



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

Version Detection

- | | |
|---------------------------------|---|
| • Operating system detection | <code>nmap -O [target]</code> |
| • Attempt to guess an unknown | <code>nmap -O -osscan-guess [target]</code> |
| • Service version detection | <code>nmap -sV [target]</code> |
| • Troubleshooting version scans | <code>nmap -sV -version-trace [target]</code> |
| • Perform a RPC scan | <code>nmap -sR [target]</code> |

Output Options

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

Ndiff

- | | |
|--------------------------|---|
| • Comparison using Ndiff | <code>ndiff [scan1.xml] [scan2.xml]</code> |
| • Ndiff verbose mode | <code>ndiff -v [scan1.xml] [scan2.xml]</code> |
| • XML output mode | <code>ndiff -xml [scan1.xml] [scan2.xml]</code> |