Nmap - The Basics

Host Discovery: Who Is Offline

we should mention that Nmap uses multiple ways 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`

important to run nmap as root or with sudo as using local accounts can restrict types of scans

```
root@tryhackme:~# nmap -sn 192.168.66.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-07 13:49 EEST
Nmap scan report for XiaoQiang (192.168.66.1)
Host is up (0.0069s latency).
MAC Address: 44:DF:65:D8:FE:6C (Unknown)
Nmap scan report for S190023240007 (192.168.66.88)
Host is up (0.090s latency).
MAC Address: 7C:DF:A1:D3:8C:5C (Espressif)
Nmap scan report for wlan0 (192.168.66.97)
Host is up (0.20s latency).
MAC Address: 10:D5:61:E2:18:E6 (Tuya Smart)
Nmap scan report for 192.168.66.179
Host is up (0.10s latency).
MAC Address: E4:AA:EC:8F:88:C9 (Tianjin Hualai Technology)
[...]
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.64 seconds
```

Scanning a “Local” Network

to scan a local network such as ethernet or wifi we are connected to

can just use nmap then the ip address

example command:
`nmap -sn 192.168.66.0/24`

scanning local network allows us to look up the MAC addresses of devices connected

Scanning a “Remote” Network

means that at least one router separates our system from this network

Our system has the IP address `192.168.66.89` and belongs to the `192.168.66.0/24` network. In the terminal below we scan the target network `192.168.11.0/24` where there are two or more routers (hops) separate our local system from the target hosts

```
root@tryhackme:~# nmap -sn 192.168.11.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-07 14:05 EEST
Nmap scan report for 192.168.11.1
Host is up (0.018s latency).
Nmap scan report for 192.168.11.151
Host is up (0.0013s latency).
Nmap scan report for 192.168.11.152
Host is up (0.13s latency).
Nmap scan report for 192.168.11.154
Host is up (0.22s latency).
Nmap scan report for 192.168.11.155
Host is up (2.3s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.67 seconds
```

- `192.168.11.1` is live and responded to the ICMP echo (ping) request.
- `192.168.11.2` seems down. Nmap sent two ICMP echo (ping) requests, two ICMP timestamp requests, two TCP packets to port 443 with the SYN flag set, and two TCP packets to port 80 with the ACK flag set. The target didn't respond to any. We observe several ICMP destination unreachable packets from the `192.168.11.151` router.

can have more control over how Nmap discovers live hosts such as `-PS[portlist]`, `-PA[portlist]`, `-PU[portlist]` for TCP SYN, TCP ACK, and UDP discovery via the given ports

Nmap offers a list scan with the option `-sL` This scan only lists the targets to scan without actually scanning them

`-sn` aims to discover live hosts without attempting to discover the services running on them. This scan might be helpful if you want to discover the devices on a network without causing much noise

Port Scanning: Who Is Listening

web servers, which usually listen on TCP ports 80 and 443, and DNS servers, which typically listen on UDP (and TCP) port 53.

Scanning TCP Ports

most basic way to know whether a TCP port is open would be to attempt to `telnet`

Connect Scan

nmap -sT [ip] - connect scan tries to complete TCP three-way handshake with every target TCP port

SYN Scan (Stealth)

namp -sS [ip]-

the SYN scan only executes the first step: it sends a TCP SYN packet.

The advantage is that this is expected to lead to fewer logs as the connection is never

established

Scanning UDP Ports

Although most services use TCP for communication, many use UDP. Examples include DNS, DHCP, NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), and VoIP (Voice over IP).

