Nmap Basic Port Scans

TryHackMe: Nmap Basic Port Scans

Opgaveinformation

Opgavens formål at opnå basisk viden om nnmap og scanningstyper.

Opgave + løsning

Opgave 2 - TCP and UDP Ports

In the same sense that an IP address specifies a host on a network among many others, a TCP port or UDP port is used to identify a network service running on that host. A server provides the network service, and it adheres to a specific network protocol. Examples include providing time, responding to DNS queries, and serving web pages. A port is usually linked to a service using that specific port number. For instance, an HTTP server would bind to TCP port 80 by default; moreover, if the HTTP server supports SSL/TLS, it would listen on TCP port 443. (TCP ports 80 and 443 are the default ports for HTTP and HTTPS; however, the webserver administrator might choose other port numbers if necessary.) Furthermore, no more than one service can listen on any TCP or UDP port (on the same IP address).

At the risk of oversimplification, we can classify ports in two states:

1. Open port indicates that there is some service listening on that port.
2. Closed port indicates that there is no service listening on that port.

However, in practical situations, we need to consider the impact of firewalls. For instance, a port might be open, but a firewall might be blocking the packets. Therefore, Nmap considers the following six states:

1. Open: indicates that a service is listening on the specified port.
2. Closed: indicates that no service is listening on the specified port, although the port is accessible. By accessible, we mean that it is reachable and is not blocked by a firewall or other security appliances/programs.
3. Filtered: means that Nmap cannot determine if the port is open or closed because the port is not accessible. This state is usually due to a firewall preventing Nmap from reaching that port. Nmap's packets may be blocked from reaching the port; alternatively, the responses are blocked from reaching Nmap's host.
4. Unfiltered: means that Nmap cannot determine if the port is open or closed, although the port is accessible. This state is encountered when using an ACK scan -sA.

5. Open|Filtered: This means that Nmap cannot determine whether the port is open or filtered.
6. Closed|Filtered: This means that Nmap cannot decide whether a port is closed or filtered.

Jeg bruger Wikipedia: List of TCP and UDP Ports til at finde svaret på nogen af nedenstående.

Which service uses UDP port 53 by default?

- Svar: Domain Name Server (DNS)

Which service uses TCP port 22 by default?

- Svar: Secure Shell (SSH)

Which service uses TCP port 22 by default?

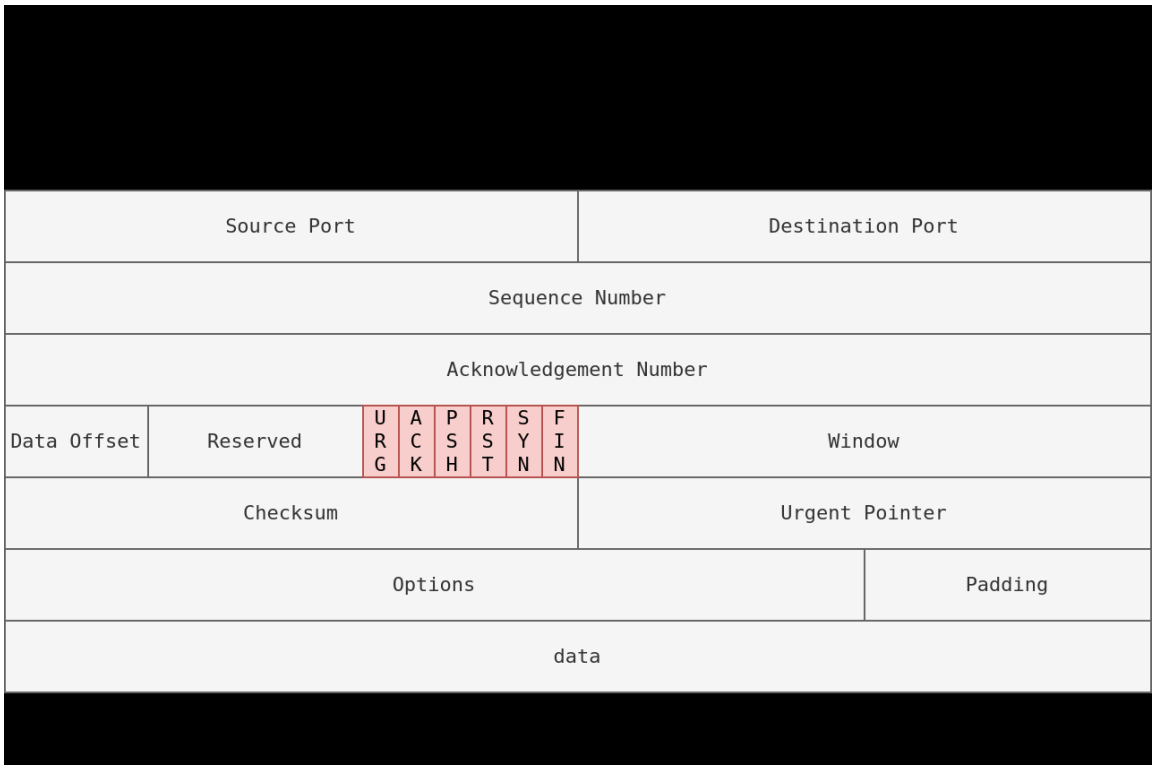
- Svar: 6

Which port state is the most interesting to discover as a pentester?

