Nmap Cheat Sheet: Commands & Examples (2022) ∞

CHEAT-SHEET 18 Feb 2022 Arr0way

Nmap (network mapper), the god of port scanners used for network discovery and the basis for most security enumeration during the initial stages of a penetration test. The tool was written and maintained by Fyodor AKA Gordon Lyon.

Nmap displays exposed services on a target machine along with other useful information such as the verion and OS detection.

Nmap has made twelve movie appearances, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

Original Post Date: 13/12/2014 |
Last Updated: 18/02/2022

Table of Contents

Nmap in a nutshell

- Host discovery
- Port discovery / enumeration
- Service discovery
- Operating system version detection
- Hardware (MAC) address detection

All Blog
Cheat Sheets
Techniques
Security Hardening
WalkThroughs

CHEAT SHEETS

Reverse Shell Cheat Sheet: PHP, Python, Powershell, Bash, NC, JSP, Java, Perl
Nmap Cheat Sheet: Commands & Examples (2022)
DNS Tunneling dnscat2 Cheat Sheet
SSH Lateral Movement Cheat Sheet
Android Pen Testing Environment Setup
Password Reset Testing Cheat Sheet
SSRF Cheat Sheet & Bypass Techniques
Penetration Testing Tools Cheat Sheet
LFI Cheat Sheet
Vi Cheat Sheet
Systemd Cheat Sheet
nbtscan Cheat Sheet
Linux Commands Cheat Sheet
More »

WALKTHROUGHS

InsomniHack CTF Teaser - Smartcat2 Writeup
InsomniHack CTF Teaser - Smartcat1 Writeup
FristiLeaks 1.3 Walkthrough
SickOS 1.1 - Walkthrough
The Wall Boot2Root Walkthrough
More »

TECHNIQUES

SSH & Meterpreter Pivoting Techniques
More »

SECURITY HARDENING

Security Harden CentOS 7
More »

/DEV/URANDOM

MacBook - Post Install Config + Apps

- Service version detection
- Vulnerability / exploit detection, using Nmap scripts (NSE)
- Nmap IDS / Portscan Detection & Scan Time Optimisation

Nmap Command Examples

Basic Nmap scanning examples, often used at the first stage of enumeration.

COMMAND	DESCRIPTION
`nmap -sP 10.0.0.0/24`	Ping scans the network, listing machines that respond to ping.
`nmap -p 1-65535 -sV -sS -T4 target`	Full TCP port scan using with service version detection - usually my first scan, I find T4 more accurate than T5 and still "pretty quick".
`nmap -v -sS -A -T4 target`	Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + traceroute and scripts against target services.
`nmap -v -sS -A -T5 target`	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + traceroute and scripts against target services.
`nmap -v -sV -O -sS -T5 target`	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection.
`nmap -v -p 1-65535 -sV -O -sS -T4 target`	Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + full port range scan.
`nmap -v -p 1-65535 -sV -O -sS -T5 target`	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + full port range scan.

Agressive scan timings are faster, but could yeild inaccurate results!
T5 uses very aggressive scan timings and could lead to missed ports, T4 is a better compromise if you need fast results.

Nmap scan from file

COMMAND	DESCRIPTION
`nmap -iL ip-addresses.txt`	Scans a list of IP addresses, you can add options before / after.

Nmap Scan all Ports

COMMAND	DESCRIPTION
`nmap -p- target`	Nmap scan all ports, TCP ports.

Nmap output formats

COMMAND	DESCRIPTION
`nmap -sV -p 139,445 -oG grep-output.txt 10.0.1.0/24`	Outputs "grepable" output to a file, in this example Netbios servers. E.g, The output file could be grepped for "Open".
`nmap -sS -sV -T5 10.0.1.99 --webxml -oX - | xsltproc --output file.html -`	Export nmap output to HTML report.

