Network Scanning Tools Cheatsheet

A comprehensive guide to network scanning tools, their functionalities, and common usage scenarios. This cheat sheet covers essential commands, options, and techniques for network reconnaissance and security auditing.

Nmap Basics

Nmap Scan Types

`TCP Connect Scan (-sT)`	Establishes a full TCP connection. Requires no special privileges.
`SYN Scan (-sS)`	Half-open scan; sends SYN packets, less likely to be logged. Requires root privileges.
`UDP Scan (-sU)`	Sends UDP packets to the target. Can be slow and unreliable due to UDP's nature.
`FIN Scan (-sF)`	Sends a FIN packet. Stealthier than SYN scan, but may not work on all systems.
`Xmas Scan (-sX)`	Sends a FIN, PSH, and URG packet. Similar to FIN scan in stealth.
`Null Scan (-sN)`	Sends a packet with no flags set. Stealthiest, but least reliable.

Target Specification

- `nmap <target>` - Scan a single target.
- `nmap <target1> <target2> <target3>` - Scan multiple targets.
- `nmap <target1,target2,target3>` - Scan multiple targets with comma separated values.
- `nmap <network>/<CIDR>` - Scan an entire subnet. Example: `nmap 192.168.1.0/24`.
- `nmap -iL <input_file>` - Scan targets listed in a file.
- `nmap -p <port ranges> <target>` - Scan specific port or range. Example: `nmap -p 22,80,443 192.168.1.1` or `nmap -p 1-1000 192.168.1.1`.

Common Nmap Options

`-v`	Verbose mode; increases the level of detail.
`-A`	Aggressive scan; enables OS detection, version detection, script scanning, and traceroute.
`-T<0-5>`	Timing template; sets the scan speed (0 is slowest, 5 is fastest).
`-p <ports>`	Specifies the ports to scan (e.g., `-p 22,80,443` or `-p 1-1000`).
`-O`	Enables OS detection.
`--script <script>`	Runs NSE scripts for advanced scanning. Example: `--script vuln` to check vulnerabilities.

Nmap Advanced Techniques

Version Detection

- `nmap -sV <target>` - Enables version detection to determine the software version running on open ports.
- `nmap -sV --version-intensity <level> <target>` - Adjust the intensity of version scanning (0-9, default is 7).
- `nmap -sV --version-light <target>` - Use light version scanning.
- `nmap -sV --version-all <target>` - Try every single probe.
- `nmap -sV --version-trace <target>` - Shows detailed version scanning activity.

OS Detection

`nmap -O <target>`	Enables OS detection to attempt to identify the operating system of the target.
`nmap -O --osscan-limit <target>`	Limits OS detection to promising targets. Use when you know at least one open and one closed TCP port.
`nmap -O --osscan-guess <target>`	Guesses the OS more aggressively.
`nmap -O --version-trace <target>`	Shows detailed OS detection activity.

NSE Scripting

- `nmap --script=<script_name> <target>` - Runs a specific NSE script against the target.
- `nmap --script=default <target>` - Runs the default set of NSE scripts.
- `nmap --script=safe <target>` - Runs scripts categorized as safe.
- `nmap --script=vuln <target>` - Runs scripts to check for known vulnerabilities.
- `nmap --script=discovery <target>` - Runs scripts for network discovery.
- `nmap --script=<script_category> <target>` - Runs all scripts within a specific category.
- `nmap --script=<path_to_script> <target>` - Runs a custom script.

Masscan Techniques

Basic Usage

- `masscan <target range> -p <port(s)>` - Scans the specified target range for the given ports.
- Example: `masscan 192.168.0.0/16 -p 80,443`
- `masscan <ip address>` - Scans a single IP address.
- `masscan <ip range>` - Scans an IP range.
- `masscan <network>/<CIDR>` - Scans an entire subnet. Example: `masscan 10.0.0.0/8`.

Rate Limiting

`--rate <pps>`	Sets the packet transmission rate in packets per second (pps).
Example	`masscan 192.168.0.0/16 -p 80 --rate 1000`
Note	A higher rate can lead to faster scans but may also cause network congestion or be blocked by firewalls.

Excluding Targets

- `--excludefile <filename>` - Excludes targets listed in the specified file.
- Example
- Create a file named `exclude.txt`.
- Add IP addresses.
- `masscan 10.0.0.0/8 -p80 --excludefile exclude.txt`

Saving Output

`-oX <filename>`	Saves the output in XML format.
`-oG <filename>`	Saves the output in Grepable format.
`-oJ <filename>`	Saves the output in JSON format.
`-oL <filename>`	Saves the output in list format.

Netdiscover Usage

Interface Selection

`netdiscover -i <interface>` - Specifies the network interface to use for scanning.
Example: `netdiscover -i eth0`
If no interface is specified, Netdiscover attempts to auto-detect one.

Range Specification

`-r <range>`	Defines the IP range to scan. Use CIDR notation for subnets.
Example	`netdiscover -r 192.168.1.0/24`
Note	If no range is specified, Netdiscover scans the entire subnet of the selected interface.

Passive Mode

`-p` - Enables passive mode, which only listens for ARP packets without sending any probes.
In passive mode, Netdiscover relies on network traffic to discover hosts.
Useful in environments where active scanning is not desired or allowed.

Saving and Loading Results

`-s <file>`	Saves the discovered hosts to a file.
`-l <file>`	Loads a list of known hosts from a file to avoid re-scanning.
Example	`netdiscover -r 192.168.1.0/24 -s discovered_hosts.txt`