Nmap: The Basics

Introduction

Ways that NMAP uses to specify its targets :

- IP range using - := If you want to scan all the IP addresses from 192.168.0.1 to 192.168.0.10, you can write `192.168.0.1-10`
- IP subnet using `/`: If you want to scan a subnet, you can express it as `192.168.0.1/24`, and this would be equivalent to `192.168.0.0-255`
- Hostname: You can also specify your target by hostname, for example, `example.thm`

NMAP offers the `-sn` option to discover hosts on a network

Host Discovery: Who Is Online

Scanning a local network

The following command is used to scan a local network `nmap -sn .....(followed by the ip address)`

Scanning a Remote network

Nmap offers a list scan with the option `-sL` . This scan only lists the targets without actually scanning them. For example, `nmap -sL 192........` will list the 257 targets that will be scanned

- Interesting question (must learn about subnetting)

What is the last IP address that will be scanned when your scan target is `192.168.0.1/27`?

Answer : 192.168.0.31

Port Scanning: Who Is Listening

Scanning TCP Ports

The easiest way to know whether a TCP port is open would be to attempt to `telnet` to the port.

Connect Scan

The connect scan can be triggered using `-sT`. It tries to complete the TCP three-way handshake with every target TCP port. If the TCP port turns out to be open and Nmap connects successfully, Nmap will tear down the established connection.

SYN Scan (Stealth)

It is a TCP-based port scanning technique that sends a SYN packet to a target port and analyzes the response (SYN-ACK for open, RST for closed, or no response for filtered) without completing the TCP handshake. It is faster and stealthier than a full TCP connect scan, making it a popular choice for network discovery and security assessments. Tools like `Nmap -sS` are commonly used for SYN scanning.

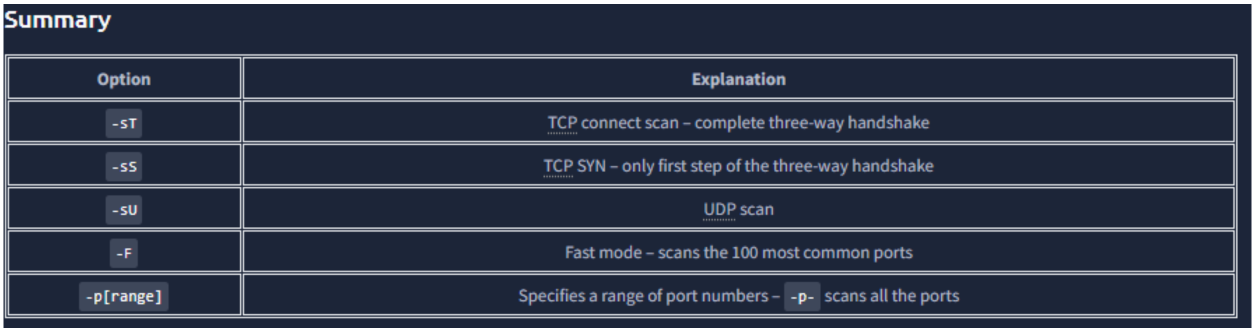
Scanning UDP Ports

Many services use UDP for communication such as DNS, DHCP, NTP, SNMP. The reason is because UDP is faster and it doesn’t require establishing a connection and tearing it down afterwards. Nmap offer the option `-sU` to scan for UDP services.

Limiting the Target Ports

Nmap scans the most common 1,000 ports by default. However, this might not be what you are looking for. Therefore, Nmap offers you a few more options.

- `-F` is for fast mode which scans the most famous 100 ports instead of the default 1000
- `p[range]` allows you to specify a range of ports to scan. For example, `p10-1024` scans from port 10 to port 1024, while `p-25` will scan all the ports between 1 and 25. Note that `p-` scans all the ports and is equivalent to `p1-65535` and is the best option if you want to be as thorough as possible.



Summary

Option	Explanation
`-sT`	TCP connect scan – complete three-way handshake
`-sS`	TCP SYN – only first step of the three-way handshake
`-sU`	UDP scan
`-F`	Fast mode – scans the 100 most common ports
`-p[range]`	Specifies a range of port numbers – `-p-` scans all the ports

Version Detection : Extract more Information

OS Detection

You can enable OS detection by adding the `-O` option. it allows to guess the target machine's operating system. an example for running it is at follows : `nmap -sS -O 192.168.124.211`

