

5. Switch to the newly created user from `root`.

```
1. 1
1. su John
```

Copied!Wrap Toggled!

```
┌──(root㉿9042d8b7f288)-[/]
└─# useradd John

┌──(root㉿9042d8b7f288)-[/]
└─# su John
$ ||
```

6. Run the SYN scan for the ports 22,113 and 139 as `John`.

```
1. nmap -p22,113,139 scanme.nmap.org
```

Copied!Wrap Toggled!

But `John` is not a root user. To do SYN scan as a regular user, you need to provide `-sS` option to the command.

```
┌──(root㉿9042d8b7f288)-[/]
└─# su John
$ nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:01 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ ||
```

7. Run the following command to run SYN scan as a regular user.

```
1. nmap -p22,113,139 -sS scanme.nmap.org
```

Copied!Wrap Toggled!

As you can see, the regular user is disallowed to run the scan.

```
┌──(root㉿9042d8b7f288)-[/]
└─# su John
$ nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:01 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ nmap -p22,113,139 -sS scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:02 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ nmap -p22,113,139 -sS scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:02 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ exit

┌──(root㉿9042d8b7f288)-[/]
└─# ||
```

8. Exit the user prompt, to switch back to `root` user.

```
1. exit
```

Copied!Wrap Toggled!

```
┌──(root㉿9042d8b7f288)-[/]
└─# su John
$ nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:01 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ nmap -p22,113,139 -sS scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:02 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ nmap -p22,113,139 -sS scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:02 UTC
Couldn't open a raw socket. Error: Operation not permitted (1)
$ exit

┌──(root㉿9042d8b7f288)-[/]
└─# ||
```

8. To understand what nmap is doing at packet level, you can specify the `packet-trace` option. This gives you a detailed output.

```
1. nmap -d --packet-trace -p22,113,139 scanme.nmap.org
```

Copied!Wrap Toggled!

```
Packet capture filter (device eth0): dst host 172.17.0.3 and (icmp or icmp6 or ((tcp or udp or sctp) an
d (src host 45.33.32.156)))
SENT (0.1229s) TCP 172.17.0.3:40268 > 45.33.32.156:139 S ttl=56 id=50325 iplen=44  seq=2554032925 win=1
024 <mss 1460>
SENT (0.1229s) TCP 172.17.0.3:40268 > 45.33.32.156:22 S ttl=40 id=63368 iplen=44  seq=2554032925 win=10
24 <mss 1460>
SENT (0.1230s) TCP 172.17.0.3:40268 > 45.33.32.156:113 S ttl=50 id=46735 iplen=44  seq=2554032925 win=1
024 <mss 1460>
RCVD (0.1408s) TCP 45.33.32.156:443 > 172.17.0.3:40012 RA ttl=37 id=31845 iplen=40  seq=0 win=0
RCVD (0.1951s) TCP 45.33.32.156:139 > 172.17.0.3:40268 RA ttl=37 id=21490 iplen=40  seq=0 win=0
RCVD (0.1951s) TCP 45.33.32.156:22 > 172.17.0.3:40268 SA ttl=37 id=22881 iplen=44  seq=452884930 win=65
535 <mss 1460>
Discovered open port 22/tcp on 45.33.32.156
RCVD (0.2033s) TCP 45.33.32.156:113 > 172.17.0.3:40268 RA ttl=37 id=17787 iplen=40  seq=0 win=0
Completed SYN Stealth Scan at 15:03, 0.09s elapsed (3 total ports)
Overall sending rates: 31.61 packets / s, 1390.76 bytes / s.
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 37 (0.029s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156
Scanned at 2025-08-05 15:03:07 UTC for 0s

PORT    STATE  SERVICE     REASON
22/tcp  open   ssh         syn-ack ttl 37
113/tcp closed ident       reset ttl 37
139/tcp closed netbios-ssn reset ttl 37
Final times for host: srtt: 29058 rttvar: 37412  to: 178706

Read from /usr/share/nmap: nmap-protocols nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
           Raw packets sent: 7 (284B) | Rcvd: 5 (204B)

┌──(root㉿9042d8b7f288)-[/]
└─# ||
```

