MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

PREMIUM PROFESSIONAL REFERENCE · 2026

Nmap Port Scanning & NSE Scripting Cheat Sheet

464 Command Field Guide

A structured command library for discovery, enumeration, NSE, output, timing, and authorized network assessment.

104	155	205
Basic	Intermediate	Expert

https://mnatech.in/ @mna_tech_academy +91 9216110094

How to use this guide

This reference is designed for legal labs, approved assessments, troubleshooting, and professional learning. Replace placeholders with systems you own or are explicitly authorized to test.

> **Authorization first:** Scanning, exploitation, interception, and administrative commands can disrupt services or expose data. Confirm written scope, use conservative rates, preserve evidence, and stop if impact appears.

Contents

01 · Basic — 104 Commands
Discovery, ports, output, service and OS fundamentals

02 · Intermediate — 155 Commands
Service-specific NSE, timing, exclusions and operational control

03 · Expert — 205 Commands
Advanced scan types, packet behavior, NSE selection and audit workflows

04 · Flag Decoder & Workflow
How to build a safe scan plan

05 · Official References
Primary documentation used for validation

01

Basic — 104 Commands

Discovery, ports, output, service and OS fundamentals

Basic 001 · Default TCP scan

```
nmap scanme.nmap.org
```

Scans the most common TCP ports using Nmap defaults.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 002 · Default TCP scan

```
nmap 192.0.2.10
```

Scans the most common TCP ports using Nmap defaults.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 003 · Default TCP scan

```
nmap 192.0.2.0/28
```

Scans the most common TCP ports using Nmap defaults.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 004 · Default TCP scan

```
nmap -iL targets.txt
```

Scans the most common TCP ports using Nmap defaults.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 005 · Host discovery only

```
nmap -sn scanme.nmap.org
```

Finds live hosts without a port scan.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 006 · Host discovery only

```
nmap -sn 192.0.2.10
```

Finds live hosts without a port scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 007 · Host discovery only

```
nmap -sn 192.0.2.0/28
```

Finds live hosts without a port scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 008 · Host discovery only

```
nmap -sn -iL targets.txt
```

Finds live hosts without a port scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 009 · Skip host discovery

```
nmap -Pn scanme.nmap.org
```

Treats targets as online when ping probes are blocked.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 010 · Skip host discovery

```
nmap -Pn 192.0.2.10
```

Treats targets as online when ping probes are blocked.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 011 · Skip host discovery

```
nmap -Pn 192.0.2.0/28
```

Treats targets as online when ping probes are blocked.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 012 · Skip host discovery

```
nmap -Pn -iL targets.txt
```

Treats targets as online when ping probes are blocked.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 013 · TCP connect scan

```
nmap -sT scanme.nmap.org
```

Uses the operating system connect call for a full TCP handshake.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 014 · TCP connect scan

```
nmap -sT 192.0.2.10
```

Uses the operating system connect call for a full TCP handshake.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 015 · TCP connect scan

```
nmap -sT 192.0.2.0/28
```

Uses the operating system connect call for a full TCP handshake.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 016 · TCP connect scan

```
nmap -sT -iL targets.txt
```

Uses the operating system connect call for a full TCP handshake.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 017 · TCP SYN scan

```
nmap -sS scanme.nmap.org
```

Performs a half-open SYN scan; typically requires elevated privileges.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 018 · TCP SYN scan

```
nmap -sS 192.0.2.10
```

Performs a half-open SYN scan; typically requires elevated privileges.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 019 · TCP SYN scan

```
nmap -sS 192.0.2.0/28
```

Performs a half-open SYN scan; typically requires elevated privileges.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 020 · TCP SYN scan

```
nmap -sS -iL targets.txt
```

Performs a half-open SYN scan; typically requires elevated privileges.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 021 · Top UDP services

```
nmap -sU --top-ports 20 scanme.nmap.org
```

