

Nmap Basic port Scan

In this room, you explore the fundamentals of port scanning using Nmap—one of the most indispensable tools in network reconnaissance. You'll dive into different scan techniques like TCP Connect (-sT), TCP SYN (-sS), and UDP (-sU) scans, and learn how to interpret port states. Let's get started!

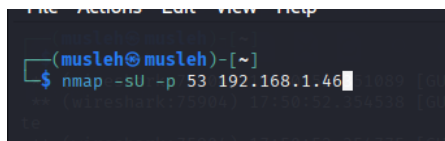
*note I will be using metasploitable2 as a target for scanning for flexibility and better explanation.

Task 2: TCP and UDP Ports

Which service uses UDP port 53 by default?

Answer: DNS

Explanation: UDP port 53 is reserved for the Domain Name System, used for resolving hostnames to IP addresses.

A terminal window with a dark background. The prompt is (musleh@musleh)-[~]. The command nmap -sU -p 53 192.168.1.46 has been entered and is followed by a cursor. The terminal title bar shows 'File Actions Edit View Help'.

No.	Time	Source	Destination	Protocol	Length	Info
16	2025-08-29 21:51:27.774487470	2a01:9700:5996:b601...	2a01:9700:5996:b601...	DNS	164	Standard query response 0xc0e1 No such name
17	2025-08-29 21:51:27.902825935	TaicangT&WEI_0c:7f:...	Broadcast	ARP	60	Who has 192.168.1.23? Tell 192.168.1.1
18	2025-08-29 21:51:27.902826626	192.168.1.20	224.0.0.251	MDNS	584	Standard query response 0x0000 PTR, cache
19	2025-08-29 21:51:27.902826672	fe80::6c99:4aff:feb...	ff02::fb	MDNS	524	Standard query response 0x0000 PTR, cache
20	2025-08-29 21:51:28.146502761	PCSSystemtec_04:42:...	Broadcast	ARP	42	Who has 192.168.1.46? Tell 192.168.1.40
21	2025-08-29 21:51:28.147445824	PCSSystemtec_9b:df:...	PCSSystemtec_04:42:...	ARP	60	192.168.1.46 is at 08:00:27:9b:df:95
22	2025-08-29 21:51:28.147455423	192.168.1.40	192.168.1.46	DNS	72	Standard query 0x0000 TXT version.bind
23	2025-08-29 21:51:28.147529440	192.168.1.40	192.168.1.46	DNS	54	Server status request 0x0000
24	2025-08-29 21:51:28.147573609	192.168.1.40	192.168.1.46	DNS	88	Standard query 0x0000 PTR _services._dns-s
25	2025-08-29 21:51:28.189841028	192.168.1.46	192.168.1.40	DNS	104	Standard query response 0x0000 TXT version
26	2025-08-29 21:51:28.192624503	192.168.1.40	192.168.1.46	ICMP	132	Destination unreachable (Port unreachable)

▶ Frame 22: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:04:42:0f), Dst: PCSSystemtec_9b:df:95 (08:00:27:9b:df:95)
 ▶ Internet Protocol Version 4, Src: 192.168.1.40, Dst: 192.168.1.46
 ▶ User Datagram Protocol, Src Port: 52467, Dst Port: 53
 Source Port: 52467
 Destination Port: 53
 Length: 38
 Checksum: 0x8c27 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 [Stream Packet Number: 1]
 [Timestamps]
 UDP payload (30 bytes)
 ▶ Domain Name System (query)

Which service uses TCP port 22 by default?

Answer: SSH

Explanation: TCP port 22 is used by Secure Shell (SSH) for encrypted remote connections.

```

(musleh@musleh)-[~]
$ nmap -PN -p 22 192.168.1.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 17:58 EDT
Nmap scan report for 192.168.1.46
Host is up (0.00079s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

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

No.	Time	Source	Destination	Protocol	Length	Info
8	2025-08-29 21:58:03.881217774	192.168.1.40	192.168.1.46	TCP	58	50163 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	2025-08-29 21:58:03.882207687	192.168.1.46	192.168.1.40	TCP	60	22 → 50163 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10	2025-08-29 21:58:03.883999786	192.168.1.40	192.168.1.46	TCP	54	50163 → 22 [RST] Seq=1 Win=0 Len=0
402	2025-08-29 21:59:06.285468004	192.168.1.46	192.168.1.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstat
403	2025-08-29 21:59:06.286094875	192.168.1.46	192.168.1.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstat

...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 42
 Protocol: TCP (6)
 Header Checksum: 0xd945 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.40
 Destination Address: 192.168.1.46
 [Stream index: 1]
 ▶ Transmission Control Protocol, Src Port: 50163, Dst Port: 22, Seq: 0, Len: 0

How many port states does Nmap consider?

Answer: 6

Explanation:

Nmap categorizes ports as open, closed, filtered, unfiltered, open | filtered, closed | filtered. This helps pentesters understand network accessibility.

Which port state is most interesting to a pentester?

Answer: Open

Explanation:

Open ports indicate active services that can potentially be exploited.

Task 3: TCP Flags

What 3 letters represent the Reset flag?

Answer: RST

Explanation: The RST flag immediately terminates or rejects a TCP connection.

Which flag needs to be set to initiate a TCP connection?

Answer: SYN

Explanation:

SYN is the first step of the TCP three-way handshake, signaling the initiation of a connection.

Task 4: TCP Connect Scan

Which port was closed before but now open?

Answer: 110

Explanation:

Port 110, commonly used by POP3 (email retrieval), became available between scans.

What does Nmap guess the service is?

Answer: POP3

Explanation:

Nmap identifies the running service based on standard port assignments.

