Nmap Quick Reference Cheat Sheet

Recommended Comprehensive Scan

`nmap -A -p- [target]`
Thorough scan including OS detection, version detection, script scanning, and traceroute on all ports.

What Does It Mean?

- `-p-`
  Scan all ports (1-65535).
- `-A`
  Aggressive scan (OS detection, version detection, script scanning, traceroute).

`-A` Included Flags

- `-O`
  OS detection.
- `--sC`
  Run safe and default NSE scripts.
- `--traceroute`
  Perform traceroute to target.

Include & Exclude Targets

- `--exclude [host1,host2,...]`
  Exclude specific targets from the scan.
- `-iL [filename]`
  Include targets listed in a file.
- `--excludefile [filename]`
  Exclude targets listed in a file (no strikes).

Logging & Output

- `-oN [file].txt`
  Normal text output.
- `-oX [file].xml`
  XML format output.
- `-oG [file].gnmap`
  Greppable format output.
- `-oA [basename]`
  All output formats simultaneously.

Common Options & Flags

- `--open`
  Display only open ports.
- `--resume [filename]`
  Resume an interrupted scan.
- `--top-ports [number]`
  Scan the most common ports.
- `-F`
  Fast scan (--top-ports=100).
- `-Pn`
  Skip host discovery (ping).
- `-sn`
  Only host discovery (ping).
- `-sL`
  Generate list.
  Don't send packets to target.
- `-T0` - `-T5`
  Scan speed settings range from slow, stealthy scans to fast, but less accurate, scans (Default: -T3).

Note: By default, Nmap pings before scanning ports. Use `-Pn` to skip pinging.

Tuning & Performance

- `--min-hostgroup [number]`
  `--max-hostgroup [number]`
  Control parallel host scanning groups.
- `--min-rtt-timeout [time]`
  `--max-rtt-timeout [time]`
  `--initial-rtt-timeout [time]`
  Set round-trip timeout to improve speed.
- `--min-rate [number]`
  `--max-rate [number]`
  Set packet sending rate.
- `--min-parallelism [number]`
  `--max-parallelism [number]`
  Control probe parallelization.
- `--max-retries [number]`
  Cap the number of port scan probe retransmissions.
- `--host-timeout [time]`
  Give up on the target after this time.

Note: Options that take a `<time>` parameter are in seconds, or you can append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g., 30m).

Advanced Techniques & Evasion

- `-sI [zombie_host]`
  Zombie (Idle) Scan: Use a third-party host IP to hide your identity.
- `-D RND:10`
  Decoy scan with 10 random IP addresses to obscure the real scanner.
- `-D decoy1,decoy2,ME`
  Use specific decoy IPs plus your own.
- `--source-port [port]`
  Specify source port (useful for firewall evasion).
- `--randomize-hosts`
  Randomize scan order to avoid detection.
- `-f`
  Fragment packets to evade firewall detection.
- `-R`
  Always reverse DNS look up
- `-n`
  Never reverse DNS look up

Timings (YMMV)

- Nmap algorithmically determines speeds based on many factors.
- Details: Port Scanning Algorithms
- Real world tweaks to increase your scan speeds
  If results seem unusual, adjust the settings.

- `--min-rate=1500`
  Adjust within a range, e.g., 1500 to 5000
- `--max-retries=0`
- `--host-timeout=1s`
- `-T5`
  Adjust within a range, e.g., -T4 to -T5

Generate list of ports

```
PORTS=$(nmap 127.0.0.1 \
--top-ports=100 -oX - | \
grep "," -m 1 | \
cut -d'"' -f8)
```

Useful for other tools like masscan
`masscan -p $PORTS [target]`