Nmap Cheatsheet

Essential commands for network discovery and security auditing

This cheatsheet provides a quick reference to fundamental Nmap operations, syntax, and advanced features, ideal for both beginners and experienced security professionals for efficient network reconnaissance and vulnerability assessment.

Host Discovery — Find active hosts on network

Port Scanning — Identify open ports and services

Service Detection — Determine service versions

OS Detection — Identify operating systems

Script Scanning — Run NSE scripts for deeper analysis

Installation & Setup

Linux Installation

Install Nmap using your distribution's package manager.

```
# Ubuntu/Debian
sudo apt update && sudo apt install nmap

# RHEL/Fedora/CentOS
sudo dnf install nmap

# Verify installation
nmap --version
```

macOS Installation

Install using Homebrew package manager.

```
# Install via Homebrew
brew install nmap

# Direct download from nmap.org
# Download .dmg from https://nmap.org/download.html
```

Windows Installation

Download and install from the official website.

```
# Download installer from
https://nmap.org/download.html
# Run the .exe installer with administrator privileges
# Includes Zenmap GUI and command-line version
```

Basic Verification

Test your installation and get help.

```
# Display version information
nmap --version

# Show help menu
nmap -h

# Extended help and options
man nmap
```

Basic Scanning Techniques

Basic Nmap scanning commands, often used at the first stage of enumeration.

01

Simple Host Scan: `nmap [target]`

Basic scan of a single host or IP address.

```
# Scan single IP
nmap 192.168.1.1

# Scan hostname
nmap example.com

# Scan multiple IPs
nmap 192.168.1.1 192.168.1.5
192.168.1.10
```

02

Network Range Scan

Nmap allows hostnames, IP addresses, subnets.

```
# Scan IP range
nmap 192.168.1.1-254

# Scan subnet with CIDR notation
nmap 192.168.1.0/24

# Scan multiple networks
nmap 192.168.1.0/24 10.0.0.0/8
```

03

Input from File

Scan targets listed in a file.

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

# Exclude specific hosts
nmap 192.168.1.0/24 --exclude
192.168.1.1

# Exclude from file
nmap 192.168.1.0/24 --excludefile
exclude.txt
```

Host Discovery Techniques

Ping Scan: `nmap -sn`

Host discovery is a key way many analysts and pentesters use Nmap. Its purpose is to gain an overview of which systems are online.

```
# Ping scan only (no port scan)
nmap -sn 192.168.1.0/24

# Skip host discovery (assume all hosts up)
nmap -Pn 192.168.1.1

# ICMP echo ping
nmap -PE 192.168.1.0/24
```

TCP Ping Techniques

Use TCP packets for host discovery.

```
# TCP SYN ping to port 80
nmap -PS80 192.168.1.0/24

# TCP ACK ping
nmap -PA80 192.168.1.0/24

# TCP SYN ping to multiple ports
nmap -PS22,80,443 192.168.1.0/24
```

UDP Ping: `nmap -PU`

Use UDP packets for host discovery.

```
# UDP ping to common ports
nmap -PU53,67,68,137 192.168.1.0/24

# UDP ping to default ports
nmap -PU 192.168.1.0/24
```

ARP Ping: `nmap -PR`

Use ARP requests for local network discovery.

```
# ARP ping (default for local networks)
nmap -PR 192.168.1.0/24

# Disable ARP ping
nmap --disable-arp-ping 192.168.1.0/24
```

Port Scanning Types

Nmap supports a whole host of scan types, however, the most common ones include TCP connect scans and SYN scans.

TCP SYN Scan: `nmap -sS`

This scan is stealthier, as Nmap sends an RST packet, which prevents multiple requests and shortens the scan time.

