

## Lab Ethecal Hacking Nmap

### Targets the network range

```
(kali㉿kali)-[~]  
$ nmap 10.29.2.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:17 EDT  
Stats: 0:00:30 elapsed; 13 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.39% done
```

### Disables Port scanning

```
(kali㉿kali)-[~]  
$ nmap -sn  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:22 EDT  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
```

### Stores the results in all formats starting with name 'Tnet'

```
(kali㉿kali)-[~] Wiki Questions and Answers Mailing Lists SharkFest  
$ nmap 10.29.2.0/24 -oA tnet You are running Wireshark 4.0.3 (Git v4.0.3 packaged as 4.0.3-1).  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:24 EDT  
Stats: 0:00:31 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.47% done  
Stats: 0:00:31 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.58% done  
Stats: 0:00:32 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.62% done  
Stats: 0:00:33 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.62% done  
Stats: 0:00:35 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.63% done  
Stats: 0:00:35 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.63% done  
Stats: 0:00:39 elapsed; 10 hosts completed (64 up), 64 undergoing Connect Scan  
Connect Scan Timing: About 0.65% done
```

### Scans only specified port

```
(kali㉿kali)-[~] or capture  
$ nmap 10.129.2.28 -p 21  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:28 EDT  
Nmap scan report for 10.129.2.28  
Host is up (0.0050s latency).  
  
PORT      STATE      SERVICE  
21/tcp    filtered  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

### Disables DNS resolution

```
[kali@kali]~$  
$ nmap 10.129.2.28 -n  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:32 EDT  
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 47.00% done; ETC: 03:33 (0:00:32 remaining)  
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 47.25% done; ETC: 03:33 (0:00:31 remaining)  
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 47.30% done; ETC: 03:33 (0:00:31 remaining)  
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 47.45% done; ETC: 03:33 (0:00:31 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 47.30% done; ETC: 03:33 (0:00:31 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 49.55% done; ETC: 03:33 (0:00:34 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 50.15% done; ETC: 03:33 (0:00:33 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 50.25% done; ETC: 03:33 (0:00:34 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 50.35% done; ETC: 03:33 (0:00:34 remaining)  
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 50.50% done; ETC: 03:33 (0:00:33 remaining)  
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 64.30% done; ETC: 03:33 (0:00:21 remaining)  
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 70.45% done; ETC: 03:33 (0:00:17 remaining)  
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 72.10% done; ETC: 03:33 (0:00:17 remaining)  
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 75.90% done; ETC: 03:33 (0:00:17 remaining)  
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 77.70% done; ETC: 03:33 (0:00:16 remaining)  
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 89.85% done; ETC: 03:33 (0:00:08 remaining)  
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 96.15% done; ETC: 03:33 (0:00:04 remaining)  
Nmap scan report for 10.129.2.28  
Host is up (0.014s latency).  
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 96.98 seconds
```

### To enable verbose mode

### To get the source port

```
(kali㉿kali)-[~]
$ nmap -p 80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 01:54 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
```

## To trace the packet

```
(kali㉿kali)-[~]
└─$ nmap 10.129.2.28 --packet-trace
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 03:36 EDT
CONN (0.0504s) TCP localhost > 10.129.2.28:80 ⇒ Operation now in progress
CONN (0.0507s) TCP localhost > 10.129.2.28:443 ⇒ Operation now in progress
CONN (0.0556s) TCP localhost > 10.129.2.28:80 ⇒ Connected
NSOCK INFO [0.0560s] nssock_ioc_new2(): nssock_ioc_new (IOD #1)
NSOCK INFO [0.0560s] nssock_connect_udp(): UDP connection requested to 192.168.2.2:53 (IOD #1) EID 8
NSOCK INFO [0.0560s] nssock_read(): Read request from IOD #1 [192.168.2.2:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0560s] nssock_write(): Write request for 42 bytes to IOD #1 EID 27 [192.168.2.2:53]
NSOCK INFO [0.0560s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.2.2:53]
NSOCK INFO [0.0560s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.2.2:53]
NSOCK INFO [0.0640s] nssock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.2.2:53] (119 bytes)
NSOCK INFO [0.0640s] nssock_read(): Read request from IOD #1 [192.168.2.2:53] (timeout: -1ms) EID 34
NSOCK INFO [0.0640s] nssock_ioc_delete(): nssock_ioc_delete (IOD #1)
NSOCK INFO [0.0640s] nevent_delete(): nevent_delete on event #34 (type READ)
CONN (0.0653s) TCP localhost > 10.129.2.28:554 ⇒ Operation now in progress
CONN (0.0655s) TCP localhost > 10.129.2.28:5900 ⇒ Operation now in progress
CONN (0.0657s) TCP localhost > 10.129.2.28:445 ⇒ Operation now in progress
CONN (0.0660s) TCP localhost > 10.129.2.28:1720 ⇒ Operation now in progress
```

```
CONN (0.0671s) TCP localhost > 10.129.2.28:1125 ⇒ Operation now in progress
CONN (0.0673s) TCP localhost > 10.129.2.28:3809 ⇒ Operation now in progress
CONN (0.0675s) TCP localhost > 10.129.2.28:3809 ⇒ Operation now in progress
Nmap scan report for 10.129.2.28
Host is up (0.019s latency).
Not shown: 995 filtered tcp ports (no-response), 3 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

## Script scan to gather more information

```
(kali㉿kali)-[~/nithesh]
└─$ nmap -sC 10.29.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-31 12:40 EDT
Stats: 0:01:25 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 82.03% done; ETC: 12:42 (0:00:18 remaining)
Stats: 0:01:26 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 83.01% done; ETC: 12:42 (0:00:17 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.93 seconds
```

## Perform a traceroute to the target

```
(kali㉿kali)-[~/nithesh]
└─$ nmap --traceroute 10.29.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-31 13:07 EDT
Traceroute has to be run as root
QUITTING!
```

## Ping scan (only checks if the target is up)

```
(kali㉿kali)-[~/nithesh]
└─$ nmap -sP 10.29.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-31 13:15 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.32 seconds
```

## TCP connect scan

```
(kali㉿kali)-[~/nithesh]
└─$ nmap -sT 10.29.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-31 13:19 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.33 seconds
```

## UDP scan

```
(kali㉿kali)-[~/nithesh]  
$ nmap -sU 10.29.2.0/24  
You requested a scan type which requires root privileges.  
QUITTING!
```