NMAP CHEATSHEET

Zero To Mastery

V1.02

HEEELLLOOOOO!

I'm Andrei Neagoie, Founder and Lead Instructor of the Zero To Mastery Academy.

After working as a Senior Software Developer over the years, I now dedicate 100% of my time teaching others valuable software development skills, help them break into the tech industry, and advance their careers. In the last few years, **over 750,000** students around the world have taken my courses and many of them are now working at companies like **Apple**, **Google**, **Amazon**, **Tesla**, **IBM**, **Shopify**, just to name a few.

This cheatsheet provides you with all the Nmap essentials in one place. If you're new to the world of Ethical Hacking and want to learn how to use Nmap + Ethical Hacking + Penetration Testing from scratch and master the most modern ethical hacking tools and best practices for 2022, check out our Complete Ethical Hacking Bootcamp.

Happy hacking!
Andrei

Founder & Lead Instructor, Zero To Mastery
Andrei Neagoie

P.S. I also recently wrote a book called Principles For Programmers. You can download the first five chapters for free here.

CONTENTS

NMAP OVERVIEW

What is Nmap? Why is Nmap useful?

Nmap is an essential open-source tool for Ethical Hackers and Penetration testers. It was initially created by Gordon Lyon (aka Fyodor). Nmap themselves do a great job describing the tool (see below) and what is does, so why re-invent the wheel?

> *Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.*

Want to see what an actual Nmap scan looks like and how to perform an NMAP scan? Watch this free lesson from the Zero To Mastery Ethical Hacking Bootcamp.

NMAP HELP

We can use `nmap -h` to display an extended help menu of Nmap. In this extended help menu, you can find an overview of all possible options, and which arguments some of them require in order to work. Note that you can also use `man npm` for an in-depth manual about nmap.

NMAP TARGETING

Nmap is an interesting tool that can be used in various ways. You can scan one single target or multiple targets. Here is a list of examples, showing the ways you can target something:

Command	Description
`nmap 192.168.1.1`	Scanning a single IP
`nmap www.domain.com`	Scanning a hostname
`nmap 192.168.1.1-100`	Scanning an IP range
`nmap 192.168.1.1/24`	Scanning a subnet
`nmap -iL list.txt`	Scanning from a predefined list

NMAP SCAN TYPES

Besides the basic `nmap < target >`, we can also use various scanning types in Nmap. Each of them has their own unique capabilities, but also often come with the downside of one being noisier than the other. Let us see which types we have:

Command	Description	Root /Sudo	Noise level
nmap -sS <_target>	This is a TCP SYN SCAN, also known as a stealth scan. This scan only sends a SYN packet and awaits a SYN/ACK response. When nmap receives a SYN/ACK on a specific probed port, it means the port exists on the machine and is open. This is a fast and pretty accurate scan, which you will use most of the time.	Required	Very Low

nmap -sT <_target>	The -sT scan is more accurate than a -sS scan, but the downside is that it is slower, makes more noise and easily detected by well set-up firewalls. This is because it makes a full three-way handshake (or better said, a full TCP connection) with the host.	Not Required	Medium
nmap -sU <_target>	This scan is used to scan for UDP ports. This is typically a slower and more difficult scan. Though most services use TCP, there are also services that use UDP, such as: DNS, SNMP, DHCP. So this scan is still useful as there are still exploitable UDP services. So don't make the mistake of skipping this scan, you might find something!	Required	Medium
nmap -sn <_target(s)>	This is a simple and fast ping scan to see which hosts reply to ICMP ping packets. This is useful if you are on the same (sub)network as the IP range you are scanning and if you only want to know which devices are live. You can also get the same result by using -Pn.	Not Required	Very Low
nmap -sV <_target>	This is a service version scan. In order to know what exploits will work, it is very helpful to know the service version behind an open port. It might be that a certain exploit only works in one specific version of a certain service, as it might be patched in a new version.	Not Required	Medium
nmap -O <_target>	This is a remote OS detection scan. We use this scan to learn what OS the target runs on. This is very useful as it gives an idea of what kind of exploits might work on the target, and which exploits won't work. Note that this scan only works if there is at least 1 open port and 1 closed port..	Required	Medium
nmap -A <_target>	This is an aggressive scan. This scan performs an OS detection, version detection, script scanning, and traceroute. Though it returns a lot of information, you will be alarming the target as this is probably the noisiest scan.	Required	Very High

