# Nmap Cheat Sheet

by xoulea via cheatography.com/198356/cs/41960/

## Basic Scanning Techiniques

| Nmap Query | Nmap Command |
|---|---|
| Scan a single target | nmap [target] |
| Scan multiple targets | nmap [target1,target-2,etc] |
| Scan a list of targets | nmap -iL [list.txt] |
| Scan a range of hosts | nmap [range of IP addresses] |
| Scan an entire subnet | nmap [IP address/cdir] |
| Scan random hosts | nmap -iR [number] |
| Excluding targets from a scan | nmap [targets] –exclude [targets] |
| Excluding targets using a list | nmap [targets] –excludefile [list.txt] |
| Perform an aggressive scan | nmap -A [target] |
| Scan an IPv6 target | nmap -6 [target] |

## Version Detection

| Nmap Query | Nmap Command |
|---|---|
| Operating system detection | nmap -O [target] |
| Attempt to guess an unknown | nmap -O –osscan-guess [target] |
| Service version detection | nmap -sV [target] |
| Troubleshooting version scans | nmap -sV –version--trace [target] |
| Perform a RPC scan | nmap -sR [target] |

## Discover Options

| Nmap Query | Nmap Command |
|---|---|
| Perform a ping scan only | nmap -sP [target] |
| Don’t ping | nmap -PN [target] |

## Discover Options (cont)

| | |
|---|---|
| TCP SYN Ping | nmap -PS [target] |
| TCP ACK ping | nmap -PA [target] |
| UDP ping | nmap -PU [target] |
| SCTP Init Ping | nmap -PY [target] |
| ICMP echo ping | nmap -PE [target] |
| ICMP Timestamp ping | nmap -PP [target] |
| ICMP address mask ping | nmap -PM [target] |
| IP protocol ping | nmap -PO [target] |
| ARP ping | nmap -PR [target] |
| Traceroute | nmap –traceroute [target] |
| Force reverse DNS resolution | nmap -R [target] |
| Disable reverse DNS resolution | nmap -n [target] |
| Alternative DNS lookup | nmap –system-dns [target] |
| Manually specify DNS servers | nmap –dns-servers [servers] [target] |
| Create a host list | nmap -sL [targets] |

## Scripting Engine

| Nmap Query | Nmap Command |
|---|---|
| Execute individual scripts | nmap –script [script.nse] [target] |
| Execute multiple scripts | nmap –script [expression] [target] |
| Execute scripts by category | nmap –script [cat] [target] |
| Execute multiple scripts categories | nmap –script [cat1,-cat2, etc] |
| Troubleshoot scripts | nmap –script [script] –script-trace [target] |

## Scripting Engine (cont)

| | |
|---|---|
| Update the script database | nmap –script-updatedb |

## Firewall Evasion Techniques

| Nmap Query | Nmap Command |
|---|---|
| Fragment packets | nmap -f [target] |
| Specify a specific MTU | nmap –mtu [MTU] [target] |
| Use a decoy | nmap -D RND: [number] [target] |
| Idle zombie scan | nmap -sI [zombie] [target] |
| Manually specify a source port | nmap –source-port [port] [target] |
| Append random data | nmap –data-length [size] [target] |
| Randomize target scan order | nmap –randomize-hosts [target] |
| Spoof MAC Address | nmap –spoof-mac [MAC\|0\|vendor] [target] |
| Send bad checksums | nmap –badsum [target] |

## Output Options

| Nmap Query | Nmap Command |
|---|---|
| Save output to a text file | nmap -oN [scan.txt] [target] |
| Save output to a xml file | nmap -oX [scan.xml] [target] |
| Grepable output | nmap -oG [scan.txt] [target] |
| Output all supported file types | nmap -oA [path/filename] [target] |
| Periodically display statistics | nmap –stats-every [time] [target] |
| 133t output | nmap -oS [scan.txt] [target] |

By **xoulea**
cheatography.com/xoulea/

Published 5th January, 2024.
Last updated 5th January, 2024.


Sponsored by **Readable.com**
Measure your website readability!
https://readable.com