```
root@ip-10-10-212-74:~# nmap -sT 10.10.54.201
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-29 23:29 BST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 23:29 (0:00:00 remaining)
Nmap scan report for ip-10-10-54-201.eu-west-1.compute.internal (10.10.54.201)
Host is up (0.0010s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp    open  pop3
111/tcp    open  rpcbind
143/tcp    open  imap
993/tcp    open  imaps
995/tcp    open  pop3s
MAC Address: 02:DC:C7:0A:48:41 (Unknown)
```

Task 5: TCP SYN Scan

- Let's show the difference between normal tcp scan and syn scan

1- syn scan :

```
(musleh@musleh)-[~]  
$ nmap -sS 192.168.1.46  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 18:35 EDT  
Nmap scan report for 192.168.1.46  
Host is up (0.00041s latency).  
Not shown: 977 closed tcp ports (reset)
```

2095	2025-08-29	22:35:13.378980052	192.168.1.46	192.168.1.40	TCP	60 1309 → 55614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2096	2025-08-29	22:35:13.379044097	192.168.1.40	192.168.1.46	TCP	58 55614 → 8090	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
2097	2025-08-29	22:35:13.379228543	192.168.1.46	192.168.1.40	TCP	60 8090 → 55614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2098	2025-08-29	22:35:13.379298785	192.168.1.40	192.168.1.46	TCP	58 55614 → 9290	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
2099	2025-08-29	22:35:13.379495855	192.168.1.40	192.168.1.46	TCP	58 55614 → 6839	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
2100	2025-08-29	22:35:13.379672224	192.168.1.46	192.168.1.40	TCP	60 9290 → 55614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101	2025-08-29	22:35:13.379672312	192.168.1.46	192.168.1.40	TCP	60 6839 → 55614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2102	2025-08-29	22:35:13.379741964	192.168.1.40	192.168.1.46	TCP	58 55614 → 5002	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
2103	2025-08-29	22:35:13.379948324	192.168.1.40	192.168.1.46	TCP	58 55614 → 5986	[SYN]	Seq=0 Win=1024 Len=0 MSS=1460
2104	2025-08-29	22:35:13.380126353	192.168.1.46	192.168.1.40	TCP	60 5002 → 55614	[RST, ACK]	Seq=1 Ack=1 Win=0 Len=0

- * as you can see nmap send a syn message then receive a syn ack then it send back rst ack to end up the connection

2- full tcp connection :

```
(musleh@musleh)-[~]  
$ nmap -sT -p 22 192.168.1.46  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 18:43 EDT  
Nmap scan report for 192.168.1.46  
Host is up (0.00087s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

No.	Time	Source	Destination	Protocol	Length	Info
41	2025-08-29 22:43:46.456160461	192.168.1.40	192.168.1.46	TCP	74	53574 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=
42	2025-08-29 22:43:46.457271920	192.168.1.46	192.168.1.40	TCP	74	22 → 53574 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
43	2025-08-29 22:43:46.457344599	192.168.1.40	192.168.1.46	TCP	66	53574 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=18
44	2025-08-29 22:43:46.457725113	192.168.1.40	192.168.1.46	TCP	66	53574 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSV=

- * here as we can see it establishes a full connection then send a rst/ack to stop the connection

What is the new open port?

Answer: 6667

Explanation:

TCP SYN scan reveals port 6667 is open

What service name does Nmap guess?

Answer: IRC

Explanation:

Nmap uses its service detection database to identify services running on standard ports.

Task 6: UDP Scan

What UDP port is now open?

Answer: 53

Explanation:

UDP port 53 is open for DNS services; UDP scanning is slower due to its connectionless

-sU (UDP scan): Scans UDP ports, which are connectionless, so Nmap may need to send multiple probes to determine if a port is open or filtered.

-F (fast mode): Scans only the most common ports instead of the full range, making the scan quicker.

-v (verbose): Provides detailed output during the scan, showing progress and host responses.

What service does Nmap name it?

Answer: Domain

Explanation:

Nmap labels UDP port 53 as “domain,” which corresponds to DNS.

Task 7: Fine-Tuning Scope and Performance

*** keep those in your mind :**

paranoid (0)

sneaky (1)

polite (2)

normal (3)

aggressive (4)

insane (5)

those are the options for -T argument from T(0-5) which stands for scanning timing .

Option to scan TCP ports between 5000 and 5500?

Answer: -p5000-5500

Explanation:

Specifies a custom range of ports to scan instead of default ports.

```
(musleh@musleh)-[~]  
$ nmap -sS -p 5000-5500 192.168.1.46  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 19:06 EDT  
Nmap scan report for 192.168.1.46  
Host is up (0.00067s latency).  
Not shown: 500 closed tcp ports (reset)  
PORT      STATE SERVICE  
5432/tcp  open  postgresql  
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
```

Ensure Nmap runs at least 64 probes simultaneously?

Answer: --min-parallelism=64

Explanation:

Adjusts concurrency to speed up scans by sending multiple probes at once.

Option to make Nmap very slow and 'paranoid'?

Answer: -T0

Explanation:

Sets the timing template to the slowest setting to evade IDS/IPS detection.

Summary

This room teaches core Nmap techniques:

TCP Connect Scan (-sT): Full handshake, straightforward but easily detectable.

TCP SYN Scan (-sS): Half-open scan, stealthier since it never completes the handshake.

UDP Scan (-sU): Slower, used for connectionless services like DNS.

Port States: Nmap classifies ports to guide further enumeration.

Fine-tuning flags: Options like -p, --min-parallelism, and -T0 allow control over scope and speed.