NMap KungFu

©Prawez Samani

Firewall/IDS Evasion and Spoofing

- Maximum Fragmentation (8 & 16 byte) — -f/-ff (Use Fragmented IP Packets)
- Maximum Fragmentation (8 & 16 byte) — --mtu <databytes>(Maximum Transmission Unit)
- Cloak A Scan With Decoys — -D <decoy1,decoy2[,ME],...> (Create Decoys)
- Spoof Source Address — -S <IP_Address> (Source Address)
- Use Specified Interface — -e <iface> (Packet Interface)
- Use Given Port Number — -g/--source-port (Source Port Scan)
- Append custom binary data to sent packets — --data (Custom Binary Data)
- Append custom binary data to sent packets — --data-string (Custom String Data)
- Append Random Data to Sent Packets — --data-length <databytes> (Random Data Length)
- Send packets with specified ip options — --ip-options (Specify IP Option)
- --ttl <value> (Time To Live)
- 2,048 hosts at a time are randomly chosen — --randomize_hosts/-rH (Randomize Hosts)
- --spoof-mac <mac address/prefix/vendor name> (MAC Spoofing)
- Relay Connections Through HTTP/SOCKS4 Proxies — --proxies <url1,[url2],...>(Chain Of Proxies)
- Send Packets With a Bogus TCP/UDP/SCTP Checksum — --badsum (Bogus Packet)

Timing and Performance Tuning Options

- Parallel Host Scan Group Sizes
  - Default Group Size 5 >>> 1024 — --min-hostgroup <numbers> (Min Parallel Hosts Per Scan)
  - Common Choice is 256 — --max-hostgroup <numbers> (Max Parallel Hosts Per Scan)
- Probe Parallelization
  - Default Based On Network Performance — --min-parallelism <numprobes> (Mini Parallel Probe)
  - 10 Might Be Reasonable — --max-parallelism <numprobes> (Max Parallel Probe)
- Specifies Probe Round Trip Time
  - 100ms Reasonable Aggressive — --initial-rtt-timeout <milliseconds> (Initial Probe Round Trip Timeout)
  - Rarely Used Option — --min-rtt-timeout <milliseconds> (Mini Probe Round Trip Timeout)
  - Nor Exceed 1000ms — --max-rtt-timeout <milliseconds> (Max Probe Round Trip Timeout)
- 3 Reasonable, 0 to prevent any retransmissions
- Default -T Profile 10
  - --max-retries <numtries> (Maxi Ports Probe Retransmissions)
- Max Amount of Time You Are Willing To Wait — --host-timeout <milliseconds> (Slow Hosts Timeout)
- Exceeds Time Will Be Terminated & No Output — --script-timeout (Slow Scripts Timeout)
- Delay Time Between Probes
  - Evade Threshold Based (IDS/IPS) — --scan-delay <milliseconds> (Mini Delay Between Probes)
  - Too Low Can Lead To Wasteful Packet Retransmissions & Possible Missed Ports — --max-scan-delay <milliseconds> (Maxi Delay Between Probes)
- Send Packets No Slower Than <Number> Per Second — --min-rate <number> (Mini Slower Packet Send)
- Send Packets No Faster Than <Number> Per Second — --max-rate <number> (Max Faster Packet Send)
- Reduce Accuracy, Useful When You Only Care About Open Ports — --defeat-rst-ratelimit (Ignore RST Packets Rate Limits)
- Chance For Inaccuracy Is Greater — --defeat-icmp-ratelimit (Ignore ICMP error messages Rate Limits)
- select(2)-Based Fallback Engine is Guaranteed To Be Available — --nsock-engine epoll | kqueue | poll | select (Use nsock IO Multiplexing Engine)
- Paranoid (T0) | Sneaky (T1) | Polite (T2) | Normal (T3) | Aggressive (T4) | Insane (T5)
- -T0 and -T1 May Be Useful For Avoiding IDS Alerts
  - --timing/-T<0 | 1 | 2 | 3 | 4 | 5> (Timing Template)
- Please Refer The Timing Templates & Their Effects Table

Scripting Engine Options (NSE)

- -sC Is Equivalent To --script=default — -sC/--script <Lua Script> (Using Script)
- --script-args <n1=v1,[n2=v2,...]> (Script Argument)
- --script-args-file=filename (Script Argument Into File)
- --datadir <directory_name> (Custom Data Directory)
- Show All Data Sent and Received By Script
- Subset of --packet-trace, Specifying That Enables Script Tracing Too
  - --script-trace (Data Status)
- --script-updatedb (Update Script Database)
- --script-help <Lua Script> (Show Help About Script)

Run Time Interaction & Reporting Options

- Output In The Three Major Formats At Once — -oA (All Format)
- -oN <filename> (Normal Format)
- -oX <filename> (XML Format)
- -oS <filename> (Script Kiddie Format)
- -oG <filename> (Grepable Format)
- Verbosity & Debugging
  - Verbose Mode — -v/-vv/-v3/--verbose (Increase Verbosity Level)
  - Debug Mode — -d/-dd/-d9/--debug (Increase Debugging Level)
  - Displays The Packet That Determined A Port Or Hosts State — --reason (Host & Port State Reason)
  - Only Show Open (or Possibly Open) Ports — --open (Open Port)
  - Prints A Timing Status Message After Each Interval — --stats-every <time> (Print Periodic Timing Stats)
  - Print A Summary Of Every Packet Sent Or Received (Include All 3 Trace) — --packet-trace (Packet Status)
  - Print Host Interfaces and Routes (For Debugging) — -iflist (List Interfaces)
- --append-output (Append Outputs In Files)
- Append New Results In The Data Files If Scan Were Interrupted — --resume <filename> (Resume An Aborted Scan)
- XSL Style Sheet To Transform XML Output To HTML — --stylesheet <path/URL> (Style Sheet)
- Convenience Option, Reference Style Sheet From Nmap.Org — --webxml (Reference Style Sheet)
- Prevent Associating Of XSL Style Sheet w/XML Output — --no-stylesheet (No Style Sheet)
- Log Errors/Warnings To The Normal-Format Output File — --log-errors (Logs Status)
- --noninteractive (Noninteractive Mode)