Nmap Netbios Examples

COMMAND	DESCRIPTION

More »

OTHER BLOG

Insecure Direct Object Reference (IDOR): Definition, Examples & How to Find
Encrypted Notes App Solution (iOS, Android, MacOS, Linux, Windows)
HowTo: Kali Linux Chromium Install for Web App Pen Testing
Jenkins RCE via Unauthenticated API
MacBook - Post Install Config + Apps
enum4linux Cheat Sheet
Linux Local Enumeration Script
HowTo Install Quassel on Ubuntu
HowTo Install KeepNote on OSX Mavericks

COMMAND	DESCRIPTION
`nmap -sV -v -p 139,445 10.0.0.1/24`	Find all Netbios servers on subnet
`nmap -sU --script nbstat.nse -p 137 target`	Nmap display Netbios name
`nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p 445 target`	Nmap check if Netbios servers are vulnerable to MS08-067

!! --script-args=unsafe=1 has the potential to crash servers / services
Becareful when running this command.

Nmap Nikto Scan

COMMAND	DESCRIPTION
`nmap -p80 10.0.1.0/24 -oG - | nikto.pl -h -`	Scans for http servers on port 80 and pipes into Nikto for scanning.
`nmap -p80,443 10.0.1.0/24 -oG - | nikto.pl -h -`	Scans for http/https servers on port 80, 443 and pipes into Nikto for scanning.

Nmap Cheatsheet

Target Specification

Nmap allows hostnames, IP addresses, subnets.

Example blah.highon.coffee, nmap.org/24, 192.168.0.1; 10.0.0-255.1-254

COMMAND	DESCRIPTION
`-iL`	inputfilename: Input from list of hosts/networks
`-iR`	num hosts: Choose random targets
`--exclude`	host1[,host2][,host3],... : Exclude hosts/networks
`--excludefile`	exclude_file: Exclude list from file

Host Discovery

COMMAND	DESCRIPTION
`-sL`	List Scan - simply list targets to scan
`-sn`	Nmap ping scan / sweep - runs a nmap network scan, with port scanning disabled
`-Pn`	Treat all hosts as online -- skip host discovery
`-PS/PA/PU/PY[portlist]`	TCP SYN/ACK, UDP or SCTP discovery to given ports. Allows you to specify a specific port nmap uses to verify a host is up e.g., -PS22 (by default nmap sends to a bunch of common ports, this allows you to be specific)
`-PE/PP/PM`	ICMP echo, timestamp, and netmask request discovery probes
`-PO[protocol list]`	IP Protocol Ping
`-n/-R`	Never do DNS resolution/Always resolve [default: sometimes]

Scan Techniques

COMMAND	DESCRIPTION

`-sS`
`-sT`
`-sA`
`-sW`
`-sM`
	TCP SYN scan
	Connect scan
	ACK scan
	Window scan
	Maimon scan

COMMAND	DESCRIPTION
`-sU`	UDP Scan

`-sN`
`-sF`
`-sX`
	TCP Null scan
	FIN scan
	Xmas scan

`--scanflags`	Customize TCP scan flags
`-sI zombie host[:probeport]`	Idle scan
`-sY` `-sZ`	SCTP INIT scan COOKIE-ECHO scan
`-sO`	IP protocol scan
`-b "FTP relay host"`	FTP bounce scan

Port Specification and Scan Order

COMMAND	DESCRIPTION
`-p`	Specify ports, e.g. -p80,443 or -p1-65535
`-p U:PORT`	Scan UDP ports with Nmap, e.g. -p U:53
`-F`	Fast mode, scans fewer ports than the default scan
`-r`	Scan ports consecutively - don't randomize
`--top-ports "number"`	Scan "number" most common ports
`--port-ratio "ratio"`	Scan ports more common than "ratio"

Service Version Detection

COMMAND	DESCRIPTION
`-sV`	Probe open ports to determine service/version info
`--version-intensity "level"`	Set from 0 (light) to 9 (try all probes)
`--version-light`	Limit to most likely probes (intensity 2)
`--version-all`	Try every single probe (intensity 9)
`--version-trace`	Show detailed version scan activity (for debugging)