Service and Version Detection

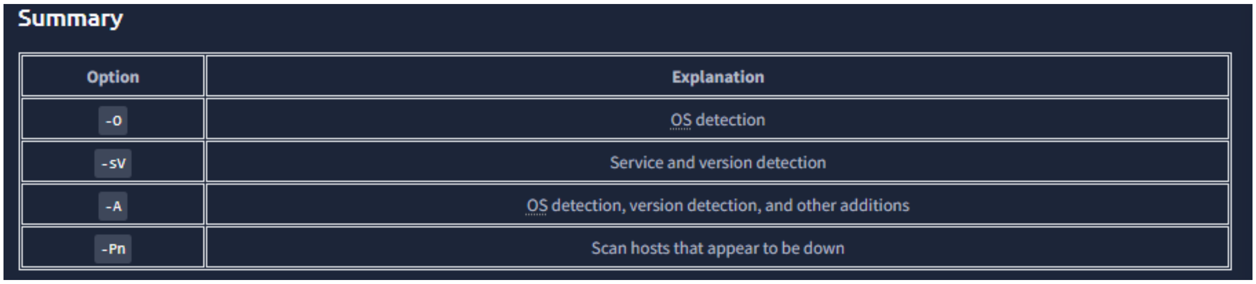
Using `-sV` enables version detection. The example below is the execution of the code that shows what services are listening on the ports

`nmap -sS -sV 192.168.124.211`

What if you can have both `-O`, `-sV` and some more in one option? That would be `-A`. This option enables OS detection, version scanning, and traceroute, among other things.

Forcing the Scan

When we run our port scan, such as using `-sS,` there is a possibility that the target host does not reply during the host discovery phase (e.g. a host doesn’t reply to ICMP requests). Consequently, Nmap will mark this host as down and won’t launch a port scan against it. We can ask Nmap to treat all hosts as online and port scan every host, including those that didn’t respond during the host discovery phase. This choice can be triggered by adding the `-Pn` option.

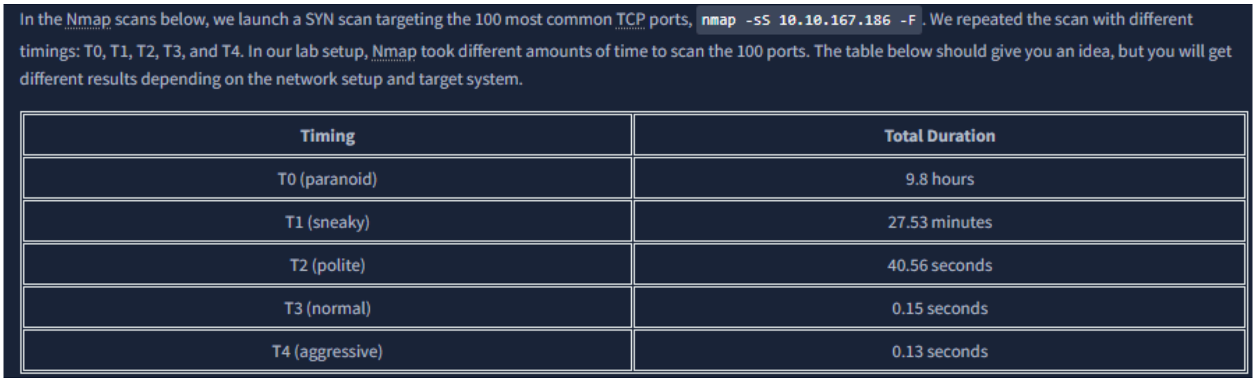


Summary

Option	Explanation
-O	OS detection
-sV	Service and version detection
-A	OS detection, version detection, and other additions
-Pn	Scan hosts that appear to be down

Timing: How fast is fast

Running the scan at its normal speed might trigger an IDS or other security solutions. The pace of the scan can be determined using 6 timing templates provided by Nmap. paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). You can pick the timing template by its name or number. For example, you can add `-T0` (or `-T 0`) or `-T paranoid` to opt for the slowest timing.



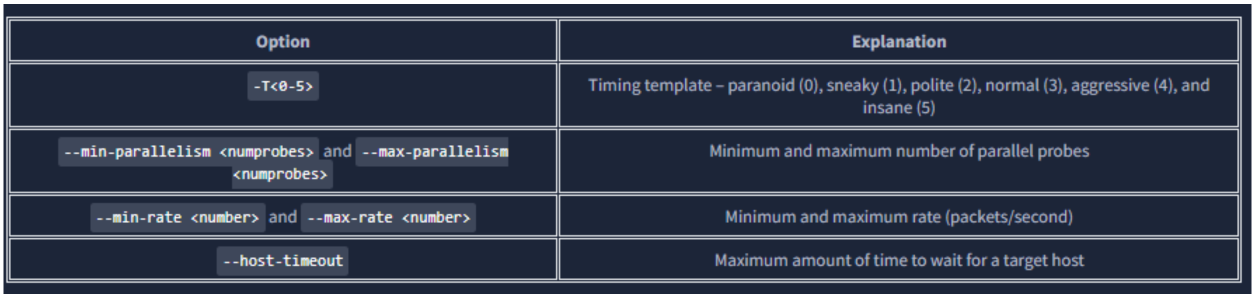
In the Nmap scans below, we launch a SYN scan targeting the 100 most common TCP ports, `nmap -sS 10.10.167.186 -F`. We repeated the scan with different timings: T0, T1, T2, T3, and T4. In our lab setup, Nmap took different amounts of time to scan the 100 ports. The table below should give you an idea, but you will get different results depending on the network setup and target system.

