🗺️ NMAP COMPLETE CHEAT SHEET

📖 Basic Syntax

```
nmap [Scan Type(s)] [Options] {target specification}
```

🔍 Common Scan Types

Scan Type	Command	Description	Use Case
SYN Scan	`-sS`	SYN (Stealth) Scan	Default, fast, stealthy - doesn't complete TCP handshake
TCP Connect	`-sT`	TCP Connect Scan	Used when SYN scan not available (no root privileges)
UDP Scan	`-sU`	UDP Scan	Scan UDP ports (DNS, SNMP, DHCP)
Ping Scan	`-sn`	Ping Scan (no port scan)	Host discovery only, no port scanning
ACK Scan	`-sA`	ACK Scan	Firewall rule testing, determine if filtered
Null Scan	`-sN`	Null Scan	No flags set - can evade some firewalls
FIN Scan	`-sF`	FIN Scan	FIN flag set - stealthy scan
Xmas Scan	`-sX`	Xmas Scan	FIN, PSH, URG flags - lights up like Christmas tree

🎯 Target Specification

Method	Command	Description
Single IP	`nmap 192.168.1.1`	Scan single IP address
IP Range	`nmap 192.168.1.1-50`	Scan range of IPs
CIDR Notation	`nmap 192.168.1.0/24`	Scan entire subnet
Multiple IPs	`nmap 192.168.1.1 192.168.1.5`	Scan multiple specific IPs

Method	Command	Description
From File	`nmap -iL targets.txt`	Read targets from file
Exclude Hosts	`nmap 192.168.1.0/24 --exclude 192.168.1.1`	Exclude specific hosts
Exclude File	`nmap 192.168.1.0/24 --excludefile exclude.txt`	Exclude hosts from file

🔌 Port Scanning Options

Option	Command	Description
Specific Ports	`-p 22,80,443`	Scan specific ports
Port Range	`-p 1-1000`	Scan port range
All Ports	`-p-`	Scan all 65535 ports
Top Ports	`--top-ports 100`	Scan top N most common ports
Fast Scan	`-F`	Fast scan (top 100 ports)
Sequential	`-r`	Scan ports sequentially (not random)
Port Protocol	`-p U:53,T:80`	UDP port 53, TCP port 80

🔬 Service and OS Detection

Option	Command	Description	Example
Version Detection	`-sV`	Probe open ports to determine service/version	`nmap -sV 192.168.1.1`
OS Detection	`-O`	Enable OS detection	`nmap -O 192.168.1.1`
Aggressive OS Guess	`--osscan-guess`	Aggressive OS detection	`nmap -O --osscan-guess 192.168.1.1`
Version Intensity	`--version-intensity 0-9`	Set version detection intensity (default 7)	`nmap -sV --version-intensity 9 target.com`
Version Light	`--version-light`	Light version detection (faster)	`nmap -sV --version-light target.com`

Option	Command	Description	Example
Version All	`--version-all`	Try every probe (slower but thorough)	`nmap -sV --version-all target.com`

🚀 Advanced Scans

Option	Command	Description	Use Case
Aggressive	`-A`	Aggressive scan (OS, version, script, traceroute)	`nmap -A 192.168.1.1`
Timing T0	`-T0`	Paranoid (very slow, IDS evasion)	`nmap -T0 target.com`
Timing T1	`-T1`	Sneaky (slow, IDS evasion)	`nmap -T1 target.com`
Timing T2	`-T2`	Polite (slow down to use less bandwidth)	`nmap -T2 target.com`
Timing T3	`-T3`	Normal (default timing)	`nmap -T3 target.com`
Timing T4	`-T4`	Aggressive (faster, assumes fast network)	`nmap -T4 target.com`
Timing T5	`-T5`	Insane (very fast, may miss ports)	`nmap -T5 target.com`
Max Retries	`--max-retries N`	Limit probe retransmissions	`nmap --max-retries 2 target.com`
Host Timeout	`--host-timeout 30m`	Give up on slow hosts	`nmap --host-timeout 5m target.com`
Min Rate	`--min-rate 1000`	Send packets at minimum rate	`nmap --min-rate 1000 target.com`
Max Rate	`--max-rate 10000`	Send packets at maximum rate	`nmap --max-rate 5000 target.com`

📜 Nmap Scripting Engine (NSE)