Checks twenty common UDP ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 022 · Top UDP services

```
nmap -sU --top-ports 20 192.0.2.10
```

Checks twenty common UDP ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 023 · Top UDP services

```
nmap -sU --top-ports 20 192.0.2.0/28
```

Checks twenty common UDP ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 024 · Top UDP services

```
nmap -sU --top-ports 20 -iL targets.txt
```

Checks twenty common UDP ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 025 · Single port

```
nmap -p 80 scanme.nmap.org
```

Tests TCP port 80 only.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 026 · Single port

```
nmap -p 80 192.0.2.10
```

Tests TCP port 80 only.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 027 · Single port

```
nmap -p 80 192.0.2.0/28
```

Tests TCP port 80 only.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 028 · Single port

```
nmap -p 80 -iL targets.txt
```

Tests TCP port 80 only.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 029 · Selected ports

```
nmap -p 22,80,443 scanme.nmap.org
```

Tests a short explicit TCP port list.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 030 · Selected ports

```
nmap -p 22,80,443 192.0.2.10
```

Tests a short explicit TCP port list.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 031 · Selected ports

```
nmap -p 22,80,443 192.0.2.0/28
```

Tests a short explicit TCP port list.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 032 · Selected ports

```
nmap -p 22,80,443 -iL targets.txt
```

Tests a short explicit TCP port list.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 033 · Port range

```
nmap -p 1-1024 scanme.nmap.org
```

Scans the well-known TCP port range.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 034 · Port range

```
nmap -p 1-1024 192.0.2.10
```

Scans the well-known TCP port range.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 035 · Port range

```
nmap -p 1-1024 192.0.2.0/28
```

Scans the well-known TCP port range.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 036 · Port range

```
nmap -p 1-1024 -iL targets.txt
```

Scans the well-known TCP port range.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 037 · Top 100 ports

```
nmap --top-ports 100 scanme.nmap.org
```

Scans the 100 most frequently observed ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 038 · Top 100 ports

```
nmap --top-ports 100 192.0.2.10
```

Scans the 100 most frequently observed ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 039 · Top 100 ports

```
nmap --top-ports 100 192.0.2.0/28
```

Scans the 100 most frequently observed ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 040 · Top 100 ports

```
nmap --top-ports 100 -iL targets.txt
```

Scans the 100 most frequently observed ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 041 · Fast scan

```
nmap -F scanme.nmap.org
```

Scans Nmap's smaller fast-port set.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 042 · Fast scan

```
nmap -F 192.0.2.10
```

Scans Nmap's smaller fast-port set.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 043 · Fast scan

```
nmap -F 192.0.2.0/28
```

Scans Nmap's smaller fast-port set.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 044 · Fast scan

```
nmap -F -iL targets.txt
```

Scans Nmap's smaller fast-port set.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 045 · All TCP ports

```
nmap -p- scanme.nmap.org
```

Scans TCP ports 1 through 65535.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 046 · All TCP ports

```
nmap -p- 192.0.2.10
```

Scans TCP ports 1 through 65535.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 047 · All TCP ports

```
nmap -p- 192.0.2.0/28
```

Scans TCP ports 1 through 65535.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 048 · All TCP ports

```
nmap -p- -iL targets.txt
```

Scans TCP ports 1 through 65535.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 049 · Service detection

```
nmap -sV scanme.nmap.org
```

Probes open ports to identify services and versions.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 050 · Service detection

```
nmap -sV 192.0.2.10
```

Probes open ports to identify services and versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 051 · Service detection

```
nmap -sV 192.0.2.0/28
```

Probes open ports to identify services and versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 052 · Service detection

```
nmap -sV -iL targets.txt
```

Probes open ports to identify services and versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 053 · OS detection

```
nmap -O scanme.nmap.org
```

Attempts operating-system fingerprinting.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 054 · OS detection

```
nmap -O 192.0.2.10
```

Attempts operating-system fingerprinting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 055 · OS detection

```
nmap -O 192.0.2.0/28
```

