Nmap Complete Reference Guide

Installation & Setup

```bash
# Check if installed
nmap --version

# Install on Debian/Ubuntu/Kali
sudo apt update && sudo apt install nmap -y

# Help and documentation
nmap --help
man nmap

# Update Nmap
sudo apt update && sudo apt upgrade nmap
```

Target Specification

```bash
```

```
# Single target
nmap 192.168.1.1
nmap scanme.nmap.org

# Multiple targets
nmap 192.168.1.1 192.168.1.2
nmap 192.168.1.1,2,3

# Range of IPs
nmap 192.168.1.1-10
nmap 192.168.1.1-255

# Subnet scanning
nmap 192.168.1.0/24

# Exclude targets
nmap 192.168.1.0/24 --exclude 192.168.1.1
nmap 192.168.1.0/24 --excludefile exclude.txt

# Read targets from file
nmap -iL targets.txt
```

Host Discovery

bash

```
# Ping sweep - check if hosts are up
nmap -sn 192.168.1.0/24

# Skip ping (assume host is up)
nmap -Pn target.com

# TCP SYN ping
nmap -PS target.com

# TCP ACK ping
nmap -PA target.com

# UDP ping
nmap -PU target.com

# ICMP ping types
nmap -PE target.com  # ICMP Echo
nmap -PP target.com  # ICMP Timestamp
nmap -PM target.com  # ICMP Netmask

# ARP scan (local network only)
nmap -PR 192.168.1.0/24
```

Scan Techniques

TCP Scans

bash

```
# TCP SYN scan (half-open, stealth)
sudo nmap -sS target.com

# TCP Connect scan (full connection)
nmap -sT target.com

# TCP ACK scan (firewall detection)
sudo nmap -sA target.com

# TCP Window scan
sudo nmap -sW target.com

# TCP Maimon scan
sudo nmap -sM target.com

# TCP FIN scan
sudo nmap -sF target.com

# TCP NULL scan
sudo nmap -sN target.com

# TCP XMAS scan
sudo nmap -sX target.com
```

UDP Scans

bash

```
# UDP scan (slow but important)
sudo nmap -sU target.com

# UDP scan top ports only
sudo nmap -sU --top-ports 100 target.com

# Combined TCP SYN + UDP
sudo nmap -sS -sU target.com
```

Other Scan Types

bash

```
# IP protocol scan
sudo nmap -sO target.com

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

# FTP bounce scan
nmap -b ftp_server target.com
```

Port Specification

bash

```
# Single port
nmap -p 80 target.com

# Multiple specific ports
nmap -p 22,80,443 target.com

# Port range
nmap -p 1-1000 target.com
nmap -p 80-90 target.com

# All 65535 ports
nmap -p- target.com
nmap -p 1-65535 target.com

# Top common ports
nmap --top-ports 10 target.com
nmap --top-ports 100 target.com
nmap --top-ports 1000 target.com

# Fast scan (top 100 ports)
nmap -F target.com

# TCP and UDP ports
nmap -p T:80,443,U:53,161 target.com

# Protocol-specific ports
nmap -p U:53,111,137 target.com  # UDP only
nmap -p T:21-25,80,443 target.com  # TCP only
```

Service & Version Detection

bash

```
# Service version detection
nmap -sV target.com

# Intensity levels (0-9)
nmap -sV --version-intensity 5 target.com
nmap -sV --version-intensity 9 target.com  # Most aggressive

# Version light (faster)
nmap -sV --version-light target.com

# Version all (slower but thorough)
nmap -sV --version-all target.com

# Version trace (debugging)
nmap -sV --version-trace target.com
```

Operating System Detection

bash

```
# OS detection
sudo nmap -O target.com

# Aggressive OS detection
sudo nmap -O --osscan-guess target.com

# OS scan limit (skip if no open/closed ports)
sudo nmap -O --osscan-limit target.com

# Maximum OS detection tries
sudo nmap -O --max-os-tries 2 target.com
```