Script Scan

COMMAND	DESCRIPTION
`-sC`	equivalent to --script=default
`--script="Lua scripts"`	"Lua scripts" is a comma separated list of directories, script-files or script-categories
`--script-args=n1=v1,[n2=v2,...]`	provide arguments to scripts
`-script-args-file=filename`	provide NSE script args in a file
`--script-trace`	Show all data sent and received
`--script-updatedb`	Update script database
`--script-help="Lua scripts"`	Show help about scripts

OS Detection

COMMAND	DESCRIPTION
`-O`	Enable OS Detection
`--osscan-limit`	Limit OS detection to promising targets
`--osscan-guess`	Guess OS more aggressively

Timing and Performance

Options which take TIME are in seconds, or append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

COMMAND	DESCRIPTION
`-T 0-5`	Set timing template - higher is faster (less accurate)
`--min-hostgroup SIZE` `--max-hostgroup SIZE`	Parallel host scan group sizes
`--min-parallelism NUMPROBES` `--max-parallelism NUMPROBES`	Probe parallelization

`--min-rtt-timeout TIME`
`--max-rtt-timeout TIME`
`--initial-rtt-timeout TIME`
	Specifies probe round trip time

`--max-retries TRIES`	Caps number of port scan probe retransmissions
`--host-timeout TIME`	Give up on target after this long
`--scan-delay TIME` `--max-scan-delay TIME`	Adjust delay between probes
`--min-rate NUMBER`	Send packets no slower than NUMBER per second
`--max-rate NUMBER`	Send packets no faster than NUMBER per second

Firewalls IDS Evasion and Spoofing

COMMAND	DESCRIPTION
`-f; --mtu VALUE`	Fragment packets (optionally w/given MTU)
`-D decoy1,decoy2,ME`	Cloak a scan with decoys
`-S IP-ADDRESS`	Spoof source address
`-e IFACE`	Use specified interface
`-g PORTNUM` `--source-port PORTNUM`	Use given port number
`--proxies url1,[url2],...`	Relay connections through HTTP / SOCKS4 proxies
`--data-length NUM`	Append random data to sent packets
`--ip-options OPTIONS`	Send packets with specified ip options
`--ttl VALUE`	Set IP time to live field
`--spoof-mac ADDR/PREFIX/VENDOR`	Spoof NMAP MAC address
`--badsum`	Send packets with a bogus TCP/UDP/SCTP checksum

Nmap Output Options

COMMAND	DESCRIPTION
`-oN`	Output Normal
`-oX`	Output to XML
`-oS`	Script Kiddie / 1337 speak... sigh
`-oG`	Output greppable - easy to grep nmap output
`-oA BASENAME`	Output in the three major formats at once
`-v`	Increase verbosity level use -vv or more for greater effect
`-d`	Increase debugging level use -dd or more for greater effect
`--reason`	Display the reason a port is in a particular state
`--open`	Only show open or possibly open ports

COMMAND	DESCRIPTION
`--packet-trace`	Show all packets sent / received
`--iflist`	Print host interfaces and routes for debugging
`--log-errors`	Log errors/warnings to the normal-format output file
`--append-output`	Append to rather than clobber specified output files
`--resume FILENAME`	Resume an aborted scan
`--stylesheet PATH/URL`	XSL stylesheet to transform XML output to HTML
`--webxml`	Reference stylesheet from Nmap.Org for more portable XML
`--no-stylesheet`	Prevent associating of XSL stylesheet w/XML output

Misc Nmap Options

COMMAND	DESCRIPTION
`-6`	Enable IPv6 scanning
`-A`	Enable OS detection, version detection, script scanning, and traceroute
`--datedir DIRNAME`	Specify custom Nmap data file location
`--send-eth` `--send-ip`	Send using raw ethernet frames or IP packets
`--privileged`	Assume that the user is fully privileged
`--unprivileged`	Assume the user lacks raw socket privileges
`-V`	Show nmap version number
`-h`	Show nmap help screen

Nmap Enumeration Examples

The following are real world examples of Nmap enumeration.

Enumerating Netbios

The following example enumerates Netbios on the target networks, the same process can be applied to other services by modifying ports / NSE scripts.

Detect all exposed Netbios servers on the subnet.

