Nmap Cheatsheet

Dr Ayman El Hajjar

School of Computer Science and Engineering, University of Westminster

Host Discovery

Techniques used to identify live hosts on a network. These scans help determine which systems are reachable before deeper enumeration.

- Ping Scan: `nmap -sn <IP>`
- Subnet Sweep: `nmap -sn <network>/24`
- ARP Scan (LAN): `sudo nmap -PR <network>/24`
- Disable DNS: `-n`

Scan Fundamentals

Core Nmap options that control verbosity, speed, and basic scan behaviour. These settings influence how quickly and how thoroughly Nmap probes a target.

- Fast Scan: `nmap -F <IP>`
- Verbose: `nmap -v <IP>`
- Very Verbose: `nmap -vv <IP>`
- Timing Templates: `-T0` to `-T5`

Timing & Performance

Controls how aggressively Nmap sends packets and how long it waits for responses. These options help tune scans for speed or stealth depending on the environment.

- Max Rate: `-max-rate <pps>`
- Min Rate: `-min-rate <pps>`
- Host Timeout: `-host-timeout 30s`
- Disable DNS: `-n`

Port States

Definitions used by Nmap to classify how a target responds to probes. Understanding these states helps interpret scan results accurately.

- open - service accepts connections
- closed - reachable but no service
- filtered - firewall blocks probes
- unfiltered - reachable but state unknown
- open|filtered - ambiguous (UDP/NULL/FIN/Xmas)

Top 10 Useful Flags

A quick reference to the most frequently used Nmap options. These flags appear in most practical scanning workflows.

- `-sS` - SYN scan
- `-sV` - service version detection
- `-O` - OS detection
- `-A` - aggressive scan
- `-p-` - scan all ports
- `-F` - fast scan
- `-T4` - faster timing
- `-sU` - UDP scan
- `-iL` - input list
- `-oA` - all output formats

About Nmap

Nmap is a network scanning and enumeration tool used to identify hosts, services, and operating systems. It supports multiple scan types, performance tuning, and a powerful scripting engine.

TCP Scan Methods

Different TCP-based techniques used to identify open, closed, or filtered ports. Each method interacts with the TCP handshake in a unique way.

- SYN Scan: `nmap -sS <IP>`
- Connect Scan: `nmap -sT <IP>`
- ACK Scan: `nmap -sA <IP>`
- FIN Scan: `nmap -sF <IP>`
- NULL Scan: `nmap -sN <IP>`
- Xmas Scan: `nmap -sX <IP>`

Enumeration Options

Options used to gather detailed information about services, OS, and configurations. These scans help build a deeper understanding of the target.

- OS Detection: `nmap -O <IP>`
- Service Version: `nmap -sV <IP>`
- UDP Scan: `nmap -sU <IP>`
- Default Scripts: `nmap -sC <IP>`
- Full Enumeration: `nmap -A <IP>`

Common Scan Combos

Frequently used combinations that speed up reconnaissance and improve coverage. These presets simplify common scanning workflows.

- Top 100 Ports: `nmap -top-ports 100 <IP>`
- Full TCP Scan: `nmap -p- <IP>`
- Version + Scripts: `nmap -sV -sC <IP>`
- OS + Version: `nmap -O -sV <IP>`

UDP Essentials

Key commands for scanning UDP services, which behave differently from TCP. UDP scans are slower and often require retries.

- Basic: `nmap -sU <IP>`
- Top Ports: `nmap -sU -top-ports 20 <IP>`
- Combined TCP+UDP: `nmap -sS -sU <IP>`
- Aggressive Versioning: `-version-intensity 9`

Quick Host Information

Commands used to gather basic metadata about a host without performing a full scan. These are useful for quick reconnaissance.

- Reverse DNS: `nmap -sL <IP>`
- Traceroute: `nmap -traceroute <IP>`
- Ping only: `nmap -sn <IP>`
- ARP only: `nmap -PR <IP>`

Targeting & Output

Controls how targets are supplied and how scan results are saved. These options help automate and document scanning.

