Advanced Nmap & NSE Quick Reference

OS & Version Detection

Operating System Detection

```bash
# Basic 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
```

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
```

NSE Script Categories

Default Scripts

```bash
# Run 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

```bash
```

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

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

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

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

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

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

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

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

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

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

Script Wildcards

bash

```bash
# All HTTP scripts
nmap --script="http-*" target.com

# All SMB scripts
nmap --script="smb-*" target.com

# All SQL scripts
nmap --script="*sql*" target.com

# All FTP scripts
nmap --script="ftp-*" target.com
```

Script Arguments

```bash
# HTTP form brute force with wordlists
nmap --script=http-form-brute \
 --script-args userdb=users.txt,passdb=passwords.txt \
 target.com

# SMB brute force
nmap --script=smb-brute \
 --script-args userdb=users.txt,passdb=pass.txt \
 -p 445 target.com

# SSH brute force
nmap --script=ssh-brute \
 --script-args userdb=users.txt,passdb=passwords.txt \
 -p 22 target.com
```

Popular NSE Scripts

```bash
```

```
# SMB enumeration
nmap --script=smb-enum-shares -p 445 target.com
nmap --script=smb-os-discovery -p 445 target.com
nmap --script=smb-enum-users -p 445 target.com

# FTP enumeration
nmap --script=ftp-anon -p 21 target.com
nmap --script=ftp-brute -p 21 target.com

# HTTP enumeration
nmap --script=http-title -p 80,443 target.com
nmap --script=http-headers -p 80,443 target.com
nmap --script=http-methods -p 80,443 target.com
nmap --script=http-robots.txt -p 80,443 target.com

# SSL/TLS testing
nmap --script=ssl-cert -p 443 target.com
nmap --script=ssl-enum-ciphers -p 443 target.com

# Database detection
nmap --script=mysql-info -p 3306 target.com
nmap --script=ms-sql-info -p 1433 target.com

# Vulnerability scanning
nmap --script=vuln target.com
nmap --script=http-vuln-* target.com
```

Firewall & IDS Evasion

Timing Templates

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)
```

Packet Fragmentation

```bash
# Fragment packets
nmap -f target.com

# 8-byte fragments
nmap -ff target.com

# Custom MTU (must be multiple of 8)
nmap --mtu 16 target.com
```

Decoy Scanning

```bash
# Random decoys
nmap -D RND:10 target.com

# Specific decoys (ME = your real IP)
nmap -D decoy1,decoy2,ME,decoy3 target.com

# Many random decoys
nmap -D RND:15 target.com
```

Source Port Spoofing

```bash
# Common source ports that bypass firewalls
nmap --source-port 53 target.com    # DNS
nmap --source-port 80 target.com    # HTTP
nmap --source-port 443 target.com   # HTTPS
nmap -g 53 target.com               # Short form
```

Other Evasion Techniques

```bash
```

```
# 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        # Apple vendor
nmap --spoof-mac 00:11:22:33:44:55 target.com

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

# Bad checksum (test firewall)
nmap --badsum target.com

# Custom scan delay
nmap --scan-delay 1s target.com
nmap --max-scan-delay 10s target.com

# Rate limiting
nmap --min-rate 100 target.com
nmap --max-rate 1000 target.com
```

Advanced Combinations

Comprehensive Scans

bash

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

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

# Stealth comprehensive
sudo nmap -sS -O -sV -sC -T2 target.com

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

# Only scan open ports
nmap --open target.com
```

Custom Timing

bash

```
# Custom timing options
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
```

Stealth Scanning

bash

```
# Maximum stealth scan
sudo nmap -sS -T0 -f -D RND:10 --source-port 53 target.com

# Moderate stealth
sudo nmap -sS -T2 -f target.com

# Bypass common firewall rules
nmap -f -D RND:5 --source-port 53 -T2 target.com
```

Script Management

Script Database

bash

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

# Find script location
ls /usr/share/nmap/scripts/ | grep http

# Get script help
nmap --script-help=http-title
nmap --script-help=smb-enum-shares

# Script categories location
ls /usr/share/nmap/scripts/
```

Script Debugging

bash

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

# Debug script execution
nmap -d --script=http-title target.com

# Verbose script output
nmap -v --script=vuln target.com
```

Real-World Scenarios

Web Server Assessment

```bash
# Complete web server analysis
nmap -p 80,443,8080,8443 --script=http-* target.com

# SSL/TLS assessment
nmap -p 443 --script=ssl-* target.com

# Web vulnerability scan
nmap -p 80,443 --script=http-vuln-* target.com
```

Windows Network Assessment

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

# Windows service detection
nmap -p 135,139,445,3389 -sV target.com

# Domain controller assessment
nmap -p 88,389,636,3268 --script=ldap-* target.com
```

Database Assessment

```bash
# Database service detection
nmap -p 1433,3306,5432,1521,27017 -sV target.com

# MySQL assessment
nmap -p 3306 --script=mysql-* target.com

# MSSQL assessment
nmap -p 1433 --script=ms-sql-* target.com
```

Network Infrastructure

```bash
# Network device detection
nmap -p 22,23,80,443,161 --script=snmp-*,http-* target.com

# Router/switch assessment
nmap --script=broadcast-* target-network

# SNMP enumeration
nmap -p 161 --script=snmp-* target.com
```

Troubleshooting

Common Issues & Solutions

```bash
# Permission denied for SYN scan
sudo nmap -sS target.com
# OR use TCP connect scan
nmap -sT target.com

# Scan too slow
nmap -T4 --top-ports 1000 target.com

# Host seems down
nmap -Pn target.com

# Firewall blocking
nmap -f -D RND:5 -T2 target.com

# Need specific interface
nmap -e eth0 target.com

# Scripts not found
sudo nmap --script-updatedb
```

Performance Optimization

```bash
# Limit scan scope
nmap --top-ports 100 target.com

# Increase timing
nmap -T4 target.com

# Parallel host scanning
nmap --min-hostgroup 64 target.com

# Reduce retries
nmap --max-retries 1 target.com

# Set timeouts
nmap --host-timeout 5m target.com
```

Pro Tips

Best Practices

- Always use `-T4` for faster scans unless stealth 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
- Test in controlled environments first

Legal & Ethical Considerations

- Only scan systems you own or have permission to test
- Some scripts can crash services or trigger alerts
- Intrusive and exploit scripts can cause damage

- DoS scripts can make services unavailable
- Always get written permission for penetration testing
- Follow responsible disclosure for vulnerabilities found

Script Categories by Risk Level

Safe: `safe`, `discovery`, `version`, `auth`
Moderate: `brute`, `vuln`
High Risk: `intrusive`, `exploit`, `dos`, `malware`

Use higher risk categories only in controlled test environments!