9. You can include higher debug levels to get more detailed output. Try the above command with `-d5`.

```
1. nmap -d5 --packet-trace -p22,113,139 scanme.nmap.org
```

```
0x5B37 urp=0] IP [ver=4 ihl=5 tos=0x00 iplen=40 id=38750 foff=0 ttl=37 proto=6 csum=0x04a1]
Found 45.33.32.156 in incomplete hosts list.
Discovered closed port 113/tcp on 45.33.32.156
Timeout vals: srtt: 15373 rttvar: 21282 to: 100501 delta 80679 ==> srtt: 23536 rttvar: 32288 to: 152688
Timeout vals: srtt: 69984 rttvar: 69984 to: 349920 delta 80679 ==> srtt: 71320 rttvar: 55161 to: 291964
RCVD (0.2167s) TCP [45.33.32.156:139 > 172.17.0.3:45283 RA seq=0 ack=4103779544 off=5 res=0 win=0 csum=
0x5B1D urp=0] IP [ver=4 ihl=5 tos=0x00 iplen=40 id=24507 foff=0 ttl=37 proto=6 csum=0x3c44]
Found 45.33.32.156 in incomplete hosts list.
Discovered closed port 139/tcp on 45.33.32.156
Timeout vals: srtt: 23536 rttvar: 32288 to: 152688 delta 84123 ==> srtt: 31109 rttvar: 39362 to: 188557
Timeout vals: srtt: 71320 rttvar: 55161 to: 291964 delta 84123 ==> srtt: 72920 rttvar: 44571 to: 251204
Moving 45.33.32.156 to completed hosts list with 0 outstanding probes.
Changing global ping host to 45.33.32.156.
Completed SYN Stealth Scan at 15:04, 0.10s elapsed (3 total ports)
Overall sending rates: 31.47 packets / s, 1384.56 bytes / s.
pcap stats: 4 packets received by filter, 0 dropped by kernel.
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 37 (0.031s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156
Scanned at 2025-08-05 15:04:00 UTC for 0s

PORT    STATE  SERVICE     REASON
22/tcp  open   ssh         syn-ack ttl 37
113/tcp closed ident       reset ttl 37
139/tcp closed netbios-ssn reset ttl 37
Final times for host: srtt: 31109 rttvar: 39362  to: 188557

Read from /usr/share/nmap: nmap-protocols nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
           Raw packets sent: 7 (284B) | Rcvd: 5 (204B)

┌──(root㉿9042d8b7f288)-[/]
└─#
```

Practice Exercise:

1. Try to nmap one of the public websites. eg., `google.com`.

```
┌──(root㉿9042d8b7f288)-[/]
└─# nmap google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:05 UTC
Nmap scan report for google.com (142.251.179.139)
Host is up (0.0034s latency).
Other addresses for google.com (not scanned): 142.251.179.139 142.251.179.138 142.251.179.138 142.251.1
79.113 142.251.179.113 142.251.179.102 142.251.179.102 142.251.179.101 142.251.179.101 142.251.179.100
142.251.179.100
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds

┌──(root㉿9042d8b7f288)-[/]
└─#
```

2. Make a note of the open ports. Run nmap SYN scan on the open ports.

```
┌──(root㉿9042d8b7f288)-[/]
└─# nmap -sS -p80,443 google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 15:06 UTC
Nmap scan report for google.com (142.251.179.139)
Host is up (0.0036s latency).
Other addresses for google.com (not scanned): 142.251.179.139 142.251.179.138 142.251.179.138 142.251.1
79.113 142.251.179.113 142.251.179.102 142.251.179.102 142.251.179.101 142.251.179.101 142.251.179.100
142.251.179.100

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(root㉿9042d8b7f288)-[/]
└─#
```