Script Scanning (NSE)

bash

```
# Default scripts
nmap -sC target.com
nmap --script=default target.com

# Specific script
nmap --script=http-title target.com

# Multiple scripts
nmap --script=http-title,http-headers target.com

# Script categories
nmap --script=safe target.com
nmap --script=intrusive target.com
nmap --script=vuln target.com
nmap --script=exploit target.com
nmap --script=dos target.com
nmap --script=malware target.com
nmap --script=discovery target.com
nmap --script=version target.com
nmap --script=auth target.com

# Script wildcards
nmap --script="http-*" target.com
nmap --script="smb-*" target.com
nmap --script="*sql*" target.com

# Script arguments
nmap --script=http-form-brute \
 --script-args userdb=users.txt,passdb=passwords.txt \
 target.com

# Script help
nmap --script-help http-title
```

Timing and Performance

bash

```
# Timing templates (0=paranoid to 5=insane)
nmap -T0 target.com  # Paranoid (very slow)
nmap -T1 target.com  # Sneaky
nmap -T2 target.com  # Polite
nmap -T3 target.com  # Normal (default)
nmap -T4 target.com  # Aggressive (recommended)
nmap -T5 target.com  # Insane (very fast)

# Custom timing
nmap --min-hostgroup 50 target.com
nmap --max-hostgroup 100 target.com
nmap --min-parallelism 50 target.com
nmap --max-parallelism 100 target.com
nmap --min-rtt-timeout 100ms target.com
nmap --max-rtt-timeout 500ms target.com
nmap --max-retries 2 target.com
nmap --host-timeout 300s target.com
nmap --scan-delay 1s target.com
nmap --max-scan-delay 10s target.com
nmap --min-rate 100 target.com
nmap --max-rate 1000 target.com
```

Firewall/IDS Evasion

bash

```
# Fragment packets
nmap -f target.com
nmap -ff target.com  # 8-byte fragments

# Decoy scans
nmap -D RND:10 target.com  # Random decoys
nmap -D decoy1,decoy2,ME,decoy3 target.com

# Source port spoofing
nmap --source-port 53 target.com
nmap -g 53 target.com

# Randomize target order
nmap --randomize-hosts target1 target2 target3

# MAC address spoofing
nmap --spoof-mac 0 target.com  # Random MAC
nmap --spoof-mac Apple target.com
nmap --spoof-mac 00:11:22:33:44:55 target.com

# Data length modification
nmap --data-length 25 target.com

# IP options
nmap --ip-options "L 192.168.1.1 192.168.1.2" target.com

# TTL modification
nmap --ttl 64 target.com

# Bad checksum
nmap --badsum target.com

# IPv6 scanning
nmap -6 target.com
```

Output Formats

bash

```
# Normal output
nmap -oN scan.txt target.com

# XML output
nmap -oX scan.xml target.com

# Grepable output
nmap -oG scan.gnmap target.com

# Script kiddie format
nmap -oS scan.skid target.com

# All formats at once
nmap -oA scan_results target.com

# Append to file
nmap -oN scan.txt --append-output target.com

# No output to stdout
nmap -oN scan.txt --open target.com > /dev/null
```

Common Port Numbers & Services

```
20/21   - FTP (File Transfer Protocol)
22      - SSH (Secure Shell)
23      - Telnet
25      - SMTP (Simple Mail Transfer Protocol)
53      - DNS (Domain Name System)
67/68   - DHCP
69      - TFTP (Trivial File Transfer Protocol)
80      - HTTP (HyperText Transfer Protocol)
88      - Kerberos
110     - POP3 (Post Office Protocol v3)
111     - RPC (Remote Procedure Call)
135     - RPC Endpoint Mapper
137/138/139 - NetBIOS
143     - IMAP (Internet Message Access Protocol)
161/162 - SNMP (Simple Network Management Protocol)
389     - LDAP (Lightweight Directory Access Protocol)
443     - HTTPS (HTTP Secure)
```

```
445   - SMB (Server Message Block)
465   - SMTPS (SMTP Secure)
514   - Syslog
587   - SMTP (submission)
636   - LDAPS (LDAP Secure)
993   - IMAPS (IMAP Secure)
995   - POP3S (POP3 Secure)
1433  - MSSQL (Microsoft SQL Server)
1521  - Oracle Database
3306  - MySQL Database
3389  - RDP (Remote Desktop Protocol)
5432  - PostgreSQL Database
5900  - VNC (Virtual Network Computing)
5985/5986 - WinRM (Windows Remote Management)
6379  - Redis
8080  - HTTP Alternate
8443  - HTTPS Alternate
27017 - MongoDB
```