-sU - to scan for UDP services

Limiting the Target Ports

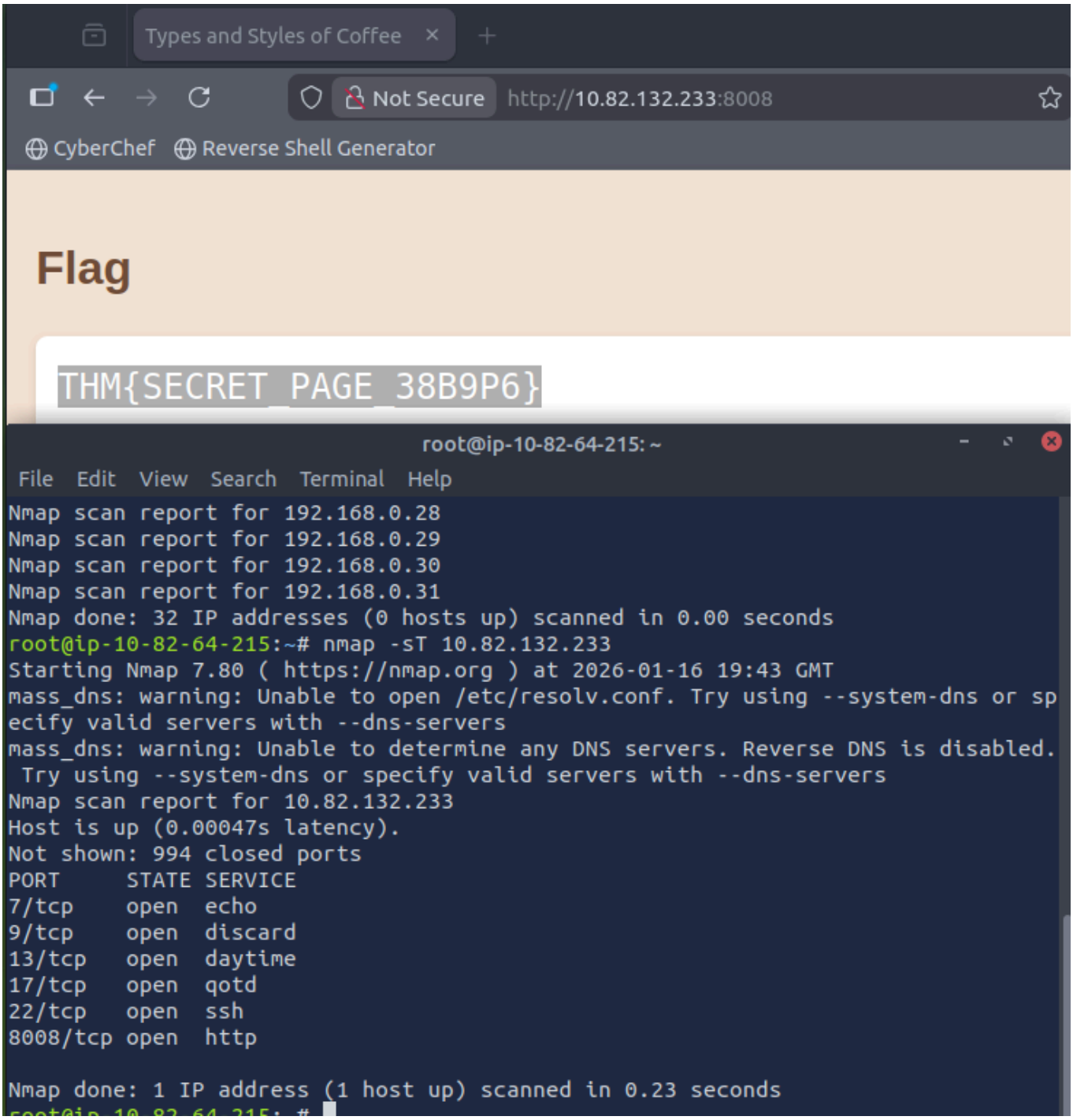
Nmap scans the most common 1,000 ports by default. However, this might not be what you are looking for. Therefore, Nmap offers you a few more options.

- `-F` is for Fast mode, which scans the 100 most common 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.
- Tip: The most common services use a port number between 1 and 1024 for either UDP or TCP. These ports are also known as **well-known ports**. Use `-p1-1024` to scan for the well-known ports.