Script Category	Command	Description	Example
Default Scripts	`--script=default`	Run default NSE scripts	`nmap --script=default target.com`
Vulnerability	`--script=vuln`	Scan for vulnerabilities	`nmap --script=vuln target.com`
HTTP Scripts	`--script=http*`	All HTTP-related scripts	`nmap --script=http* -p80,443 target.com`
Auth Scripts	`--script=auth`	Authentication bypass scripts	`nmap --script=auth target.com`
Brute Force	`--script=brute`	Brute force attacks	`nmap --script=brute target.com`
Discovery	`--script=discovery`	Network discovery scripts	`nmap --script=discovery target.com`
DOS	`--script=dos`	Denial of Service scripts	`nmap --script=dos target.com`
Exploit	`--script=exploit`	Exploitation scripts	`nmap --script=exploit target.com`
External	`--script=external`	Scripts using external services	`nmap --script=external target.com`
Fuzzer	`--script=fuzzer`	Fuzzing scripts	`nmap --script=fuzzer target.com`
Intrusive	`--script=intrusive`	Intrusive scripts (may crash)	`nmap --script=intrusive target.com`
Malware	`--script=malware`	Check for malware	`nmap --script=malware target.com`
Safe	`--script=safe`	Safe scripts (won't crash)	`nmap --script=safe target.com`
Version	`--script=version`	Version detection scripts	`nmap --script=version target.com`
Script Help	`--script-help=scriptname`	Display help for specific script	`--script-help=http-enum`

Useful NSE Script Examples

```
# SMB vulnerabilities
nmap --script smb-vuln* -p445 target.com

# HTTP enumeration
```

```
nmap --script http-enum -p80,443 target.com

# SSL/TLS vulnerabilities
nmap --script ssl* -p443 target.com

# DNS zone transfer
nmap --script dns-zone-transfer --script-args dns-zone-
transfer.domain=example.com -p53 target.com

# SQL injection detection
nmap --script http-sql-injection target.com

# FTP anonymous login
nmap --script ftp-anon -p21 target.com

# SSH authentication methods
nmap --script ssh-auth-methods -p22 target.com

# SMB shares enumeration
nmap --script smb-enum-shares -p445 target.com

# HTTP methods
nmap --script http-methods -p80 target.com

# SSL certificate info
nmap --script ssl-cert -p443 target.com
```

💾 Output Options

Format	Command	Description	Use Case
Normal Output	`-oN output.txt`	Human-readable format	Easy to read, documentation
XML Output	`-oX output.xml`	XML format	Importing into other tools
Greppable	`-oG output.gnmap`	Greppable format	Easy parsing with grep/awk
All Formats	`-oA basename`	Save in all formats (N, X, G)	Comprehensive output
Script Kiddie	`-oS output.txt`	Script kiddie format (leet speak)	Just for fun

Format	Command	Description	Use Case
Append Output	`--append-output`	Append to existing file	Continue previous scan
Verbose	`-v`	Increase verbosity	See more details during scan
Very Verbose	`-vv`	Even more verbose	Maximum scan details
Debug	`-d`	Enable debugging	Troubleshooting
Packet Trace	`--packet-trace`	Show packets sent/received	Deep packet analysis

---

🛡️ Firewall/IDS Evasion Techniques

Technique	Command	Description	Example
Decoy Scan	`-D decoy1,decoy2,ME`	Use decoy IPs to hide real source	`nmap -D 192.168.1.5,192.168.1.6,ME target.com`
Random Decoys	`-D RND:10`	Generate random decoys	`nmap -D RND:10 target.com`
Spoof Source IP	`-S spoofed-IP`	Spoof source IP address	`nmap -S 192.168.1.5 -e eth0 -Pn target.com`
Spoof MAC	`--spoof-mac MAC`	Spoof MAC address	`nmap --spoof-mac 00:11:22:33:44:55 target.com`
Source Port	`--source-port 53`	Use specific source port	`nmap --source-port 53 target.com`
Append Data	`--data-length 25`	Append random data to packets	`nmap --data-length 25 target.com`
Randomize Hosts	`--randomize-hosts`	Randomize target scan order	`nmap --randomize-hosts 192.168.1.0/24`
Scan Delay	`--scan-delay 1s`	Add delay between probes	`nmap --scan-delay 2s target.com`
Max Scan Delay	`--max-scan-delay 5s`	Maximum delay between probes	`nmap --max-scan-delay 5s target.com`

Technique	Command	Description	Example
Fragment Packets	`-f`	Fragment IP packets	`nmap -f target.com`
MTU Fragment	`--mtu 16`	Specify custom MTU	`nmap --mtu 24 target.com`
Bad Checksum	`--badsum`	Send packets with bad checksums	`nmap --badsum target.com`
Idle Scan	`-sI zombie_host`	Use zombie host for scanning	`nmap -sI zombie_host target.com`

