NMAP QUICK REFERENCE CARD

`nmap [scan-types] [opts] <ip> [spec]`

Port Specification

`nmap -p 80 10.20.4.2` ..... Port specific
`nmap -p 23-100 10.20.4.2` ..... Port range
`nmap -pU:110,T:23 10.20.4.2` ... UDP/TCP Specific
`nmap -p- 10.20.4.2` ..... All ports
`nmap -smtp,https 10.20.4.2` ..... Protocol specific
`nmap -F 10.20.4.2` ..... Fast, for speed up
`nmap -p "*" ftp 10.20.4.2` ..... Using name
`nmap -r ftp 10.20.4.2` ..... Sequential

Host `/10.20.4.1` *Discovery*

`nmap 10.20.4.1 -sL` ..... List without scanning
`nmap 10.20.4.1/8 -sn` ..... Disable port scanning
`nmap 10.20.4.1-8 -Pn` ..... Port scan only
`nmap 10.20.4.12 -PS22-25,80` .... `TCP-SYN` discovery
`nmap 10.20.4.12 -PA22-25,80` .... `TCP-ACK` discovery
`nmap 10.20.4.1-8 -PU53` ..... `UDP` discovery
`nmap 10.20.4.1/8 -PR` ..... `ARP` discovery (local)
`nmap 10.20.4.1 -n` ..... no `DNS` resolution

Version Detection

`nmap 10.20.4.1 -sV` ..... Try detect version of service
`nmap...-sV --version-intensity 6` ... Intensity 0-9
`nmap...-sV --version-all` ..... Intensity 9
`nmap...-sV --version-light` ..... Enable light mode
`nmap...-sV --version-trace` ..... Trace version scan
`nmap 10.20.4.1 -sV` ..... RPC scan
`nmap 10.20.4.1 -A` .. OS/Vers Detection + Scriptscan
`nmap 10.20.4.1 -O` ..... Remote OS detection

Firewall Proofing

`nmap -f 1.2.4.1` ..... Scan fragment packets
`nmap -mtu [MTU] 1.2.4.1` ..... Specify MTU
`nmap -D RND: <num> 10.20.4.1` ..... Use a decoy
`nmap -sI [zombie] 1.2.4.1` ..... Scan idle zombie
`nmap --source-port 33220...` ... Manual source port
`nmap --data-length 64...` .... Random append data
`nmap --randomize-hosts 1.2.4.1` Scan order random
`nmap --spoof-mac [MAC]...` ..... Scan order random
`nmap --badsum` ..... Bad checksum

Scan Types

`nmap 10.20.4.1 -sS` ..... `TCP-SYN` port scan
`nmap 10.20.4.1 -sT` ..... `TCP-CONNECT` port scan
`nmap 10.20.4.1 -sA` ..... `TCP-ACK` port scan
`nmap 10.20.4.1 -sU` ..... `UDP` port scan
`nmap -Sf 10.20.4.1` ..... `TCP-FIN` scan
`nmap -SX 10.20.4.1` ..... `XMAS` scan
`nmap -Sp 10.20.4.1` ..... Ping scan
`nmap -Su 10.20.4.1` ..... `UDP` scan
`nmap -Sa 10.20.4.1` ..... `TCP-ACK` scan
`nmap -Sl 10.20.4.1` ..... List scan

Timing Options

`nmap -T0 10.20.4.1` ..... Slowest scan
`nmap -T1 10.20.4.1` ..... Avoid IDS scan
`nmap -T2 10.20.4.1` ..... Timely scan
`nmap -T3 10.20.4.1` ..... Default scan
`nmap -T4 10.20.4.1` ..... Aggressive scan
`nmap -T5 10.20.4.1` ..... Very aggressive scan

Output

`nmap -oN scan.txt 10.20.4.2` ..... Text file
`nmap -oX scan.xml 10.20.4.2` ..... XML file
`nmap -oG scan.txt 10.20.4.2` ..... Grepable text file
`nmap -oA scan.txt 10.20.4.2` ..... All file types
`nmap --stats-every [time] 10.20.4.2` ... Statistics

Scan Options

`nmap -sP 10.20.4.1` ..... Ping scan only
`nmap -PN 10.20.4.1` ..... No ping scan
`nmap -PS 10.20.4.1` ..... `TCP-SYN` scan
`nmap -PA 10.20.4.1` ..... `TCP-ACK` scan
`nmap -PU 10.20.4.1` ..... `UDP` ping scan
`nmap -PY 10.20.4.1` ..... `SCTP` scan
`nmap -PE 10.20.4.1` ..... `ICMP` echo ping
`nmap -PP 10.20.4.1` ..... `ICMP` timestamp ping
`nmap -PM 10.20.4.1` ..... `ICMP` address mask ping
`nmap -PO 10.20.4.1` ..... `IP` protocol ping
`nmap -PR 10.20.4.1` ..... `ARP` ping
`nmap -traceroute 10.20.4.1` ..... Traceroute
`nmap -R 10.20.4.1` ..... Force reverse `DNS` resolution
`nmap -n 10.20.4.1` .... Disable reverse `DNS` resolution
`nmap -system-dns 10.20.4.1` .. Alternate `DNS` lookup
`nmap -dns-servers <server> 10.20.4.1` Manual `DNS`
`nmap -sL 10.20.4.1-10` ..... Create host list

Scripts NSE

`nmap --script "test" 10.20.4.0/8` ..... Exec script
`nmap --script-updatedb` ..... Add new scripts
`nmap -sV -sC` ..... Use safe default scripts
`nmap -script-help "test"` ..... Get help on script

Misc Commands

`nmap -6` ..... `IPv6` targets
`nmap --proxies <URL>:<port>,` .... Run with proxies
`nmap --open` ..... Show only open ports

`10.20.4.1` *Specification*

`nmap 10.20.4.1` ..... Single `IP` scan
`nmap 10.20.4.1 10.20.5.3` ..... Specific `IP`s scan
`nmap 10.20.4.1-254` ..... Range `IP` scan
`nmap xyz.org` ..... Domain scan
`nmap 10.20.4.0/8` ..... CIDR notation scan
`nmap -iL scan.txt` ..... Scan from file
`nmap --exclude 10.20.4.1` ..... Exclude from scan