NMAP PORT SCANNING

Sometimes you want to know if a certain port is open on a target, or perhaps you want to know ALL open ports on the target. Luckily, Nmap provides its users with ways to specify this:

Command	Description
`nmap -p <_port> <_target>`	Use -p <_port> to scan for one specific port on the target.
`nmap -p <_port_range_begin>-<_port_range_end> <_target>`	You can also use -p to scan for a range of ports, -p 1-20 <_target> would scan for the ports 1 to 20 on the target.
`nmap -p <_port_a>, <_port_n> <_port_c> <_target>`	There is also the possibility to specify multiple specific ports by separating them with a comma.
`nmap -p U:<_udp_port>, T:<_tcp_port> <_target>`	There is also the possibility to specify multiple specific ports by separating them with a comma.
`nmap -F <_target>`	The -F tells Nmap to scan for the 100 most common ports that can be open on a target.
`nmap -top-ports <_amount <_target>`	With this option, you scan for the top # ports, depending on what amount you provide.
`nmap -p- <_target>`	This option tells Nmap to scan the target for all the known ports there are in the world... there are 655,355 ports in total. This will clearly make the scan take longer to finish.

NMAP TIMING OPTIONS

Nmap allows for the use of "timing templates", which allows the user to specify how aggressive they wish to be with their scans, while leaving Nmap to pick the exact timing values. There are 6 timing templates:

Command	Description
`nmap -T0 <_target>`	T0 is the slowest scan, also referred to as the "Paranoid" scan. This option is good for IDS evasion.
`nmap -T1 <_target>`	T1 is an option faster then T0, but is still referred to as the "Sneaky" template. This timing option is also a good choice for IDS evasion.
`nmap -T2 <_target>`	The T2 option is for a timely scan and is also known as the "Polite" timing option. This one slows the scan, which results in less bandwidth usage and less target machine resources
`nmap -T3 <_target>`	T3 is also known as the default scan timer. Using this template would be the same as not using it at all. This is what Nmap uses by default when there is no template selected.
`nmap -T4 <_target>`	T4 is an option to speed up scans by making the assumption that you are on a reasonably fast and reliable network. This time template is also referred to as the "Aggressive" template.
`nmap -T5 <_target>`	T5 is an insanely fast mode, assuming that you are on an extraordinarily fast network... or if you are willing to sacrifice some accuracy for speed. That is why it is also referred to as the "Insane" mode.

NMAP SCRIPTS

Last but not least... Nmap provides us with scripts. These scripts come in categories:

- auth
- broadcast
- default. discovery
- dos
- exploit
- external
- fuzzer
- intrusive
- malware
- safe
- version
- vuln

We run a script in the following way: `nmap --script <_script/_script_group> <_taget>`

Some scripts are very noisy, some not at all. Therefore, it is important to read what each script does and if it is easily detectable by the target or not.

Do note that you need to run `--script` scans as root/sudo.

EXTRAS & ADDITIONAL RESOURCES

When you are doing a pentest, it is useful to use the -oN option to output your scan to a text file. This way, you can copy-paste it later into your pentest report. Here is how to do it:
`nmap -oN <_filename.txt> <_target>`

You can also use multiple options in one scan. For example, this is probably the most common scan you will perform: `sudo nmap -sS <_target> -oN <_filename.txt>`

Lastly, we've added some screenshots of various commands on the next page.

nmap 192.168.0.239

```
[redacted]:~/Desktop$ nmap 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 05:59 CST
Nmap scan report for 192.168.0.239
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.11 seconds
[redacted]:~/Desktop$
```

nmap -p 80 192.168.0.239

```
[redacted]:~/Desktop$ nmap -p 80 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:10 CST
Nmap scan report for 192.168.0.239
Host is up (0.00047s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds
[redacted]:~/Desktop$
```

nmap -p- 192.168.0.239

```
[redacted]@[redacted]:~/Desktop$ nmap -p- 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:11 CST
Nmap scan report for 192.168.0.239
Host is up (0.00020s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33179/tcp open  unknown
44399/tcp open  unknown
45805/tcp open  unknown
51579/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds
[redacted]@[redacted]:~/Desktop$
```

sudo nmap -sV 192.168.0.239

```
[redacted]@[redacted]:~/Desktop$ sudo nmap -sV 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:05 CST
Nmap scan report for 192.168.0.239
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9F:F3:C9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 23.62 seconds
[redacted]@[redacted]:~/Desktop$
```