- Svar: Open

Task 3 - TCP Flags

Nmap supports different types of TCP port scans. To understand the difference between these port scans, we need to review the TCP header. The TCP header is the first 24 bytes of a TCP segment. The following figure shows the TCP header as defined in RFC 793. This figure looks sophisticated at first; however, it is pretty simple to understand. In the first row, we have the source TCP port number and the destination port number. We can see that the port number is allocated 16 bits (2 bytes). In the second and third rows, we have the sequence number and the acknowledgement number. Each row has 32 bits (4 bytes) allocated, with six rows total, making up 24 bytes.



In particular, we need to focus on the flags that Nmap can set or unset. We have highlighted the TCP flags in red. Setting a flag bit means setting its value to 1. From left to right, the TCP header flags are:

1. URG: Urgent flag indicates that the urgent pointer filed is significant. The urgent pointer indicates that the incoming data is urgent, and that a TCP segment with the URG flag set is processed immediately without consideration of having to wait on previously sent TCP segments.
2. ACK: Acknowledgement flag indicates that the acknowledgement number is significant. It is used to acknowledge the receipt of a TCP segment.
3. PSH: Push flag asking TCP to pass the data to the application promptly.
4. RST: Reset flag is used to reset the connection. Another device, such as a firewall, might send it to tear a TCP connection. This flag is also used when data is sent to a host and there is no service on the receiving end to answer.
5. SYN: Synchronize flag is used to initiate a TCP 3-way handshake and synchronize sequence numbers with the other host. The sequence number should be set randomly during TCP connection establishment.
6. FIN: The sender has no more data to send.

What 3 letters represent the Reset flag?

- RST

Which flag needs to be set when you initiate a TCP connection (first packet of TCP 3-way handshake)? * SYN

Task 4 - TCP Connect Scan

TCP connect scan works by completing the TCP 3-way handshake. In standard TCP connection establishment, the client sends a TCP packet with SYN flag set, and the server responds with SYN/ACK if the port is open; finally, the client completes the 3-way handshake by sending an ACK.

We are interested in learning whether the TCP port is open, not establishing a TCP connection. Hence the connection is torn as soon as its state is confirmed by sending a RST/ACK. You can choose to run TCP connect scan using `-sT`.

Launch the VM. Open the AttackBox and execute `nmap -sT <ip>` via the terminal. A new service has been installed on this VM since our last scan, as shown in the terminal window above. Which port number was closed in the scan above but is now open on this target VM?

```
nmap -sT 10.113.161.24

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 08:02 -0500
Nmap scan report for 10.113.161.24
Host is up (0.020s latency).
Not shown: 992 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

- Svar: 110

What is Nmap's guess about the newly installed service?

- POP3

Task 5 - TCP Syn Scan

Launch the VM. Some new server software has been installed since the last time we scanned it. On the AttackBox, use the terminal to execute `nmap -sS <ip>`. What is the new open port?

```
sudo nmap -sS 10.112.150.57

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 08:14 -0500
Nmap scan report for 10.112.150.57
Host is up (0.037s latency).
Not shown: 991 closed tcp ports (reset)
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
6667/tcp open  irc
```

- Svar: 6667

What is Nmap's guess of the service name?

- IRC

Task 6 - UDP Scan

Launch the VM. On the AttackBox, use the terminal to execute `nmap -sU -F -v MACHINE_IP`. A new service has been installed since the last scan. What is the UDP port that is now open?

