# NMap Commands KungFu

OffensiveCI@Prawez Samani

## 1 Ping Options

- -PE/-PI (ICMP Echo Request Ping)
- -PN/-PD/-P0 (Don't Ping)
- -PS (TCP SYN Ping)
- -PU (UDP Ping)
- -PY (SCTP Ping)
- -PO (IP Protocol Ping)
- -PP (ICMP Timestamp Ping)
- -PM (ICMP Address Mask Ping)
- -R (Require Reverse)
- -n (Disable Reverse DNS)
- --dns-servers (Specify DNS Servers)

## 2 OS Detection

- -O (OS Fingerprinting)
- -A (Aggressive, Additional & Advanced Detection) — Guess OS More Aggressively
- --osscan-limit (Limit System Scanning)
- --osscan-guess, --fuzzy (More Guessing Flexibility)

## 3 Version Detection

- -sV (Version Scan)
- --allports (Don"t Exclude Any Ports)
- --version-intensity <Level> (Set Version Intensity) — Set from 0 (light) to 9 (Try all Probes)
- --version-light (Enable Version Scanning Light)
- --version-all (Enable Version Scan All)
- --version-trace (For Debugging) — Show Detailed Version Scan Activity — Version Trace

## 4 Scan Techniques

- -sS (TCP SYN Scan) — Half Open Scan | Stealth Scan
- -sT (TCP Connect() Scan) — Vanila Scan
- -sA (ACK Scan)
- -sW (Window Scan)
- -sM (Uriel/Maimon Scan)
- -sU (UDP Scan)
- -sN (Null Scan), -sF (FIN Scan), -sX (Xmas Tree Scan) — Stealth Scan
- --scanflags <Flags> (Customize TCP Scan Flags)
- -sP (Ping Scan)
- -sO (IP Protocol Scan)
- -sR (RPC Scan) — Remote Procedure Call
- -sP (Ping Scan)
- -sn (Ping Scan) — Disable Port Scan
- -sL (List Scan) — Simply List Targets To Scan
- -sI (Idle Scan) — Zombie Scan
- -b (FTP Bounce Attack)
- -sY (SCTP Init Scan)
- -sZ (Cookie-Echo Scans)

## 5 Host & Port Options

- --exclude (Exclude Target) — Exclude Hosts/Networks
- --excludefile (Exclude Target File)
- -iR (Random Target)
- --randomize_hosts/-rH (Randomize Hosts)
- -iL (Read Target from File) — Input From List of Hosts/Networks (Manual Scanning)
- -Pn (Treat All Hosts As Online) — Skip Host Discovery
- --system-dns (Use OS's DNS Resolver)
- --traceroute (Trace Hop Path To Each Host)
- -p <Port Range> (Only Scan Specified Ports)
- -F (Fast Scan) — Scan Fewer Ports Than The Default Scan
- -r (Scan Ports Consecutively) — Don't Randomize
- --top-ports (Scan Most Common Ports)
- --port-ratio (Scan ports more common than ratio)

## 6 Firewall/IDS Evasion and Spoofing

Timing, Tunning & Performance Options

- -f/-ff (Use Fragmented IP Packets)
- --mtu <databytes>(Maximum Transmission Unit)
- --ttl <value> (Time To Live)
- Cloak A Scan With Decoys — -D <decoy1,decoy2[,ME],...> (Create Decoys)
- Spoof Source Address — -S <IP_Address> (Source Address)
- Use Specified Interface — -e <iface> (Interface)
- Use Given Port Number — -g/--source-port (Source Port Scan)
- --proxies <url1,[url2],...>(Relay Connections Through HTTP/SOCKS4 Proxies)
- Append Random Data to Sent Packets — --data-length <databytes> (Data Length)
- MAC Spoofing — --spoof-mac <mac address/prefix/vendor name>
- Send Packets With a Bogus TCP/UDP/SCTP Checksum — --badsum (Bogus Packet)
- Host Timeout — --host-timeout <milliseconds>
- Specifies Probe Round Trip Time
  - --initial-rtt-timeout <milliseconds> (Initial Round Trip Timeout)
  - --min-rtt-timeout <milliseconds> (Minimum Round Trip Timeout)
  - --max-rtt-timeout <milliseconds> (Maximum Round Trip Timeout)
- Parallel Host Scan Group Sizes
  - --max-hostgroup <number> (Maximum Parallel Hosts per Scan)
  - --min-hostgroup <number> (Minimum Parallel Hosts per Scan)
- Probe Parallelization
  - --max-parallelism <number> (Maximum Parallel Port Scans)
  - --min-parallelism <number> (Minimum Parallel Port Scans)
- Delay Time Between Probes
  - --scan-delay <milliseconds> (Minimum Delay Between Probes)
  - --max-scan-delay <milliseconds> (Maximum Delay Between Probes)
- Paranoid (T0) | Sneaky (T1) | Polite (T2) | Normal (T3) | Aggressive (T4) | Insane (T5) — --timing/-T<0 | 1 | 2 | 3 | 4 | 5> (Timing Policies)
- Send Packets No Slower Than <Number> Per Second — --min-rate <number> (Minimum Slower Packet Send)
- Send Packets No Faster Than <Number> Per Second — --max-rate <number> (Maximum Faster Packet Send)

## 7 Run Time Interaction & Reporting Options

- Verbose Mode — -v/--verbose/-vv (Increase Verbosity Level)
- Debug Mode — -d/--debug/-dd (Increase Debugging Level)
- --interactive (Interactive Mode)
- --noninteractive (Noninteractive Mode)
- Display The Reason a Port is in a Particular State — --reason (Port Reason)
- Only Show Open (or Possibly Open) Ports — --open (Open Port)
- Packet Trace — Show All Packets Sent and Received — --packet-trace (Packet Status)
- Print Host Interfaces and Routes (For Debugging) — -iflist (List Interfaces)
- Log Errors/Warnings To The Normal-Format Output File — --log-errors (Logs Status)
- --append-output (Append Outputs)
- Resume An Aborted Scan — --resume <logfilename> (Resume Scan)
- XSL Style Sheet To Transform XML Output To HTML — --stylesheet <path/URL> (Style Sheet)
- Reference Style Sheet From Nmap.Org For More Portable XML — --webxml (Reference Style Sheet)
- Prevent Associating Of XSL Style Sheet w/XML Output — --no-stylesheet (No Style Sheet)
- Output In The Three Major Formats At Once — -oA (All Format)
- -oN <logfilename> (Normal Format)
- -oX <logfilename> (XML Format)
- -oG <logfilename> (Grepable Format)
- -oS <logfilename> (Script Kiddie Format)

## 8 Scripts & Miscellaneous Options

- -sC/--script <Lua Script> (Using Script)
- --script-args <n1=v1,[n2=v2,...]> (Script Argument)
- --script-args-file=filename (Script Argument Into File)
- Show All Data Sent and Received — --script-trace (Data Status)
- --script-updatedb (Update Script Database)
- --script-help <Lua Script> (Show About Script)
- -h/--help (Quick Reference Screen)
- -V/--version (Nmap Version)
- --datadir <directory_name> (Data Directory)
- -q (Quash Argument Vector)
- -6 (IPv6 Support)
- --privileged (Fully Privileged)
- --unprivileged (Lacks Raw Socket Privileged)
- --send-eth/--send-ip (Send Using Raw Ethernet Frames Or IP Packets)