Timing	Total Duration
T0 (paranoid)	9.8 hours
T1 (sneaky)	27.53 minutes
T2 (polite)	40.56 seconds
T3 (normal)	0.15 seconds
T4 (aggressive)	0.13 seconds

A second helpful option is the number of parallel services probes. The number of parallel probes can be controlled with `--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`. These options can be used to set a minimum and maximum on the number of TCP and UDP port probes active simultaneously for a host group. By default, `nmap` will automatically control the number of parallel probes. If the network is performing poorly, i.e., dropping packets, the number of parallel probes might fall to one; furthermore, if the network performs flawlessly, the number of parallel probes can reach several hundred.

A similar helpful option is the `--min-rate <number>` and `--max-rate <number>`. As the names indicate, they can control the minimum and maximum rates at which `nmap` sends packets. The rate is provided as the number of packets per second. It is worth mentioning that the specified rate applies to the whole scan and not to a single host.

The last option we will cover in this task is `--host-timeout <time>`. This option specifies the maximum time you are willing to wait, and it is suitable for slow hosts or hosts with slow network connections.



Option	Explanation
`-T<0-5>`	Timing template – paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5)
`--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`	Minimum and maximum number of parallel probes
`--min-rate <number>` and `--max-rate <number>`	Minimum and maximum rate (packets/second)
`--host-timeout`	Maximum amount of time to wait for a target host

Question

What is the non-numeric equivalent of `-T4`?

`-T aggressive`

Output: Controlling What You See

This task focuses on two main features:

- Showing additional information while a scan takes place
- Choosing the file format to save the scan report

Verbosity and Debugging

Knowing that sometimes the scan takes a bit long to finish, using `-v` allows to see more real time information about the scan

Most likely, the -v option is more than enough for verbose output; however, if you are still unsatisfied, you can increase the verbosity level by adding another “v” such as `-vv` or even `-vvvv`. You can also specify the verbosity level directly, for example, `-v2` and `-v4`. You can even increase the verbosity level by pressing “v” after the scan already started.

If all this verbosity does not satisfy your needs, you must consider the `-d` for debugging-level output. Similarly, you can increase the debugging level by adding one or more “d” or by specifying the debugging level directly. The maximum level is `-d9`; before choosing that, make sure you are ready for thousands of information and debugging lines.

Saving Scan Report

In many cases, we would need to save the scan results. Nmap gives us various formats. The three most useful are normal (human-friendly) output, XML output, and grepable output, in reference to the `grep` command. You can select the scan report format as follows:

`-oN <filename>` - Normal output

`-oX <filename>` - XML output

`-oG <filename>` - grep-able output (useful for grep and awk)

`-oA <basename>` - Output in all major formats

Question!

