

Nmap Base Syntax

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

Target Specification

Single IPv4: 192.168.1.1

Single IPv6: AAAA::FF

FQDN: host.local

IPv4 Range: 192.168.1.27-78

CIDR Block: 192.168.1.0/16

File: -iL targets.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 use zombie

host>

--scanflags URG/ACK/PSH/RST/SY
[flags] 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

U53,111,137 - 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

--osscan-limit 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 <file> normal

oX <file> XML

-oS <file> script kiddie

-oG <file> grepable

-oA all

<basename>

Scripting Engine Options

Use default scripts

-sC

--script=default

Run scripts (individual or list)

--script

<filename> - script filename

<category> - category of scripts

<directory> - scripts in directory

<expression> - boolean expression

[,...] - continue comma separated list

Script arguments

--script-args

<n1>=<v1>

<n2>={<n3>=<v3>}

<n4>={<v4>,<v5>}

Load script args from a file

--script-args-file <filename>

Debug information

--script-trace

Update script database

--script-updatedb



By **coffeefueled**

cheatography.com/coffeefueled/

Published 11th February, 2016.

Last updated 13th May, 2016.

Page 1 of 2.

Sponsored by **Readability-Score.com**

Measure your website readability!

<https://readability-score.com>

-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)

```
--version-all
```

debug information

```
--version-trace
```

Miscellaneous Options

-6 IPv6

-A Aggressive -O -sV -sC --
traceroute

-T Timing options

```
paranoid|0 slowest scan
sneaky|1 slower scan
polite|2 slow scan
normal|3 default
aggressive|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

--dictionary dictionary of targets
<file>

--type type of enumeration
std standard
goo Google sub-
domains
axfr test for zone
transfers
tld test against IANA
TLDs

-w deep whois analysis

--csv export to CSV

dnsenum

--dnsserver target dns server
<server>

--subfile output file
<file>

Service Enumeration

Useful command lines

```
nmap -v -p <ports> -oG <file>
<address range>
```

```
ls -l
/usr/share/nmap/scripts/<protocol>*
```

SMB TCP 139,445

nbtscan

-r use port 137

<address range> targets

enum4linux

Service Enumeration (cont)

-a all simple
enumeration

-u user -p authenticated
pass

SMTP TCP 25, 110

nc -nv <address> 25

VRFY verify address

EXPN query mail list

SNMP UDP 161

onesixtyone

-c <file> community strings

-i <file> targets

-o <file> output file

snmpwalk [opt] agent [OID]

-c <string> community string

-v {1|2c|3} version

snmpcheck enumeration tool

```
-t <address> target
-c community string
-w detect write access
```

SQL TCP 1433,3306

sqlmap

--url="url" target

--dbms=<DBMS> force dbms

-a retrieve all

--dump dump data

--os-shell retrieve shell

--crawl crawl site

<depth>



By **coffeefueled**

cheatography.com/coffeefueled/

Published 11th February, 2016.

Last updated 13th May, 2016.

Page 2 of 2.

Sponsored by **Readability-Score.com**

Measure your website readability!

<https://readability-score.com>