```
# Default scan (requires root)
nmap -sS 192.168.1.1

# SYN scan specific ports
nmap -sS -p 80,443 192.168.1.1

# Fast SYN scan
nmap -sS -T4 192.168.1.1
```

TCP Connect Scan: `nmap -sT`

Nmap sends a TCP packet to a port with the SYN flag set. This lets the user know whether ports are open, closed, or unknown.

```
# TCP connect scan (no root required)
nmap -sT 192.168.1.1

# Connect scan with timing
nmap -sT -T3 192.168.1.1
```

UDP Scan: `nmap -sU`

Scan UDP ports for services.

```
# UDP scan (slow, requires root)
nmap -sU 192.168.1.1

# UDP scan common ports
nmap -sU -p 53,67,68,161 192.168.1.1

# Combined TCP/UDP scan
nmap -sS -sU -p T:80,443,U:53,161 192.168.1.1
```

Stealth Scans

Advanced scanning techniques for evasion.

```
# FIN scan
nmap -sF 192.168.1.1

# NULL scan
nmap -sN 192.168.1.1

# Xmas scan
nmap -sX 192.168.1.1
```

Port Specification

Port Ranges: `nmap -p`

Target specific ports, ranges, or combinations of TCP and UDP ports for more precise scans.

```
# Single port
nmap -p 80 192.168.1.1

# Multiple ports
nmap -p 22,80,443 192.168.1.1

# Port range
nmap -p 1-1000 192.168.1.1

# All ports
nmap -p- 192.168.1.1
```

Protocol-Specific Ports

Specify TCP or UDP ports explicitly.

```
# TCP ports only
nmap -p T:80,443 192.168.1.1

# UDP ports only
nmap -p U:53,161 192.168.1.1

# Mixed TCP and UDP
nmap -p T:80,U:53 192.168.1.1
```

Common Port Sets

Scan frequently used ports quickly.

```
# Top 1000 ports (default)
nmap 192.168.1.1

# Top 100 ports
nmap --top-ports 100 192.168.1.1

# Fast scan (100 most common ports)
nmap -F 192.168.1.1
```

Port States

There are six different states: Open, Closed, Filtered.

```
# Show only open ports
nmap --open 192.168.1.1

# Show all port states
nmap -v 192.168.1.1
```

Service & Version Detection

When we enumerate using Nmap, determining the application and its version is vital. We can use this information to scan for known vulnerabilities.

Service Detection: `nmap -sV`

Detect which services are running and attempt to identify their software versions and configurations.

```
# Basic version detection
nmap -sV 192.168.1.1

# Aggressive version detection
nmap -sV --version-intensity 9 192.168.1.1

# Light version detection
nmap -sV --version-intensity 0 192.168.1.1
```

Service Scripts

Use scripts for enhanced service detection.

```
# Default scripts with version detection
nmap -sC -sV 192.168.1.1

# Banner grabbing
nmap --script banner 192.168.1.1

# HTTP service enumeration
nmap --script http-* 192.168.1.1
```

Operating System Detection: `nmap -O`

Use TCP/IP fingerprinting to guess the operating system of target hosts.

```
# OS detection
nmap -O 192.168.1.1

# Aggressive OS detection
nmap -O --osscan-guess 192.168.1.1

# Limit OS detection attempts
nmap -O --max-os-tries 1 192.168.1.1
```

Comprehensive Detection

Combine multiple detection techniques.

```
# Aggressive scan (OS, version, scripts)
nmap -A 192.168.1.1

# Custom aggressive scan
nmap -sS -sV -O -sC 192.168.1.1
```

Timing & Performance

Timing Templates: `nmap -T`

Adjust scan speed and stealth based on your target environment and detection risk.

```
# Paranoid (very slow, stealthy)
nmap -T0 192.168.1.1

# Sneaky (slow, stealthy)
nmap -T1 192.168.1.1

# Polite (slower, less bandwidth)
nmap -T2 192.168.1.1

# Normal (default)
nmap -T3 192.168.1.1

# Aggressive (faster)
nmap -T4 192.168.1.1

# Insane (very fast, may miss results)
nmap -T5 192.168.1.1
```

Custom Timing Options

Fine-tune how Nmap handles timeouts, retries, and parallel scanning to optimize performance.