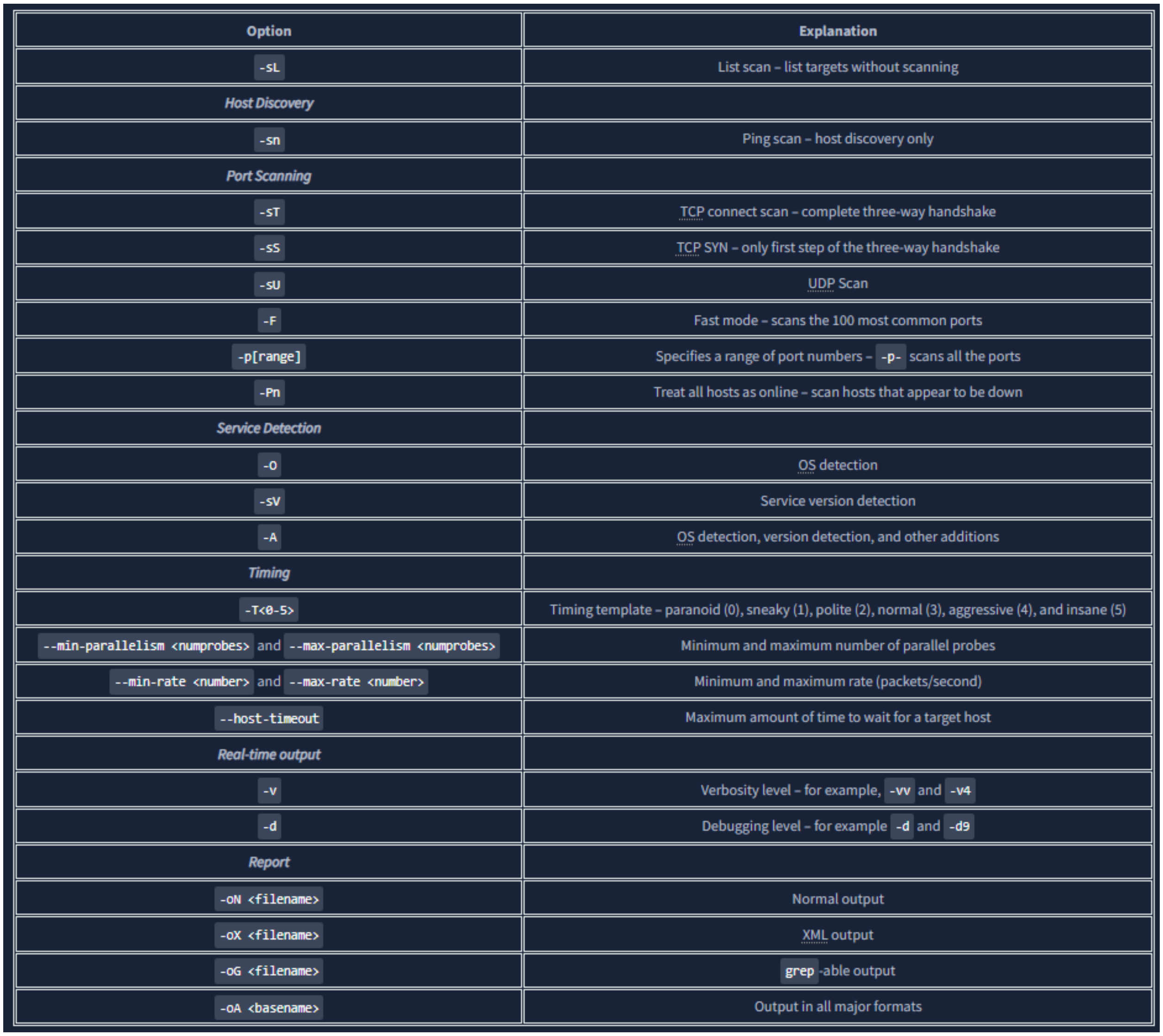
What option must you add to your `nmap` command to enable debugging ?

Answer:

`-d`

Conclusion

It is worth noting that it is best to run Nmap with `sudo` privileges so that we can make use of all its features.
Nmap would automatically use SYN scan (`-sS`) if you are running it with `sudo` privileges and will default to connect scan (`-sT`) if run as a local user. The reason is that crafting certain packets, such as sending a TCP SYN packet, requires root privileges.



Option	Explanation
`-sL`	List scan – list targets without scanning
Host Discovery	
`-sn`	Ping scan – host discovery only
Port Scanning	
`-sT`	TCP connect scan – complete three-way handshake
`-sS`	TCP SYN – only first step of the three-way handshake
`-sU`	UDP Scan
`-F`	Fast mode – scans the 100 most common ports
`-p[range]`	Specifies a range of port numbers – `-p-` scans all the ports
`-Pn`	Treat all hosts as online – scan hosts that appear to be down
Service Detection	
`-O`	OS detection
`-sV`	Service version detection
`-A`	OS detection, version detection, and other additions
Timing	
`-T<0-5>`	Timing template – paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5)
`--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`	Minimum and maximum number of parallel probes
`--min-rate <number>` and `--max-rate <number>`	Minimum and maximum rate (packets/second)
`--host-timeout`	Maximum amount of time to wait for a target host
Real-time output	
`-v`	Verbosity level – for example, `-vv` and `-v4`
`-d`	Debugging level – for example `-d` and `-d9`
Report	
`-oN <filename>`	Normal output
`-oX <filename>`	XML output
`-oG <filename>`	`grep`-able output
`-oA <basename>`	Output in all major formats

Questions:

What kind of scan will Nmap use if you run nmap MACHINE_IP with local user privileges?

Anwer:

Connect scan