Network Recon Cheat Sheet

by coffeefueled via cheatography.com/25996/cs/7096/

Nmap Base Syntax

```
# nmap [Scan Type] [Options] {targets}
```

Target Specification

Single IPv4: `192.16 8.1.1`

Single IPv6: `AAAA::FF`

FQDN: `host.local`

IPv4 Range: `192.16 8.1.27-78`

CIDR Block: `192.16 8.1.0/16`

File: `-iL target s.txt`

Host Discovery Options

`-sL`	list hosts and reverse DNS
`-sn`	discovery probes only
`-Pn`	skip discovery stage
`-n`	disable reverse DNS resolution
`-R`	force reverse DNS resolution

`--dns-servers <list>`

Scan Options

TCP Scan Types

`-sS`	SYN
`-sT`	Connect
`-sN`	NULL
`-sF`	FIN
`-sX`	Xmas (FIN, PSH, URG)
`-sA`	ACK
`-sW`	Window
`-sM`	FIN/ACK
`-sI <zombie host>`	use zombie
`--scan flags [flags]`	`URG/AC K/P SH/ RST /SY - N/FIN`

Scan Options (cont)

UDP Scan

`-sU`	UDP

SCTP Scan Types

`-sY`	INIT
`-sZ`	COOKIE ECHO

Protocol Scan

`-sO`	IP Protocol Scan

-p - Port Options

Exclude ports

> `--exclude ports <port ranges>`

Protocol specification

> `T21-25` - TCP ports 21 to 25
>
> `U53,11 1,137` - UDP ports 53, 111, 137
>
> `S22` - SCTP port 22
>
> `P` - IP Protocol

Fast port scan

> `-F` - scan top 100 ports (default 1000)

Sequential port scan

> `-r` - sequential scan (default random)

Ports in nmap-services file

> `[1-65535]` - ports in nmap-services
>
> `--port -ratio` - ports with greater ratio
>
> `--top- ports <n>` - n highest ratio

-o - OS Detection Options

`--ossc an- lim it`	only live machines
`--fuzzy`	low-probability guesses

Output Options

`-v|vv|vvv`	verbosity
`-d< 0-9>`	debugging
`--reason`	explain port and host states

File Outputs

`-oN <fi le>`	normal
`oX <fi le>`	XML
`-oS <fi le>`	script kiddie
`-oG <fi le>`	grepable
`-oA <ba sen am e>`	all

Scripting Engine Options

Use default scripts

> `-sC`
>
> `--scri pt= default`

Run scripts (individual or list)

> `--script`
>
> `<fi len ame>` - script filename
>
> `<ca teg ory>` - category of scripts
>
> `<di rec tor y>` - scripts in directory
>
> `<ex pre ssi on>` - boolean expression
>
> `[,...]` - continue comma separated list

Script arguments

> `--scri pt-args`
>
> `<n1 >=< v1>`
>
> `<n2 >={ <n3 >=< v3>}`
>
> `<n4 >={ <v4 >,< v5>}`

Load script args from a file

> `--scri pt- arg s-file <fi len - ame>`

Debug information

> `--scri pt- trace`

Update script database

> `--scri pt- upd atedb`

By **coffeefueled**

cheatography.com/coffeefueled/

Published 11th February, 2016.

Last updated 13th May, 2016.

Cheatography

Network Recon Cheat Sheet

by coffeefueled via cheatography.com/25996/cs/7096/

-sV - Version Detection Options

send less common probes (default 7)

```
--version intensity <0- 9>
```

light version scanning (intensity 2)

```
--version light
```

full version scanning (intensity 9)

```
--vers ion-all
```

debug information

```
--vers ion -trace
```

Miscellaneous Options

-6	IPv6
-A	Aggressive -O -sV -sC --trac eroute
-T	Timing options
paranoid|0	slowest scan
sneaky|1	slower scan
polite|2	slow scan
normal|3	default
aggres sive|4	faster scan
insane|5	fastest scan

Runtime Commands

v|V	+|- verbosity
d|D	+|- debugging
p|P	on|off packet tracing

DNS Enumeration

dnsrecon

--domain	domain to target
--range	IP range for reverse lookup
--name _server	DNS server
--dict ionary <fi le>	dictionary of targets
--type	type of enumeration
std	standard
goo	Google
axfr	sub-domains
tld	test for zone transfers
	test against IANA TLDs
-w	deep whois analysis
--csv	export to CSV

dnsenum

--dnss erver <se rve r>	target dns server
--subfile <fi le>	output file

Service Enumeration

Useful command lines

```
nmap -v -p <po rts> -oG <fi le> <ad dress ran ge>
```

```
ls -l /usr/s har e/n map /sc rip ts/ <pr oto - col >*
```

SMB TCP 139,445

nbtscan

-r	use port 137
<ad dress range>	targets

enum4linux

-a	all simple enumeration
-u user -p pa ss	authenticated

SMTP TCP 25, 110

nc -nv <ad dre ss> 25

VRFY	verify address
EXPN	query mail list

SNMP UDP 161

onesix tyone

-c <fi le>	community strings
-i <fi le>	targets
-o <fi le>	output file

snmpwalk [opt] agent [OID]

-c <st rin g>	community string
-v{1|2c|3}	version
snmpcheck	enumeration tool
-t <ad dre ss>	target
-c	community string
-w	detect write access

SQL TCP 1433,3306

sqlmap

--url= " url - "	target
--dbms =<D BM S>	force dbms
-a	retrieve all
--dump	dump data
--os-shell	retrieve shell
--crawl <de p th>	crawl site

By **coffeefueled**

cheatography.com/coffeefueled/

Published 11th February, 2016.
Last updated 13th May, 2016.