🌐 Host Discovery Options

Option	Command	Description	Example
Ping Scan Only	`-sn`	No port scan, only host discovery	`nmap -sn 192.168.1.0/24`
No Ping	`-Pn`	Skip host discovery, treat all as online	`nmap -Pn target.com`
TCP SYN Ping	`-PS port`	TCP SYN ping to specific port	`nmap -PS22,80,443 target.com`
TCP ACK Ping	`-PA port`	TCP ACK ping to specific port	`nmap -PA80 target.com`
UDP Ping	`-PU port`	UDP ping to specific port	`nmap -PU53 target.com`
ICMP Echo	`-PE`	ICMP echo request (ping)	`nmap -PE target.com`
ICMP Timestamp	`-PP`	ICMP timestamp request	`nmap -PP target.com`
ICMP Netmask	`-PM`	ICMP netmask request	`nmap -PM target.com`
IP Protocol Ping	`-PO protocol`	IP protocol ping	`nmap -PO1,2,4 target.com`
ARP Ping	`-PR`	ARP ping (local network only)	`nmap -PR 192.168.1.0/24`
No DNS Resolution	`-n`	Don't resolve DNS	`nmap -n target.com`

Option	Command	Description	Example
DNS Resolution	`-R`	Always resolve DNS	`nmap -R target.com`
Custom DNS	`--dns-servers server`	Use custom DNS server	`nmap --dns-servers 8.8.8.8 target.com`

🎯 Real-World Nmap Examples

Basic Network Scan 🌐

```
# Quick scan of top 100 ports
nmap -F 192.168.1.0/24

# Full scan with service detection
nmap -p- -sV 192.168.1.100

# Aggressive scan
nmap -A -T4 192.168.1.100
```

Stealth Scanning 🥷

```
# SYN scan with decoys
nmap -sS -D RND:10 -T2 target.com

# Fragmented packets with slow timing
nmap -f -T1 target.com

# Custom source port with delay
nmap --source-port 53 --scan-delay 2s target.com
```

Vulnerability Scanning 🔍

```
# Check for vulnerabilities
nmap --script vuln target.com

# SMB vulnerabilities (EternalBlue, etc.)
nmap --script smb-vuln* -p445 target.com

# Web vulnerabilities
nmap --script http-vuln* -p80,443 target.com
```

```
# SSL/TLS vulnerabilities
nmap --script ssl-heartbleed,ssl-poodle -p443 target.com
```

Service Enumeration 📊

```
# HTTP enumeration
nmap --script http-enum,http-headers,http-methods -p80,443 target.com

# FTP enumeration
nmap --script ftp-anon,ftp-bounce -p21 target.com

# SMB enumeration
nmap --script smb-enum-shares,smb-enum-users,smb-os-discovery -p445 target.com

# SMTP enumeration
nmap --script smtp-enum-users,smtp-commands -p25 target.com

# DNS enumeration
nmap --script dns-zone-transfer,dns-brute -p53 target.com
```

Network Discovery 🗺️

```
# Live host discovery
nmap -sn 192.168.1.0/24

# Identify operating systems
nmap -O 192.168.1.0/24

# Traceroute to targets
nmap --traceroute 192.168.1.100

# Identify network devices
nmap -O --osscan-guess 192.168.1.1
```

Output and Reporting 📝

```
# Save in all formats
nmap -A -oA scan_results target.com

# Verbose output to file
nmap -v -oN verbose_scan.txt target.com
```

```
# XML output for import
nmap -oX scan.xml target.com

# Greppable output
nmap -oG scan.gnmap 192.168.1.0/24
```

Advanced Techniques 🎓

```
# Idle scan (zombie scan)
nmap -sI zombie_host target.com

# IPv6 scanning
nmap -6 target.com

# Scan with script arguments
nmap --script http-brute --script-args userdb=users.txt,passdb=pass.txt
target.com

# Multiple script categories
nmap --script "default and safe" target.com

# Exclude certain scripts
nmap --script "all and not broadcast" target.com
```

💡 Nmap Pro Tips

Performance Optimization ⚡

```
# Fast network scan
nmap -T4 --min-rate 1000 192.168.1.0/24

# Very aggressive scan
nmap -T5 --max-retries 1 target.com

# Parallel host scanning
nmap --min-hostgroup 50 192.168.1.0/24

# Parallel port scanning
nmap --min-parallelism 100 target.com
```

Evasion Combinations 🎭

```
# Maximum stealth
nmap -sS -T1 -f -D RND:10 --source-port 53 --data-length 25 target.com

# Firewall bypass
nmap -sA -T4 --source-port 80 target.com

# IDS evasion with randomization
nmap -T2 --randomize-hosts --scan-delay 1s 192.168.1.0/24
```