- Input List: `nmap -iL targets.txt`
- Specific Port: `nmap -p 22 <IP>`
- Port Range: `nmap -p 1-1000 <IP>`
- Output Normal: `-oN scan.txt`
- Grepable: `-oG scan.grep`
- All Formats: `-oA scan`

Firewall & IDS Evasion

Techniques used to bypass or confuse firewalls and intrusion detection systems. These options help avoid detection or filtering.

- Fragment Packets: `-f`
- Decoys: `-D RND:10`
- Source Port Spoof: `-source-port 53`
- Bad Checksums: `-badsum`
- MAC Spoofing: `-spoof-mac <vendor>`

Output Formats

Different formats for exporting scan results for analysis or automation. These formats support scripting and reporting.

- Normal: `-oN scan.txt`
- Grepable: `-oG scan.grep`
- XML: `-oX scan.xml`
- All Formats: `-oA scan`

Common Errors & Meanings

Frequent Nmap warnings and what they typically indicate. These help troubleshoot unexpected scan results.

- `Host seems down` - ICMP blocked; try `-Pn`
- `All ports filtered` - firewall dropping probes
- `No exact OS matches` - insufficient open/closed ports
- `UDP scan slow` - normal; UDP requires retries
- `Insufficient privileges` - use `sudo`

When to Use Each Scan Type

A quick guide to choosing the right scan for the situation. Each scan type has strengths depending on the environment.

- `-sS` - stealthy and fast
- `-sT` - use without raw sockets
- `-sA` - map firewall rules
- `-sU` - discover UDP services
- `-sC` - safe default enumeration
- `-A` - full recon when noise is acceptable

Nmap Scripting Engine (NSE)

A powerful system for automating enumeration and vulnerability checks. NSE extends Nmap's capabilities with hundreds of scripts.

- Default Scripts: `nmap -sC <IP>`
- Vulnerability Scan: `nmap -script vuln <IP>`
- HTTP Enum: `nmap -script http-enum -p 80 <IP>`
- SSH Algorithms: `nmap -script ssh2-enum-algos -p 22 <IP>`
- SMB Enum: `nmap -script smb-enum-shares -p 445 <IP>`
- Script Path: `/usr/share/nmap/scripts/`

Script Execution Tips

Guidelines for using NSE scripts effectively. Helps avoid common mistakes and improve results.

- Use `-sV` with scripts for better matching
- Combine `-script` with `-p` to limit scope
- Use `-script-help <name>` to preview script usage
- Avoid intrusive scripts on production systems

Useful NSE Categories

Groups of scripts organised by purpose to simplify selection. Each category targets a specific type of task.

- `vuln` - scripts that check for known vulnerabilities
- `safe` - non-intrusive scripts that do not affect the target
- `auth` - scripts that test or enumerate authentication methods
- `discovery` - scripts that gather information about hosts and services
- `intrusive` - aggressive scripts that may disrupt services

Service-Specific Scans

Targeted scans for common services to extract detailed information. These help identify misconfigurations or weaknesses.

- SMB: `-script smb-enum-shares -p 445`
- HTTP: `-script http-title,http-enum -p 80,443`
- SSH: `-script ssh2-enum-algos -p 22`
- DNS: `-sU -p 53 -script dns-recursion`

Scan examples

Pre-built scanning patterns for common reconnaissance scenarios.

- Full Recon: `nmap -A -p- <IP>`
- Fast Recon: `nmap -T4 -F <IP>`
- Web Server: `nmap -sV -script http-enum -p 80,443 <IP>`
- SMB Audit: `nmap -sV -script smb-vuln* -p 445 <IP>`
- Stealth: `nmap -sS -T2 <IP>`

Scan Workflow

A simple sequence to structure reconnaissance from light to deep scanning.

- Step 1: Host discovery (`-sn`)
- Step 2: Fast port sweep (`-F`)
- Step 3: Full TCP scan (`-p-`)
- Step 4: Service detection (`-sV`)
- Step 5: OS detection (`-O`)
- Step 6: Scripted enumeration (`-sC`)