```
# Set minimum rate (packets per second)
nmap --min-rate 1000 192.168.1.1

# Set maximum rate
nmap --max-rate 100 192.168.1.1

# Parallel host scanning
nmap --min-hostgroup 10 192.168.1.0/24

# Custom timeout
nmap --host-timeout 5m 192.168.1.1
```

Nmap Scripting Engine (NSE)

Enhance your scans with Nmap's scripting engine for automation and deeper inspection.

Script Categories: `nmap --script`

Run scripts by category or name.

```
# Default scripts
nmap --script default 192.168.1.1

# Vulnerability scripts
nmap --script vuln 192.168.1.1

# Discovery scripts
nmap --script discovery 192.168.1.1

# Authentication scripts
nmap --script auth 192.168.1.1
```

Specific Scripts

Target specific vulnerabilities or services.

```
# SMB enumeration
nmap --script smb-enum-* 192.168.1.1

# HTTP methods
nmap --script http-methods 192.168.1.1

# SSL certificate info
nmap --script ssl-cert 192.168.1.1
```

Script Arguments

Pass arguments to customize script behavior.

```
# HTTP brute force with custom wordlist
nmap --script http-brute --script-args
userdb=users.txt,passdb=pass.txt 192.168.1.1

# SMB brute force
nmap --script smb-brute 192.168.1.1

# DNS brute force
nmap --script dns-brute example.com
```

Script Management

Manage and update NSE scripts.

```
# Update script database
nmap --script-updatedb

# List available scripts
ls /usr/share/nmap/scripts/ | grep http

# Get script help
nmap --script-help vuln
```

Output Formats & Saving Results

Save your scan results in formats like normal text, XML, or grepable output for later analysis.

Output Formats

Save results in different formats.

```
# Normal output
nmap -oN scan_results.txt 192.168.1.1

# XML output
nmap -oX scan_results.xml 192.168.1.1

# Grepable output
nmap -oG scan_results.gnmap 192.168.1.1

# All formats
nmap -oA scan_results 192.168.1.1
```

Verbose Output

Control the amount of information displayed.

```
# Verbose output
nmap -v 192.168.1.1

# Very verbose
nmap -vv 192.168.1.1

# Debug mode
nmap --packet-trace 192.168.1.1
```

Resume & Append

Continue or add to previous scans.

```
# Resume interrupted scan
nmap --resume scan_results.gnmap

# Append to existing file
nmap --append-output -oN existing_scan.txt 192.168.1.1
```

Live Results Processing

Combine Nmap output with command-line tools to extract useful insights.

```
# Extract live hosts
nmap -sn 192.168.1.0/24 | grep "Nmap scan report"

# Find web servers
nmap -p 80,443 --open 192.168.1.0/24 | grep "open"

# Export to CSV
nmap -oX - 192.168.1.1 | xsltproc --html -
```

Firewall Evasion Techniques

Packet Fragmentation: `nmap -f`

Bypass security measures using packet fragmentation, spoofed IPs, and stealthy scan methods.

```
# Fragment packets
nmap -f 192.168.1.1

# Custom MTU size
nmap --mtu 16 192.168.1.1

# Maximum transmission unit
nmap --mtu 24 192.168.1.1
```

Decoy Scanning: `nmap -D`

Hide your scan among decoy IP addresses.

```
# Use decoy IPs
nmap -D 192.168.1.100,192.168.1.101 192.168.1.1

# Random decoys
nmap -D RND:5 192.168.1.1

# Mix real and random decoys
nmap -D 192.168.1.100,RND:3 192.168.1.1
```

Source IP/Port Manipulation

Spoof source information.

