

## Scripting Engine

```
-sC Run default scripts
--script=<ScriptName>|
<ScriptCategory>|<ScriptDir>...
    Run individual or groups of scripts
--script-args=<Name1=Value1,...>
    Use the list of script arguments
--script-updatedb
    Update script database
```

## Script Categories

Nmap's script categories include, but are not limited to, the following:

**auth:** Utilize credentials or bypass authentication on target hosts.

**broadcast:** Discover hosts not included on command line by broadcasting on local network.

**brute:** Attempt to guess passwords on target systems, for a variety of protocols, including http, SNMP, IAX, MySQL, VNC, etc.

**default:** Scripts run automatically when -sC or -A are used.

**discovery:** Try to learn more information about target hosts through public sources of information, SNMP, directory services, and more.

**dos:** May cause denial of service conditions in target hosts.

**exploit:** Attempt to exploit target systems.

**external:** Interact with third-party systems not included in target list.

**fuzzer:** Send unexpected input in network protocol fields.

**intrusive:** May crash target, consume excessive resources, or otherwise impact target machines in a malicious fashion.

**malware:** Look for signs of malware infection on the target hosts.

**safe:** Designed not to impact target in a negative fashion.

**version:** Measure the version of software or protocol spoken by target hosts.

**vul:** Measure whether target systems have a known vulnerability.

## Notable Scripts

A full list of Nmap Scripting Engine scripts is available at <http://nmap.org/nsedoc/>

Some particularly useful scripts include:

*dns-zone-transfer:* Attempts to pull a zone file (AXFR) from a DNS server.

```
$ nmap --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain> -p53 <hosts>
```

*http-robots.txt:* Harvests robots.txt files from discovered web servers.

```
$ nmap --script http-robots.txt <hosts>
```

*smb-brute:* Attempts to determine valid username and password combinations via automated guessing.

```
$ nmap --script smb-brute.nse -p445 <hosts>
```

*smb-psexec:* Attempts to run a series of programs on the target machine, using credentials provided as scriptargs.

```
$ nmap --script smb-psexec.nse --script-args=smbuser=<username>,smbpass=<password>[,config=<config>] -p445 <hosts>
```

**SANS**  
INSTITUTE

**Nmap**  
**Cheat Sheet**  
**v1.0**

POCKET REFERENCE GUIDE  
SANS Institute  
<http://www.sans.org>

## Base Syntax

```
# nmap [ScanType] [Options] {targets}
```

## Target Specification

IPv4 address: 192.168.1.1  
IPv6 address: AABB:CCDD::FF%eth0  
Host name: www.target.tgt  
IP address range: 192.168.0-255.0-255  
CIDR block: 192.168.0.0/16  
Use file with lists of targets: -iL <filename>

## Target Ports

No port range specified scans 1,000 most popular ports

-F Scan 100 most popular ports

-p<port1>-<port2> Port range

-p<port1>,<port2>,... Port List

-pU:53,U:110,T20-445 Mix TCP and UDP

-r Scan linearly (do not randomize ports)

--top-ports <n> Scan n most popular ports

-p-65535 Leaving off initial port in range makes Nmap scan start at port 1

-p0- Leaving off end port in range makes Nmap scan through port 65535

-p- Scan ports 1-65535

### Probing Options

- Pn** Don't probe (assume all hosts are up)
- PB** Default probe (TCP 80, 445 & ICMP)
- PS**<portlist>  
Check whether targets are up by probing TCP ports
- PE** Use ICMP Echo Request
- PP** Use ICMP Timestamp Request
- PM** Use ICMP Netmask Request

### Scan Types

- sP** Probe only (host discovery, not port scan)
- sS** SYN Scan
- sT** TCP Connect Scan
- sU** UDP Scan
- sV** Version Scan
- o** OS Detection
- scanflags** Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

### Fine-Grained Timing Options

- min-hostgroup/max-hostgroup** <size>  
Parallel host scan group sizes
- min-parallelism/max-parallelism** <numprobes>  
Probe parallelization
- min-rtt-timeout/max-rtt-timeout/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/--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

### Aggregate Timing Options

- T0** *Paranoid*: Very slow, used for IDS evasion
- T1** *Sneaky*: Quite slow, used for IDS evasion
- T2** *Polite*: Slows down to consume less bandwidth, runs ~10 times slower than default
- T3** *Normal*: Default, a dynamic timing model based on target responsiveness
- T4** *Aggressive*: Assumes a fast and reliable network and may overwhelm targets
- T5** *Insane*: Very aggressive; will likely overwhelm targets or miss open ports

### Output Formats

- oN** Standard Nmap output
- oG** Greppable format
- oX** XML format
- oA** <basename>  
Generate Nmap, Greppable, and XML output files using basename for files

### Misc Options

- n** Disable reverse IP address lookups
- 6** Use IPv6 only
- A** Use several features, including OS Detection, Version Detection, Script Scanning (default), and traceroute
- reason** Display reason Nmap thinks port is open, closed, or filtered