

Nmap Cheatsheet

Contents

1	Basic Nmap Commands	2
1.1	Service Version Detection (-sV)	2
1.2	Default Script Scan (-sC)	3

This document shall contain everything I have learned so far about nmap. I must keep it up-to-date because I feel a bit lost in this cybersecurity journey to be frank.

1 Basic Nmap Commands

1.1 Service Version Detection (-sV)

This is the Service Detection flag (*yes; -sV is a single flag, not a combination of both s AND V*), which will tell you the name and description of the identified services.

Service Version Detection

```
$ sudo nmap -sV {target_IP}

Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-28 06:27 GMT
Nmap scan report for 10.10.171.202
Host is up (0.00011s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  tcpwrapped
13/tcp    open  daytime?
17/tcp    open  qotd?
22/tcp    open  ssh          OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8008/tcp   open  http         lighttpd 1.4.74

2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
[Detailed fingerprint data omitted for brevity]

MAC Address: 02:89:EC:B7:74:EF (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.00 seconds
```

1.2 Default Script Scan (-sC)

I sometimes use this one instead of `-sV` because it runs *default scripts*¹, which can give out additional information depending on the services running on the target. You can see a comparison in outputs between the two flags in the two boxes below.

Default Script Scan

```
$ sudo nmap -p- -sC {target_IP} # Do you notice how I had to scan all ports, not
just the top 1000?

Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-28 09:22 GMT
Nmap scan report for 10.10.219.233
Host is up (0.00024s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
|_smtp-commands: debra2.thm.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS
|_ , ENHANCEDSTATUSCODES, 8BITMIME, DSN, CHUNKING,
|_ ssl-cert: Subject: commonName=debra2.thm.local
|_ Not valid before: 2021-08-10T12:10:58
|_ Not valid after: 2031-08-08T12:10:58
|_ ssl-date: TLS randomness does not represent time
53/tcp    open  domain
|_ dns-nsid:
|_ bind.version: 9.18.28-1-deb12u2-Debian
80/tcp    open  http
|_ http-title: Welcome to nginx on Debian!
110/tcp   open  pop3
|_ pop3-capabilities: PIPELINING SASL UIDL STLS AUTH-RESP-CODE RESP-CODES CAPA TOP
|_ ssl-cert: Subject: commonName=debra2.thm.local
|_ Not valid before: 2021-08-10T12:10:58
|_ Not valid after: 2031-08-08T12:10:58
111/tcp   open  rpcbind
|_ rpcinfo:
|_   program version    port/proto  service
|_   100000  2,3,4      111/tcp    rpcbind
|_   100000  2,3,4      111/udp    rpcbind
|_   100000  3,4        111/tcp6   rpcbind
|_   100000  3,4        111/udp6   rpcbind
143/tcp   open  imap
|_ imap-capabilities: more LOGIN-REFERRALS have IDLE post-login STARTTLS listed
|_   ENABLE capabilities LOGINDISABLEDA0001 Pre-login SASL-IR OK ID LITERAL+
|_   IMAP4rev1
|_ ssl-cert: Subject: commonName=debra2.thm.local
|_ Not valid before: 2021-08-10T12:10:58
|_ Not valid after: 2031-08-08T12:10:58
993/tcp   open  imaps
|_ imap-capabilities: LOGIN-REFERRALS more IDLE capabilities OK post-login ENABLE
|_   listed have Pre-login SASL-IR AUTH=PLAINA0001 ID LITERAL+ IMAP4rev1
|_ ssl-cert: Subject: commonName=debra2.thm.local
|_ Not valid before: 2021-08-10T12:10:58
|_ Not valid after: 2031-08-08T12:10:58
995/tcp   open  pop3s
|_ pop3-capabilities: PIPELINING SASL(PLAIN) UIDL USER AUTH-RESP-CODE RESP-CODES
|_   CAPA TOP
|_ ssl-cert: Subject: commonName=debra2.thm.local
|_ Not valid before: 2021-08-10T12:10:58
|_ Not valid after: 2031-08-08T12:10:58
MAC Address: 02:DD:7B:88:3D:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 20.77 seconds
```

¹Default NSE Scripts, [Nmap.org](https://nmap.org)

Service Version Detection for Comparison

```
$ sudo nmap -sV {target_IP}

Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-28 09:21 GMT
Nmap scan report for 10.10.219.233
Host is up (0.0062s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol
2.0)
25/tcp    open  smtp      Postfix smtpd
53/tcp    open  domain    ISC BIND 9.18.28-1~deb12u2 (Debian Linux)
80/tcp    open  http      nginx 1.22.1
110/tcp   open  pop3      Dovecot pop3d
111/tcp   open  rpcbind   2-4 (RPC #100000)
143/tcp   open  imap      Dovecot imapd
993/tcp   open  ssl/imap  Dovecot imapd
995/tcp   open  ssl/pop3  Dovecot pop3d
MAC Address: 02:DD:7B:88:3D:75 (Unknown)
Service Info: Host: debra2.thm.local; OS: Linux; CPE: cpe:/o:
linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```