Port States Explained

- **Open**: Port accepts connections - service is listening
- **Closed**: Port is accessible but no service is listening
- **Filtered**: Cannot determine if port is open - firewall/filter blocking
- **Unfiltered**: Port is accessible but cannot determine if open or closed
- **Open|Filtered**: Cannot determine if port is open or filtered (UDP scans)
- **Closed|Filtered**: Cannot determine if port is closed or filtered

Advanced Techniques

```bash
```

```
# Aggressive scan (combines -O -sV -sC --traceroute)
sudo nmap -A target.com

# Version scan with default scripts
nmap -sC -sV target.com

# Fast comprehensive scan
nmap -T4 -A -v target.com

# Scan only open ports
nmap --open target.com

# Verbose output levels
nmap -v target.com    # Level 1
nmap -vv target.com   # Level 2
nmap -vvv target.com  # Level 3

# Debug output
nmap -d target.com    # Level 1
nmap -dd target.com   # Level 2

# Reason for port state
nmap --reason target.com

# Packet trace
nmap --packet-trace target.com

# Resume scan from log
nmap --resume scan.log

# Interface specification
nmap -e eth0 target.com

# Source IP specification
nmap -S 192.168.1.100 target.com

# Traceroute
nmap --traceroute target.com
```

```
# Script tracing
nmap --script-trace target.com
```

Useful Script Categories

bash

```
# Authentication scripts
nmap --script=auth target.com

# Brute force scripts
nmap --script=brute target.com

# Discovery scripts (safe)
nmap --script=discovery target.com

# DoS scripts (use carefully)
nmap --script=dos target.com

# Exploit scripts (use in controlled environment)
nmap --script=exploit target.com

# External scripts (contact external services)
nmap --script=external target.com

# Fuzzer scripts
nmap --script=fuzzer target.com

# Intrusive scripts (may harm target)
nmap --script=intrusive target.com

# Malware detection scripts
nmap --script=malware target.com

# Safe scripts (unlikely to harm)
nmap --script=safe target.com

# Version detection scripts
nmap --script=version target.com

# Vulnerability detection scripts
nmap --script=vuln target.com
```

Real-World Examples

bash

```
# Quick network discovery
nmap -sn 192.168.1.0/24

# Fast port scan
nmap -T4 -F target.com

# Comprehensive scan
sudo nmap -T4 -A -v target.com

# Web server analysis
nmap -p 80,443 --script=http-* target.com

# SMB enumeration
nmap -p 445 --script=smb-* target.com

# Database detection
nmap -p 1433,3306,5432 -sV target.com

# Vulnerability assessment
nmap --script=vuln target.com

# Stealth scan
sudo nmap -sS -T2 -f target.com

# Bypass firewall
nmap -f -D RND:10 --source-port 53 target.com
```

Troubleshooting Common Issues

bash

```
# Permission denied for SYN scan
# Solution: Use sudo or switch to TCP connect scan
sudo nmap -sS target.com
nmap -sT target.com

# Scan too slow
# Solution: Increase timing, reduce scope
nmap -T4 --top-ports 1000 target.com

# Host seems down
# Solution: Skip ping, use -Pn
nmap -Pn target.com

# Firewall blocking
# Solution: Use evasion techniques
nmap -f -D RND:5 -T2 target.com

# Need to scan specific interface
# Solution: Specify interface
nmap -e eth0 target.com
```

Pro Tips

- Always use -T4 for faster scans unless stealth is required
- Combine -sC -sV for comprehensive service detection
- Use --top-ports for faster broad scans
- Save results with -oA for all output formats
- Use -Pn when targets don't respond to ping
- Check --script-help for script documentation
- Use -v for verbose output to see progress
- Consider legal and ethical implications
- Test in controlled environments first