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

this shows 6 open TCP ports



with the Nmap scan i just did i found a tcp port 8008 which was a website since its an open port i can do the target ip with the port number and go to that website to reveal a flag

Version Detection: Extract More Information

OS Detection

-O -is os detection which triggers Nmap to rely on various indicators to make an educated guess about the target OS.

```
root@tryhackme:~# nmap -sS -O 192.168.124.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 13:37 EEST
Nmap scan report for ubuntu22lts-vm (192.168.124.211)
Host is up (0.00043s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:54:FA:4E (QEMU virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Service and Version Detection

-sV - enables version detection. This is very convenient for gathering more information about your target

```
root@tryhackme:~# nmap -sS -sV 192.168.124.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 13:33 EEST
Nmap scan report for ubuntu22lts-vm (192.168.124.211)
Host is up (0.000046s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 52:54:00:54:FA:4E (QEMU virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 0.25
```

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

-Pn - treat all hosts as online and port scan every host, including those that didn't respond during the host discovery phase

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

```
root@ip-10-82-64-215:~# nmap -sV 10.82.132.233
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-16 19:52 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disable
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.82.132.233
Host is up (0.00016s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE  VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime?
17/tcp   open  qotd?
22/tcp   open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protoc
 2.0)
8008/tcp open  http     lighttpd 1.4.74
2 services unrecognized despite returning data. If you know the service/versio
 please submit the following fingerprints at https://nmap.org/cgi-bin/submit.c
?new-service :
```

showed me the name and version of port 8008

Timing: How Fast is Fast

Nmap provides various options to control the scan speed and timing.

you can add `-T0` (or `-T 0`) or `-T paranoid` to opt for the slowest timing.

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 service probes

probes can be controlled with `--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`

can be used to set a minimum and maximum on the number of TCP and UDP port probes active simultaneously for a host group

A similar helpful option is the `--min-rate <number>` and `--max-rate <number>`. They can control the minimum and maximum rates at which `nmap` sends packets.

`--host-timeout <time>`. This option specifies the maximum time you are willing to wait

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

Output: Controlling What You See

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

Verbosity and Debugging

The best way to get more updates about what's happening is to enable verbose output by adding `-v`

this can help when a network scan is slow

```
root@tryhackme:~# nmap 192.168.139.1/24 -v
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-13 19:01 EEST
Initiating ARP Ping Scan at 19:01
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:01, 7.94s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:01
Completed Parallel DNS resolution of 1 host. at 19:02, 13.00s elapsed
Nmap scan report for 192.168.139.0 [host down]
Nmap scan report for 192.168.139.2 [host down]
[...]
Nmap scan report for 192.168.139.253 [host down]
Nmap scan report for 192.168.139.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 19:02
Completed Parallel DNS resolution of 1 host. at 19:02, 0.05s elapsed
Initiating SYN Stealth Scan at 19:02
Scanning 192.168.139.254 [1000 ports]
[...]
Initiating SYN Stealth Scan at 19:02
Scanning g5000 (192.168.139.1) [1000 ports]
Discovered open port 902/tcp on 192.168.139.1
Completed SYN Stealth Scan at 19:02, 0.03s elapsed (1000 total ports)
Nmap scan report for g5000 (192.168.139.1)
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure
```

can also use -vv (-v2) or -vvvv (-v4)

-d - used for debugging output can be increased up to the max level of -d9

Saving Scan Report

gives us various formats. The three most useful are normal (human-friendly) output, XML output, and grepable output-

- `-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

```
root@tryhackme:~# nmap -sS 192.168.139.1 -oA gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-13 19:35 EEST
Nmap scan report for g5000 (192.168.139.1)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
# ls
gateway.gnmap  gateway.nmap  gateway.xml
```

-oA is used here and can see that it makes all 3 of the formats

Summary

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

Option	Explanation
	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