Targeted Scanning 🎯

```
# Scan only specific services
nmap -p 80,443,8080,8443 --script http* target.com

# Quick vulnerability check
nmap --script "vuln and safe" -sV target.com

# Comprehensive service analysis
nmap -sV --version-all -p- target.com
```

📚 Nmap Script Categories Detailed

Category	Purpose	Risk Level	Example
auth	Authentication testing	Low-Medium	Bypass authentication
broadcast	Network broadcast/discovery	Low	DHCP, DNS-SD discovery
brute	Brute force attacks	Medium-High	Password guessing
default	Basic scripts (safe)	Low	Standard enumeration
discovery	Network/service discovery	Low	Version detection
dos	Denial of Service	High	May crash services
exploit	Active exploitation	High	Can compromise systems
external	Uses external resources	Low	Queries external databases
fuzzer	Fuzz testing	Medium-High	May crash services
intrusive	Aggressive testing	High	May be detected/blocked
malware	Malware detection	Low	Check for backdoors
safe	Won't harm target	Low	Safe enumeration
version	Version detection	Low	Service fingerprinting

Category	Purpose	Risk Level	Example
vuln	Vulnerability detection	Medium	Check for known vulns

🔧 Nmap Troubleshooting

Common Issues and Solutions ⚠️

```
# Permission denied - requires root
sudo nmap -sS target.com

# Slow scan - increase speed
nmap -T4 --min-rate 1000 target.com

# Firewall blocking - use evasion
nmap -f -D RND:5 --source-port 53 target.com

# No results - skip ping
nmap -Pn target.com

# UDP scan too slow - limit ports
nmap -sU --top-ports 20 target.com

# Debug connection issues
nmap -d --packet-trace target.com
```

📊 Nmap Output Parsing

Grep Useful Information 🔍

```
# Find open ports
grep "open" scan.gnmap

# Extract IPs with open ports
grep "Up" scan.gnmap | cut -d " " -f 2

# Find specific service
grep "http" scan.gnmap
```

```
# Count live hosts
grep -c "Status: Up" scan.gnmap
```

AWK Processing 📈

```
# Extract IPs and open ports
awk '/open/{print $2, $5}' scan.gnmap

# List only IPs with SSH open
awk '/22\/open/{print $2}' scan.gnmap
```

🎯 COMPLETE ATTACK WORKFLOW EXAMPLE

🔍 Phase 1: Reconnaissance

```
# Step 1: Host discovery
nmap -sn 192.168.1.0/24 -oA host_discovery

# Step 2: Port scanning
nmap -sS -p- --open 192.168.1.0/24 -oA full_scan

# Step 3: Service detection
nmap -sV -sC -p $(cat full_scan.gnmap | grep "/open/" | cut -d" " -f5 | cut -d"/" -f1 | sort -u | tr '\n' ',') 192.168.1.100 -oA service_scan
```

🎯 Phase 2: Enumeration

```
# Web services
nmap --script http-enum,http-headers,http-methods -p80,443 target.com

# SMB shares
nmap --script smb-enum-shares,smb-enum-users -p445 target.com

# Check for vulnerabilities
nmap --script vuln -sV target.com
```

⚔️ Phase 3: Vulnerability Assessment

```
# Comprehensive vulnerability scan
nmap --script "vuln and safe" -sV -p- target.com -oA vuln_scan
```

```
# Specific vulnerability checks
nmap --script smb-vuln-ms17-010 -p445 target.com  # EternalBlue
nmap --script ssl-heartbleed -p443 target.com     # Heartbleed
nmap --script http-shellshock -p80 target.com     # Shellshock
```

🏆 SUMMARY & BEST PRACTICES

✅ Do's

- ✔️ Always get permission before scanning
- ✔️ Start with -sn for host discovery
- ✔️ Use -oA to save all output formats
- ✔️ Use timing templates appropriately (-T0 to -T5)
- ✔️ Combine -sV with --script for better results
- ✔️ Use --reason to understand why ports are marked as open/closed/filtered

❌ Don'ts

- ❌ Don't scan without authorization
- ❌ Don't use -T5 on production networks
- ❌ Don't run intrusive scripts on critical systems
- ❌ Don't forget to use -Pn if firewalls block ping
- ❌ Don't scan entire internet ranges without proper resources

---

🔗 USEFUL RESOURCES & LINKS

📚 Official Documentation

- **Nmap Official Site:** https://nmap.org
- **Nmap Book:** https://nmap.org/book/
- **NSE Script Database:** https://nmap.org/nsedoc/
- **Nmap Reference Guide:** https://nmap.org/book/man.html

🎓 Learning Resources

- **Nmap Network Scanning** by Gordon Lyon
- **Metasploit: The Penetration Tester's Guide**

- **The Web Application Hacker's Handbook**
- **OWASP Testing Guide**