Nmap Commands Cheat Sheet

Nmap (Network Mapper) is a powerful open-source tool used for network discovery, security auditing, and vulnerability scanning.
Below are some of the most important Nmap commands with explanations.

- ## Basic Scanning

Scan a single host
`nmap 192.168.1.1`
Scans the target IP for open ports and basic information.

Scan a range of IPs
`nmap 192.168.1.1-50`
Useful for scanning multiple systems in a subnet.

Scan an entire subnet
`nmap 192.168.1.0/24`
Performs a scan on all 254 hosts in a /24 subnet.

- ## Port Scanning

Common ports scan
`nmap --top-ports 20 192.168.1.1`
Scans the 20 most commonly used ports.

Specific port scan
`nmap -p 22,80,443 192.168.1.1`
Checks only SSH, HTTP, and HTTPS.

All 65,535 ports
`nmap -p- 192.168.1.1`
Performs a full port sweep.

- ## Service & Version Detection

Detect services running on ports
`nmap -sV 192.168.1.1`
Identifies the software and version running on open ports.

- ## OS Detection

  Detect Operating System
  `nmap -O 192.168.1.1`
  Attempts to identify the target OS.

  Aggressive scan
  `nmap -A 192.168.1.1`
  Comprehensive fingerprinting of the target (OS, services, traceroute, scripts).

- ## Scan Techniques

  TCP SYN Scan (Stealth)
  `nmap -sS 192.168.1.1`
  The most popular and fast scan doesn't complete TCP handshake.

  TCP Connect Scan
  `nmap -sT 192.168.1.1`
  Completes full TCP connections, noisier but more accurate and effective.

  UDP Scan
  `nmap -sU 192.168.1.1`
  Checks open UDP ports (slower than TCP scans).

- ## NSE Scripts

  Run default scripts
  `nmap -sC 192.168.1.1`
  Uses basic Nmap scripts for common vulnerabilities.

  Vulnerability scan with scripts
  `nmap --script vuln 192.168.1.1`
  Runs vulnerability-related checks.

- ## Output & Reporting

  Save output to file
  `nmap -oN scan_results.txt 192.168.1.1`
  Saves results in a text file.

  Save in all formats
  `nmap -oA full_scan 192.168.1.1`
  Saves in normal, XML, and grepable formats.

- ## Firewall & IDS Evasion

  Fragment packets
  `nmap -f 192.168.1.1`
  Tries to bypass filters using fragmented packets.

  Spoof source IP
  `nmap -S 10.10.10.10 192.168.1.1`
  Spoofs your IP address.

  Decoy scan
  `nmap -D RND:5 192.168.1.1`
  Hides your real IP among random decoys.

  Mastering these Nmap commands allows cybersecurity professionals to perform effective reconnaissance, vulnerability scanning, and penetration testing.