```
# Spoof source IP
nmap -S 192.168.1.100 192.168.1.1

# Custom source port
nmap --source-port 53 192.168.1.1

# Random data length
nmap --data-length 25 192.168.1.1
```

Idle/Zombie Scan: `nmap -sI`

Use a zombie host to hide scan origin.

```
# Zombie scan (requires idle host)
nmap -sI zombie_host 192.168.1.1

# List idle candidates
nmap --script ipidseq 192.168.1.0/24
```

Advanced Scanning Options

DNS Resolution Control

Control how Nmap handles DNS lookups.

```
# Disable DNS resolution
nmap -n 192.168.1.1

# Force DNS resolution
nmap -R 192.168.1.1

# Custom DNS servers
nmap --dns-servers 8.8.8.8,1.1.1.1 192.168.1.1
```

IPv6 Scanning: `nmap -6`

Use these Nmap flags for additional functionality like IPv6 support.

```
# IPv6 scan
nmap -6 2001:db8::1

# IPv6 network scan
nmap -6 2001:db8::/32
```

Interface & Routing

Control network interface and routing.

```
# Specify network interface
nmap -e eth0 192.168.1.1

# Print interface and routes
nmap --iflist

# Traceroute
nmap --traceroute 192.168.1.1
```

Miscellaneous Options

Additional useful flags.

```
# Print version and exit
nmap --version

# Send on ethernet level
nmap --send-eth 192.168.1.1

# Send on IP level
nmap --send-ip 192.168.1.1
```

Real-World Examples

The following are real world examples of Nmap enumeration.

Network Discovery Workflow

Complete network enumeration process.

```
# Step 1: Discover live hosts
nmap -sn 192.168.1.0/24

# Step 2: Quick port scan
nmap -sS -T4 --top-ports 1000 192.168.1.0/24

# Step 3: Detailed scan of interesting hosts
nmap -sS -sV -sC -O 192.168.1.50

# Step 4: Comprehensive scan
nmap -p- -A -T4 192.168.1.50
```

Web Server Assessment

Focus on web services and vulnerabilities.

```
# Find web servers
nmap -sS -p 80,443,8080,8443 --open 192.168.1.0/24

# Enumerate HTTP services
nmap -sS -sV --script http-* 192.168.1.50

# Check for common vulnerabilities
nmap --script vuln -p 80,443 192.168.1.50
```

SMB/NetBIOS Enumeration

The following example enumerates Netbios on the target networks.

```
# SMB service detection
nmap -sV -p 139,445 192.168.1.0/24

# NetBIOS name discovery
nmap -sU --script nbstat -p 137 192.168.1.0/24

# SMB enumeration scripts
nmap --script smb-enum-* -p 445 192.168.1.50

# SMB vulnerability check
nmap --script smb-vuln-* -p 445 192.168.1.50
```

Stealth Assessment

Low-profile reconnaissance.

```
# Ultra-stealth scan
nmap -sS -T0 -f --data-length 200 -D RND:10 192.168.1.1

# Fragmented SYN scan
nmap -sS -f --mtu 8 -T1 192.168.1.1
```

Performance Optimization

Fast Scanning Strategies

Optimize scan speed for large networks.

```
# Fast network sweep
nmap -sS -T4 --min-rate 1000 --max-retries 1
192.168.1.0/24

# Parallel host scanning
nmap --min-hostgroup 50 --max-hostgroup 100
192.168.1.0/24

# Skip slow operations
nmap -sS -T4 --defeat-rst-ratelimit 192.168.1.0/24
```

Memory & Resource Management

Control resource usage for stability.

```
# Limit parallel probes
nmap --max-parallelism 10 192.168.1.0/24

# Control scan delays
nmap --scan-delay 100ms 192.168.1.1

# Set host timeout
nmap --host-timeout 10m 192.168.1.0/24
```

Reference: This cheatsheet covers essential Nmap commands and modern practices for network discovery and security auditing in cybersecurity workflows.