



# nmap Cheat Sheet

Built by Yuval (tistf) Nativ from [See-Security's Hacking Defined Experts](#) program  
This nmap cheat sheet is uniting a few other cheat sheets

## Basic Scanning Techniques

---

- |                                  |  |
|----------------------------------|--|
| • Scan a single target           | <code>nmap [target]</code>                           |
| • Scan multiple targets          | <code>nmap [target1,target2,etc]</code>              |
| • Scan a list of targets         | <code>nmap -iL [list.txt]</code>                     |
| • Scan a range of hosts          | <code>nmap [range of IP addresses]</code>            |
| • Scan an entire subnet          | <code>nmap [IP address/cdir]</code>                  |
| • Scan random hosts              | <code>nmap -iR [number]</code>                       |
| • Excluding targets from a scan  | <code>nmap [targets] --exclude [targets]</code>      |
| • Excluding targets using a list | <code>nmap [targets] --excludefile [list.txt]</code> |
| • Perform an aggressive scan     | <code>nmap -A [target]</code>                        |
| • Scan an IPv6 target            | <code>nmap -6 [target]</code>                        |

## Discovery Options

---

- |                                  |  |
|----------------------------------|--|
| • Perform a ping scan only       | <code>nmap -sP [target]</code>                     |
| • Don't ping                     | <code>nmap -PN [target]</code>                     |
| • TCP SYN Ping                   | <code>nmap -PS [target]</code>                     |
| • TCP ACK ping                   | <code>nmap -PA [target]</code>                     |
| • UDP ping                       | <code>nmap -PU [target]</code>                     |
| • SCTP Init Ping                 | <code>nmap -PY [target]</code>                     |
| • ICMP echo ping                 | <code>nmap -PE [target]</code>                     |
| • ICMP Timestamp ping            | <code>nmap -PP [target]</code>                     |
| • ICMP address mask ping         | <code>nmap -PM [target]</code>                     |
| • IP protocol ping               | <code>nmap -PO [target]</code>                     |
| • ARP ping                       | <code>nmap -PR [target]</code>                     |
| • Traceroute                     | <code>nmap --traceroute [target]</code>            |
| • Force reverse DNS resolution   | <code>nmap -R [target]</code>                      |
| • Disable reverse DNS resolution | <code>nmap -n [target]</code>                      |
| • Alternative DNS lookup         | <code>nmap --system-dns [target]</code>            |
| • Manually specify DNS servers   | <code>nmap --dns-servers [servers] [target]</code> |
| • Create a host list             | <code>nmap -sL [targets]</code>                    |



## Firewall Evasion Techniques

---

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

## Version Detection

---

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

## Output Options

---

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

## Ndiff

---

- Comparison using Ndiff
  - Ndiff verbose mode
  - XML output mode
- ```
ndiff [scan1.xml] [scan2.xml]
ndiff -v [scan1.xml] [scan2.xml]
ndiff -xml [scan1.xml] [scan2.xml]
```



## Nmap Scripting Engine

---

- |                                       |   |
|---------------------------------------|---|
| • Execute individual scripts          | <code>nmap -script [script.nse] [target]</code>           |
| • Execute multiple scripts            | <code>nmap -script [expression] [target]</code>           |
| • Execute scripts by category         | <code>nmap -script [cat] [target]</code>                  |
| • Execute multiple scripts categories | <code>nmap -script [cat1,cat2, etc]</code>                |
| • Troubleshoot scripts                | <code>nmap -script [script] -script-trace [target]</code> |
| • Update the script database          | <code>nmap -script-updatedb</code>                        |
| • Script categories                   |   |
| ◦ all                                 |   |
| ◦ auth                                |   |
| ◦ default                             |   |
| ◦ discovery                           |   |
| ◦ external                            |   |
| ◦ intrusive                           |   |
| ◦ malware                             |   |
| ◦ safe                                |   |
| ◦ vuln                                |   |

## References

---

- [See-Security's main page](#)
- [Hacking Defined.org](#)
- [See-Security's Facebook Page](#)
- [nmap Professional Discovery Guide](#)
- [nmap's Official Web Page](#)