Nmap Cheat Sheet ∞

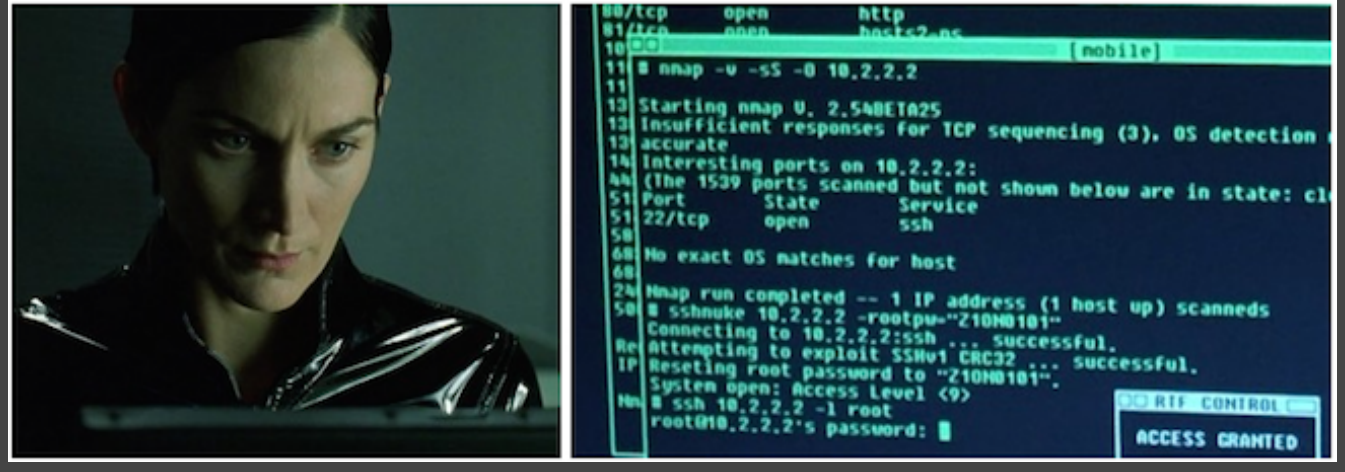
CHEAT-SHEET 13 Dec 2014  Arr0way

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 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.

Table of Contents



Nmap in a nutshell

- 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
`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".
	Prints verbose output, runs stealth syn scan,

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
More »

OTHER BLOG

HowTo: Kali

`nmap -v -sS -A -T4 target`	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 output formats

COMMAND	DESCRIPTIC
`nmap -sV -p 139,445 -oG grep-output.txt 10.0.1.0/24`	Outputs "grepable" output to a fil in this examp Netbios servers. E.g, The outp 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
`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`	Ping Scan - disable port scan
`-Pn`	Treat all hosts as online -- skip host discovery
`-PS/PA/PU/PY[portlist]`	TCP SYN/ACK, UDP or SCTP discovery to given ports
`-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

`-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
`--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.

Also...

You might want to read these

CATEGORY	POST NAME
cheat-sheet	Penetration Testing Tools Cheat Sheet
cheat-sheet	LFI Cheat Sheet
kali linux	HowTo: Kali Linux Chromium Install for Web App Pen Testing
walkthroughs	InsomniHack CTF Teaser - Smartcat2 Writeup
walkthroughs	InsomniHack CTF Teaser - Smartcat1 Writeup
walkthroughs	FristiLeaks 1.3 Walkthrough
walkthroughs	SickOS 1.1 - Walkthrough
walkthroughs	The Wall Boot2Root Walkthrough
walkthroughs	/dev/random: Sleepy Walkthrough CTF
walkthroughs	/dev/random Pipe walkthrough