nmap -T4 192.168.0.239

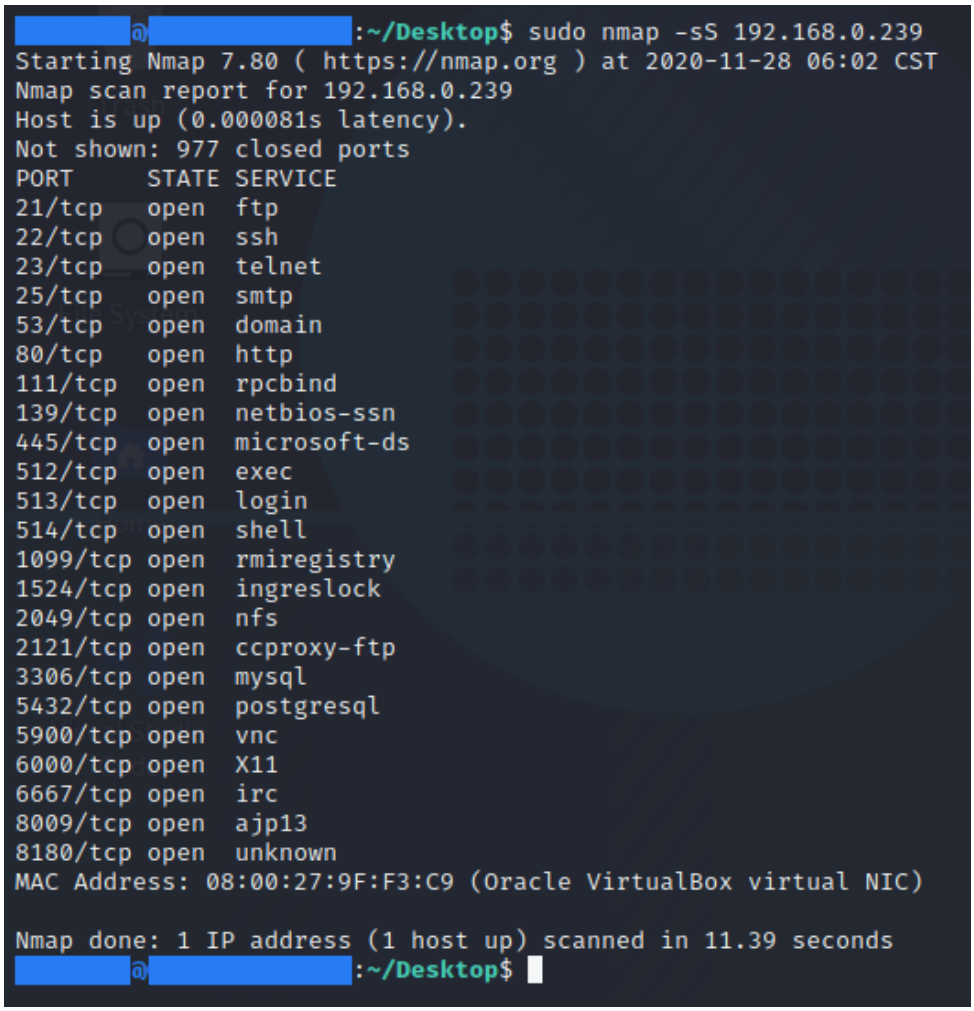
```
[redacted]@[redacted]:~/Desktop$ nmap -T4 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:19 CST
Nmap scan report for 192.168.0.239
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.11 seconds
[redacted]@[redacted]:~/Desktop$
```

nmap -sn 192.168.0.239

```
[redacted]@[redacted]:~/Desktop$ nmap -sn 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:04 CST
Nmap scan report for 192.168.0.239
Host is up (0.00039s latency).
Nmap done: 1 IP address (1 host up) scanned in 11.03 seconds
[redacted]@[redacted]:~/Desktop$
```

sudo nmap -sS 192.168.0.239



Want to dive deeper?

- Check out Gordon Lyon's Nmap Network Scanning book
- Take the Zero To Mastery Ethical Hacking Bootcamp

CREDITS

A huge thanks and credit goes to Zero To Mastery Star Mentor and Ethical Hacker, Thomas. This cheat sheet was created in part from his notes while taking and completing the Ethical Hacking Bootcamp course.