```
nmap -sU -F -v 10.114.160.253

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 08:19 -0500
Initiating Ping Scan at 08:19
Scanning 10.114.160.253 [4 ports]
Completed Ping Scan at 08:19, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:19
Completed Parallel DNS resolution of 1 host. at 08:19, 0.52s elapsed
Initiating UDP Scan at 08:19
Scanning 10.114.160.253 [100 ports]
Increasing send delay for 10.114.160.253 from 0 to 50 due to
max_successful_tryno increase to 4
Increasing send delay for 10.114.160.253 from 50 to 100 due to
max_successful_tryno increase to 5
Increasing send delay for 10.114.160.253 from 100 to 200 due to
max_successful_tryno increase to 6
Increasing send delay for 10.114.160.253 from 200 to 400 due to 11 out of 11
dropped probes since last increase.
Increasing send delay for 10.114.160.253 from 400 to 800 due to 11 out of 11
dropped probes since last increase.
UDP Scan Timing: About 42.12% done; ETC: 08:20 (0:00:43 remaining)
Discovered open port 111/udp on 10.114.160.253
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 63.50% done; ETC: 08:20 (0:00:34 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.50% done; ETC: 08:20 (0:00:33 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 65.50% done; ETC: 08:20 (0:00:32 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 66.50% done; ETC: 08:20 (0:00:31 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 71.50% done; ETC: 08:20 (0:00:26 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 72.50% done; ETC: 08:20 (0:00:25 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
```

```
UDP Scan Timing: About 73.50% done; ETC: 08:20 (0:00:24 remaining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.50% done; ETC: 08:20 (0:00:23 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.50% done; ETC: 08:20 (0:00:19 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.62% done; ETC: 08:20 (0:00:20 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.62% done; ETC: 08:20 (0:00:20 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 79.62% done; ETC: 08:20 (0:00:19 remaining)
Discovered open port 53/udp on 10.114.160.253
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 80.62% done; ETC: 08:20 (0:00:18 remaining)
Completed UDP Scan at 08:20, 106.30s elapsed (100 total ports)
Nmap scan report for 10.114.160.253
Host is up (0.020s latency).
Not shown: 97 closed udp ports (port-unreach)
PORT    STATE         SERVICE
53/udp  open          domain
68/udp  open|filtered dhcpc
111/udp open          rpcbind

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 107.00 seconds
           Raw packets sent: 277 (16.880KB) | Rcvd: 112 (9.372KB)
```

- Svar: 53

What is the service name according to Nmap?

- domain

Task 7 - Fine-Tuning Scope and Performance

You can specify the ports you want to scan instead of the default 1000 ports. Specifying the ports is intuitive by now. Let's see some examples:

- port list: `-p22,80,443` will scan ports 22, 80 and 443.
- port range: `-p1-1023` will scan all ports between 1 and 1023 inclusive, while `-p20-25` will scan ports between 20 and 25 inclusive.

You can request the scan of all ports by using `-p-`, which will scan all 65535 ports. If you want to scan the most common 100 ports, add `-F`. Using `--top-ports 10` will check the ten most common ports.

You can control the scan timing using `-T<0-5>`. `-T0` is the slowest (paranoid), while `-T5` is the fastest. According to Nmap manual page, there are six templates:

- paranoid (0)
- sneaky (1)
- polite (2)

- normal (3)
- aggressive (4)
- insane (5)

To avoid IDS alerts, you might consider `-T0` or `-T1`. For instance, `-T0` scans one port at a time and waits 5 minutes between sending each probe, so you can guess how long scanning one target would take to finish. If you don't specify any timing, Nmap uses normal `-T3`. Note that `-T5` is the most aggressive in terms of speed; however, this can affect the accuracy of the scan results due to the increased likelihood of packet loss. Note that `-T4` is often used during CTFs and when learning to scan on practice targets, whereas `-T1` is often used during real engagements where stealth is more important.

Alternatively, you can choose to control the packet rate using `--min-rate <number>` and `--max-rate <number>`. For example, `--max-rate 10` or `--max-rate=10` ensures that your scanner is not sending more than ten packets per second.

Moreover, you can control probing parallelization using `--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`. Nmap probes the targets to discover which hosts are live and which ports are open; probing parallelization specifies the number of such probes that can be run in parallel. For instance, `--min-parallelism=512` pushes Nmap to maintain at least 512 probes in parallel; these 512 probes are related to host discovery and open ports.

What is the option to scan all the TCP ports between 5000 and 5500?

- `-p5000-5500`

How can you ensure that Nmap will run at least 64 probes in parallel?

- `--min-parallelism=64`

What option would you add to make Nmap very slow and paranoid?

- `-T0`

Task 8 - Summary

Port Scan Type	Example Command
TCP Connect Scan	nmap -sT 10.114.160.253
TCP SYN Scan	sudo nmap -sS 10.114.160.253
UDP Scan	sudo nmap -sU 10.114.160.253

Option	Purpose

Option	Purpose
-p-	all ports
-p1-1023	scan ports 1 to 1023
-F	100 most common ports
-r	scan ports in consecutive order
-T<0-5>	-T0 being the slowest and T5 the fastest
--max-rate 50	rate <= 50 packets/sec
--min-rate 15	rate >= 15 packets/sec
--min-parallelism 100	at least 100 probes in parallel

2026-02-20 13:35:32