## ****Timing and Performance****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -T0 | nmap 192.168.1.1 -T0 | Paranoid (0) Intrusion Detection System evasion |
| -T1 | nmap 192.168.1.1 -T1 | Sneaky (1) Intrusion Detection System evasion |
| -T2 | nmap 192.168.1.1 -T2 | Polite (2) slows down the scan to use less bandwidth and use less target machine resources |
| -T3 | nmap 192.168.1.1 -T3 | Normal (3) which is default speed |
| -T4 | nmap 192.168.1.1 -T4 | Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network |
| -T5 | nmap 192.168.1.1 -T5 | Insane (5) speeds scan; assumes you are on an extraordinarily fast network |

## ****Timing and Performance Switches****

| **WITCH** | **EXAMPLE INPUT** | **DESCRIPTION** |
| --- | --- | --- |
| -host-timeout <time> | 1s; 4m; 2h | Give up on target after this long |
| -min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time> | 1s; 4m; 2h | Specifies probe round trip time |
| -min-hostgroup/max-hostgroup <size<size> | 50; 1024 | Parallel host scan group sizes |
| -min-parallelism/max-parallelism <numprobes> | 10; 1 | Probe parallelization |
| -max-retries <tries> | 3 | Specify the maximum number of port scan probe retransmissions |
| -min-rate <number> | 100 | Send packets no slower than <number> per second |
| -max-rate <number> | 100 | Send packets no faster than <number> per second |

## ****NSE Scripts****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** | |
| --- | --- | --- | --- |
| -sC | nmap 192.168.1.1 -sC | | Scan with default NSE scripts. Considered useful for discovery and safe |
| -script default | nmap 192.168.1.1 -script default | | Scan with default NSE scripts. Considered useful for discovery and safe |
| -script | nmap 192.168.1.1 -script=banner | | Scan with a single script. Example banner |
| -script | nmap 192.168.1.1 -script=http\* | | Scan with a wildcard. Example http |
| -script | nmap 192.168.1.1 -script=http,banner | | Scan with two scripts. Example http and banner |
| -script | nmap 192.168.1.1 -script "not intrusive" | | Scan default, but remove intrusive scripts |
| -script-args | nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.1 | | NSE script with arguments |

## ****Useful NSE Script Examples****

| **COMMAND** | **DESCRIPTION** |
| --- | --- |
| nmap -Pn -script=http-sitemap-generator scanme.nmap.org | http site map generator |
| nmap -n -Pn -p 80 -open -sV -vvv -script banner,http-title -iR 1000 | Fast search for random web servers |
| nmap -Pn -script=dns-brute domain.com | Brute forces DNS hostnames guessing subdomains |
| nmap -n -Pn -vv -O -sV -script smb-enum\*,smb-ls,smb-mbenum,smb-os-discovery,smb-s\*,smb-vuln\*,smbv2\* -vv 192.168.1.1 | Safe SMB scripts to run |
| nmap -script whois\* domain.com | Whois query |
| nmap -p80 -script http-unsafe-output-escaping scanme.nmap.org | Detect cross site scripting vulnerabilities |
| nmap -p80 -script http-sql-injection scanme.nmap.org | Check for SQL injections |

## ****Firewall / IDS Evasion and Spoofing****

| **SWITCH** | **EXAMPLE** | **DESCRIPTION** |
| --- | --- | --- |
| -f | nmap 192.168.1.1 -f | Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters |
| -mtu | nmap 192.168.1.1 -mtu 32 | Set your own offset size |
| -D | nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1 | Send scans from spoofed IPs |
| -D | nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip | Above example explained |
| -S | nmap -S www.microsoft.com www.facebook.com | Scan Facebook from Microsoft (-e eth0 -Pn may be required) |
| -g | nmap -g 53 192.168.1.1 | Use given source port number |
| -proxies | nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1 | Relay connections through HTTP/SOCKS4 proxies |
| -data-length | nmap -data-length 200 192.168.1.1 | Appends random data to sent packets |