Nmap find exposed Netbios servers

```
root:~# nmap -sV -v -p 139,445 10.0.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: MEGATRON)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
</p>
```

Nmap find Netbios name.

Nmap find exposed Netbios servers

```
root:~# nmap -sU --script nbstat.nse -p 137 10.0.1.12

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 21:26 GMT
```

```
Nmap scan report for nas.decepticons 10.0.1.12
Host is up (0.014s latency).

PORT STATE SERVICE VERSION
137/udp open netbios-ns

Host script results:
|_nbstat: NetBIOS name: STARSCREAM, NetBIOS user: unknown, NetBIOS
MAC: unknown (unknown)
Nmap done: 256 IP addresses (1 hosts up) scanned in 28.74 seconds
</p>
```

Check if Netbios servers are vulnerable to MS08-067

Nmap check MS08-067

```
root:~#
nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p 445
10.0.0.1

Nmap scan report for ie6winxp.decepticons (10.0.1.1)
Host is up (0.00026s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
| smb-check-vulns:
| MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: NOT VULNERABLE
| SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|_ MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds
</p>
```

The information gathered during the enumeration indicates the target is vulnerable to MS08-067, exploitation will confirm if it's vulnerable to MS08-067.

Nmap Scan Optimisation

Nmap Rate

To speed up your scan increase the rate, be aware that setting a high rate value will result in a less accurate scan.

```
--max-rate
--min-rate
```

Parallelism

The maximum or minimum amount of parallel tasks.

TIP: If you have an basic IDS / portscan detection blocking your scans you could lower the –min-parallelism in an attempt to reduce the number of concurrent connections

```
--min-parallelism
--max-parallelism
```

Host Group Sizes

The number of hosts scanned at the same time, Note: if you are writing output to a file e.g., -oA you will need to wait for the host group to complete scanning before the nmap output will be written to the file. Therefore if you get a lagging host you will may end up waiting a while for the output file, which brings us on to… host timeout.

```
--min-hostgroup
--max-hostgroup
```

Host Timeout

Nmap allows you to specify the timeout, which is the length of time it waits before giving up on the target. Be careful setting this super low, as you may end up with inaccurate results.

The following example would giveup after 50 seconds.

```
--host-timeout 50
```

Scan Delay

An extremely useful option to defeat basic port scan detection (SOHO devices and some IDS) that essentially monitor and block X amount of connects per second (syn flood etc).

```
--scan-delay 5s
```

For example if you know you can get away with 2 req/sec without getting blacklisted then you could use:

```
--scan-delay 1.2
```

added 200ms for a buffer

Disable DNS Lookups

Assuming you do not want domain names being looked up, use the `-n` flag to dissable resolution and speed up the scan.

Nmap Black List Detection?

1. It ussally takes and extemely long time to complete
2. Droppped probes nmap will increase the timeout, but it's likely you are already black listed
3. To confirm, recheck a port that you know was open before

As far as I know there is no way of detecting for black listing within nmap natively.

Optimising Portscans for Targets

Once you have identified a target firewall / IDS you can look up the default settings for the portscan black list by reading the manual and use the nmap command switches above to obtain the best performance without getting black listed.

Follow Arr0way

Twitter GitHub

Also...

You might want to read these

CATEGORY	POST NAME
cheat-sheet	Reverse Shell Cheat Sheet: PHP, Python, Powershell, Bash, NC, JSP, Java, Perl
Web App Security	Insecure Direct Object Reference (IDOR): Definition, Examples & How to Find
SecOps	Encrypted Notes App Solution (iOS, Android, MacOS, Linux, Windows)
cheat-sheet	DNS Tunneling dnscat2 Cheat Sheet
cheat-sheet	SSH Lateral Movement Cheat Sheet
cheat-sheet	Android Pen Testing Environment Setup
cheat-sheet	Password Reset Testing Cheat Sheet
cheat-sheet	SSRF Cheat Sheet & Bypass Techniques
cheat-sheet	Penetration Testing Tools Cheat Sheet
cheat-sheet	LFI Cheat Sheet