

Nmap Cheatsheet

Contents

1	Basic Nmap Commands	2
1.1	Service Version Detection (-sV)	2

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
```