



# Nmap Cheat Sheet

**CHEAT-SHEET**13 Dec 2014  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 penetration testing. 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 version and OS

## Table of Contents

- Nmap Examples
  - Nmap scan from file
  - Nmap output formats
  - Nmap Netbios Examples
  - Nmap Nikto Scan
- Nmap Cheatsheet
  - Target Specification
  - Host Discovery
  - Scan Techniques

All Blog  
Cheat Sheets  
Techniques  
Security Hardening  
WalkThroughs

## CHEAT SHEETS

Penetration Testing Tools  
Cheat Sheet  
LFI Cheat Sheet  
Vi Cheat Sheet  
Systemd Cheat Sheet  
Reverse Shell Cheat Sheet  
nbtscan Cheat Sheet  
Nmap Cheat Sheet  
Linux Commands Cheat

detection.

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



```

80/tcp open http host2.ns [mobile]
81/tcp open http host2.ns
10/ [mobile]
11 $ nmap -v -sS -O 10.2.2.2
11
13 Starting nmap 0.2.5ABETA25
13 Insufficient responses for TCP sequencing (3), OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
14 (The 1539 ports scanned but not shown below are in state: closed)
15 Port      State    Service
15 22/tcp    open     ssh
16
17 No exact OS matches for host
18
19 Nmap run completed -- 1 IP address (1 host up) scanned
20 $ sshmu 10.2.2.2 -rootpu="Z10H0101"
21 Connecting to 10.2.2.2:ssh ...
22 Re-Attempting to exploit SSHv1 CRC32 ...
23 IP Resetting root password to "Z10H0101" ...
24 System open: Access Level <9>
25 $ ssh 10.2.2.2 -1 root
26 root@10.2.2.2's password: [REDACTED]
27 [REDACTED] ACCESS GRANTED
  
```

## Nmap in a nutshell

- Port Specification and Scan Order
- Service Version Detection
- Script Scan
- OS Detection
- Timing and Performance
- Firewalls/IDS Evasion and Spoofing
- Nmap Output Options
- Misc Nmap Options
- Nmap Enumeration Examples
  - Enumerating Netbios

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](#)

- Host discovery
- Port discovery / enumeration
- Service discovery
- Operating system version detection
- Hardware (MAC) address detection
- Service version detection
- Vulnerability / exploit detection, using Nmap scripts (NSE)

## Nmap Examples

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

COMMAND	DESCRIPTION
<code>nmap -sP 10.0.0.0/24</code>	Ping scans the network, listing machines that respond to ping.
<code>nmap -p 1-65535 -sV -sS -T4 target</code>	Full TCP port scan using with service version detection - usually my first scan, I find T4 more accurate than T5 and still "pretty quick".
	Prints verbose output, runs stealth syn

7  
More »

### /DEV/URANDOM

MacBook - Post Install  
Config + Apps  
More »

### OTHER BLOG

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

<code>nmap -v -sS -A -T4 target</code>	scan, T4 timing, OS and version detection + traceroute and scripts against target services.
<code>nmap -v -sS -A -T5 target</code>	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + traceroute and scripts against target services.
<code>nmap -v -sV -O -sS -T5 target</code>	Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection.
<code>nmap -v -p 1-65535 -sV -O -sS -T4 target</code>	Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + full port range scan.
<code>nmap -v -p 1-65535 -sV -O -sS -T5 target</code>	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
<code>nmap -iL ip-addresses.txt</code>	Scans a list of IP addresses, you can add options before / after.

## Nmap output formats

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

## Nmap Netbios Examples

COMMAND	DESCRIPTION
<code>nmap -sV -v -p 139,445 10.0.0.1/24</code>	Find all Netbios servers on subnet
<code>nmap -sU --script nbstat.nse -p 137 target</code>	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
<pre>nmap -p80 10.0.1.0/24 -oG -   nikto.pl -h -</pre>	Scans for http servers on port 80 and pipes into Nikto for scanning.
<pre>nmap -p80,443 10.0.1.0/24 -oG -   nikto.pl -h -</pre>	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
<code>-iL</code>	inputfilename: Input from list of hosts/networks
<code>-iR</code>	num hosts: Choose random targets
<code>--exclude</code>	host1[,host2][,host3],... : Exclude hosts/networks
<code>--excludefile</code>	exclude_file: Exclude list from file

## Host Discovery

COMMAND	DESCRIPTION
<code>-sL</code>	List Scan - simply list targets to scan
<code>-sn</code>	Ping Scan - disable port scan
<code>-Pn</code>	Treat all hosts as online -- skip host discovery
<code>-PS/PA/PU/PY[portlist]</code>	TCP SYN/ACK, UDP or SCTP discovery to given ports
<code>-PE/PP/PM</code>	ICMP echo, timestamp, and netmask request discovery probes
<code>-PO[protocol list]</code>	IP Protocol Ping

`-n / -R`

Never do DNS resolution/Always resolve [default: sometimes]

## Scan Techniques

COMMAND	DESCRIPTION
<code>-sS</code> <code>-sT</code> <code>-sA</code> <code>-sW</code> <code>-sM</code>	TCP SYN scan Connect scan ACK scan Window scan Maimon scan
<code>-sU</code>	UDP Scan
<code>-sN</code> <code>-sF</code> <code>-sX</code>	TCP Null scan FIN scan Xmas scan
<code>--scanflags</code>	Customize TCP scan flags
<code>-sI zombie host[:probeport]</code>	Idle scan
<code>-sY</code> <code>-sZ</code>	SCTP INIT scan COOKIE-ECHO scan
<code>-sO</code>	IP protocol scan

```
-b "FTP relay host"
```

FTP bounce scan

## Port Specification and Scan Order

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

## Service Version Detection

COMMAND	DESCRIPTION
<code>-sV</code>	Probe open ports to determine service/version info
<code>--version-intensity "level"</code>	Set from 0 (light) to 9 (try all probes)
<code>--version-light</code>	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
<code>-sC</code>	equivalent to <code>--script=default</code>
<code>--script="Lua scripts"</code>	"Lua scripts" is a comma separated list of directories, script-files or script-categories
<code>--script-args=n1=v1,[n2=v2,...]</code>	provide arguments to scripts
<code>-script-args-file=filename</code>	provide NSE script args in a file
<code>--script-trace</code>	Show all data sent and received
<code>--script-updatedb</code>	Update script database
<code>--script-help="Lua scripts"</code>	Show help about scripts

## OS Detection

COMMAND	DESCRIPTION

<code>-O</code>	Enable OS Detection
<code>--osscan-limit</code>	Limit OS detection to promising targets
<code>--osscan-guess</code>	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
<code>-T 0-5</code>	Set timing template - higher is faster (less accurate)
<code>--min-hostgroup SIZE</code> <code>--max-hostgroup SIZE</code>	Parallel host scan group sizes
<code>--min-parallelism NUMPROBES</code> <code>--max-parallelism NUMPROBES</code>	Probe parallelization
<code>--min-rtt-timeout TIME</code> <code>--max-rtt-timeout TIME</code> <code>--initial-rtt-timeout TIME</code>	Specifies probe round trip time
<code>--max-retries TRIES</code>	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
--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.

## Share this on...

 Twitter  Facebook  Google+  Reddit

## Follow Arr0way

 Twitter  GitHub

## Also...