3. Do a `packet-trace` to the same ports that you have scanned above.

```
NSOCK INFO [0.0890s] nsock_read(): Read request from IOD #1 [192.168.65.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0890s] nsock_write(): Write request for 45 bytes to IOD #1 EID 27 [192.168.65.1:53]
NSOCK INFO [0.0890s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.65.1:
53]
NSOCK INFO [0.0890s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.65.1:5
3]
NSOCK INFO [0.0890s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.65.1:53
] (45 bytes): .s..........139.62.253.172.in-addr.arpa.....
NSOCK INFO [0.0890s] nsock_read(): Read request from IOD #1 [192.168.65.1:53] (timeout: -1ms) EID 34
NSOCK INFO [0.0890s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.0890s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.1026s) TCP 172.17.0.3:43565 > 172.253.62.139:443 S ttl=57 id=10332 iplen=44  seq=1405245588 win
=1024 <mss 1460>
SENT (0.1026s) TCP 172.17.0.3:43565 > 172.253.62.139:80 S ttl=56 id=16501 iplen=44  seq=1405245588 win=
1024 <mss 1460>
RCVD (0.1089s) TCP 172.253.62.139:443 > 172.17.0.3:43565 SA ttl=37 id=40279 iplen=44  seq=452912240 win
=65535 <mss 1460>
RCVD (0.1104s) TCP 172.253.62.139:80 > 172.17.0.3:43565 SA ttl=37 id=28600 iplen=44  seq=452886564 win=
65535 <mss 1460>
Nmap scan report for google.com (172.253.62.139)
Host is up (0.0050s latency).
Other addresses for google.com (not scanned): 172.253.62.139 172.253.62.138 172.253.62.138 172.253.62.1
13 172.253.62.113 172.253.62.102 172.253.62.102 172.253.62.101 172.253.62.101 172.253.62.100 172.253.62
.100

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

┌──(root㉿9042d8b7f288)-[/]
└─#
```

Bonus with Deeper Debug

```
Discovered open port 443/tcp on 172.253.62.139
Timeout vals: srtt: 4243 rttvar: 5000 to: 100000 delta 6152 ==> srtt: 4481 rttvar: 4227 to: 100000
Timeout vals: srtt: -1 rttvar: -1 to: 1000000 delta 6152 ==> srtt: 6152 rttvar: 6152 to: 100000
RCVD (0.1225s) TCP [172.253.62.139:80 > 172.17.0.3:62617 SA seq=452910718 ack=511471408 off=6 res=0 win
=65535 csum=0x8466 urp=0 <mss 1460>] IP [ver=4 ihl=5 tos=0x00 iplen=44 id=11969 foff=0 ttl=37 proto=6 c
sum=0xcf6e]
Found 172.253.62.139 in incomplete hosts list.
Discovered open port 80/tcp on 172.253.62.139
Timeout vals: srtt: 4481 rttvar: 4227 to: 100000 delta 7507 ==> srtt: 4859 rttvar: 3926 to: 100000
Timeout vals: srtt: 6152 rttvar: 6152 to: 100000 delta 7507 ==> srtt: 6321 rttvar: 4952 to: 100000
Moving 172.253.62.139 to completed hosts list with 0 outstanding probes.
Changing global ping host to 172.253.62.139.
Completed SYN Stealth Scan at 15:08, 0.02s elapsed (2 total ports)
Overall sending rates: 95.73 packets / s, 4211.94 bytes / s.
pcap stats: 2 packets received by filter, 0 dropped by kernel.
Nmap scan report for google.com (172.253.62.139)
Host is up, received reset ttl 37 (0.0049s latency).
Other addresses for google.com (not scanned): 172.253.62.139 172.253.62.138 172.253.62.138 172.253.62.1
13 172.253.62.113 172.253.62.102 172.253.62.102 172.253.62.101 172.253.62.101 172.253.62.100 172.253.62
.100
Scanned at 2025-08-05 15:08:17 UTC for 0s

PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack ttl 37
443/tcp open  https   syn-ack ttl 37
Final times for host: srtt: 4859 rttvar: 3926  to: 100000

Read from /usr/share/nmap: nmap-protocols nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
           Raw packets sent: 6 (240B) | Rcvd: 3 (128B)

┌──(root㉿9042d8b7f288)-[/]
└─#
```