Miscellaneous Options

- -6 (IPv6 Support)
- --servicedb <services file>
- --versiondb <service probes file>
- --send-eth/--send-ip (Send Using Raw Ethernet Frames Or IP Packets)
- --privileged (Fully Privileged)
- --unprivileged (Lacks Raw Socket Privileged)
- Useful For Memory-Leak Debugging — --release-memory (Release Memory Before Quitting)
- -V/--version (Nmap Version)
- -h/--help (Quick Reference Screen)
- Modify Its Argument Vector To Appear As Another Process — -q (Quash Argument Vector)

Discovery Options

- -sL (List Scan) — Simply List Targets To Scan
- -sn (Ping Scan) — Disable Port Scan
- -Pn/-P0/-PD/-PN (Don't Ping) — Treat all hosts as online - skip host discovery
- -PS (TCP SYN Ping)
- -PA/-PT (TCP ACK Ping)
- -PU (UDP Ping)
- -PY (SCTP Ping)
- -PE/-PI (ICMP Echo Request Ping) — ICMP Type 8 — Expecting a type 0 (Echo reply)
- -PP (ICMP Timestamp Ping) — ICMP Type 13 — Expecting a type 14 (Timestamp reply)
- -PM (ICMP Address Mask Ping) — ICMP Type 17 — Expecting a type 18 (Address Mask reply)
- -PO (IP Protocol Ping) — DEFAULT_PROTO_PROBE_PORT_SPEC - ICMP (proto 1), IGMP (proto 2), and IP-in-IP (proto 4)
- --disable-arp-ping (No ARP or ND Ping)
- --discovery-ignore-rst — Ignore RST replies in case firewalls may spoof TCP reset (RST) replies
- --traceroute (Trace Path To Host)
- -n (No DNS Resolution)
- -R (DNS Resolution)
- --resolve-all (Scan Each Resolved Address)
- --system-dns (System DNS Resolver)
- --dns-servers (Specify DNS Servers)

OS Detection

- -O (OS Fingerprinting)
- --osscan-limit (Limit System Scanning)
- --osscan-guess, --fuzzy (Guess OS More Aggressively)
- --max-os-tries (Max OS Detection Tries) — Default 5 Times
- -A (Aggressive, Additional & Advanced Detection)
  - Guess OS More Aggressively
  - Enable OS Detection, Version Detection, Script Scanning, and Traceroute

Version Detection

- -sV/-sR (Version Detection)
- --allports (Don't Exclude Any Ports)
- --version-intensity <Level> (Set Version Intensity) — Set from 0 to 9 (Try all Probes) — Default is 7
- --version-light (Enable Light Mode Probe) — Default is 2
- --version-all (Enable All Mode Probe) — Default is 9
- --version-trace (Extensive Debugging) — Show Version Detection Detailed Scan Activity — Version Trace: Subset of --packet-trace

Scan Techniques

- -sS (TCP SYN Scan) — Half Open Scan | Stealth Scan
  - SYN/ACK - Open
  - RST - Closed
- -sT (TCP Connect() Scan) — Vanila Scan
  - SYN/ACK - Open
  - RST - Closed
- -sA (ACK Scan) — ACK flag
  - RST - Unfiltered
  - No Response+ICMP Error - Filtered
- -sW (Window Scan) — ACK flag & check Window size
  - RST+WIN=4096 - Open
  - RST+WIN=0 - Closed
- -sM (Uriel/Maimon Scan) — FIN/ACK flags
  - RST - Open
  - No Response - Closed
- -sU (UDP Scan)
  - UDP Data - Open
  - No Response - Open | Filtered
  - ICMP Port Unreachable - Closed
- -sY (SCTP Init Scan)
- -sN (Null Scan) — 0 flags
- -sF (FIN Scan) — F flag
- -sX (Xmas Scan) — F/P/U flags
  - Stealth Scan
    - No Response - Open
    - RST - Closed
- --scanflags <Flags> (Customize TCP Flags Scan)
- -sZ (Cookie-Echo Scans)
- -sI (Idle Scan) — Zombie Scan
- -sO (IP Protocol Scan)
- -b (FTP Bounce Attack)
- -sP (Ping Scan) — Quickest Scan: No Actual Ports Are Queried

Host & Port Orders

- -iL (Read Target from File) — Input From List of Hosts/Networks (Manual Scanning)
- -iR (Random Target)
- --exclude (Exclude Target) — Exclude Hosts/Networks
- --excludefile (Exclude Target File)
- -p <Port Range> (Only Scan Specified Ports)
- --exclude-ports (Exclude Specified Ports)
- -F (Fast Scan) — Limited ports - 100 — "nmap-services" file need to be modify with 100 ports
- -r (Scan Ports Consecutively) — Don't Randomize
- --port-ratio (Scan ports more common than ratio)
- --top-ports (Scan Most Common Ports)