Attempts operating-system fingerprinting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 056 · OS detection

```
nmap -O -iL targets.txt
```

Attempts operating-system fingerprinting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 057 · Aggressive detection

```
nmap -A scanme.nmap.org
```

Enables OS, version, default scripts, and traceroute.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 058 · Aggressive detection

```
nmap -A 192.0.2.10
```

Enables OS, version, default scripts, and traceroute.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 059 · Aggressive detection

```
nmap -A 192.0.2.0/28
```

Enables OS, version, default scripts, and traceroute.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 060 · Aggressive detection

```
nmap -A -iL targets.txt
```

Enables OS, version, default scripts, and traceroute.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 061 · Default NSE scripts

```
nmap -sC scanme.nmap.org
```

Runs NSE scripts in the default category.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 062 · Default NSE scripts

```
nmap -sC 192.0.2.10
```

Runs NSE scripts in the default category.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 063 · Default NSE scripts

```
nmap -sC 192.0.2.0/28
```

Runs NSE scripts in the default category.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 064 · Default NSE scripts

```
nmap -sC -iL targets.txt
```

Runs NSE scripts in the default category.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 065 · Verbose output

```
nmap -v scanme.nmap.org
```

Shows more progress and result detail.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 066 · Verbose output

```
nmap -v 192.0.2.10
```

Shows more progress and result detail.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 067 · Verbose output

```
nmap -v 192.0.2.0/28
```

Shows more progress and result detail.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 068 · Verbose output

```
nmap -v -iL targets.txt
```

Shows more progress and result detail.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 069 · Extra verbose output

```
nmap -vv scanme.nmap.org
```

Shows even more scan progress and reasoning.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 070 · Extra verbose output

```
nmap -vv 192.0.2.10
```

Shows even more scan progress and reasoning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 071 · Extra verbose output

```
nmap -vv 192.0.2.0/28
```

Shows even more scan progress and reasoning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 072 · Extra verbose output

```
nmap -vv -iL targets.txt
```

Shows even more scan progress and reasoning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 073 · No DNS resolution

```
nmap -n scanme.nmap.org
```

Avoids reverse DNS lookup for faster predictable scans.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 074 · No DNS resolution

```
nmap -n 192.0.2.10
```

Avoids reverse DNS lookup for faster predictable scans.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 075 · No DNS resolution

```
nmap -n 192.0.2.0/28
```

Avoids reverse DNS lookup for faster predictable scans.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 076 · No DNS resolution

```
nmap -n -iL targets.txt
```

Avoids reverse DNS lookup for faster predictable scans.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 077 · Always resolve DNS

```
nmap -R scanme.nmap.org
```

Forces reverse DNS resolution for targets.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 078 · Always resolve DNS

```
nmap -R 192.0.2.10
```

Forces reverse DNS resolution for targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 079 · Always resolve DNS

```
nmap -R 192.0.2.0/28
```

Forces reverse DNS resolution for targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 080 · Always resolve DNS

```
nmap -R -iL targets.txt
```

Forces reverse DNS resolution for targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 081 · Show open ports

```
nmap --open scanme.nmap.org
```

Suppresses closed and filtered ports from final output.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 082 · Show open ports

```
nmap --open 192.0.2.10
```

Suppresses closed and filtered ports from final output.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 083 · Show open ports

```
nmap --open 192.0.2.0/28
```

Suppresses closed and filtered ports from final output.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 084 · Show open ports

```
nmap --open -iL targets.txt
```

Suppresses closed and filtered ports from final output.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 085 · Show state reason

```
nmap --reason scanme.nmap.org
```

Displays why Nmap assigned each host or port state.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 086 · Show state reason

```
nmap --reason 192.0.2.10
```

Displays why Nmap assigned each host or port state.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 087 · Show state reason

```
nmap --reason 192.0.2.0/28
```

Displays why Nmap assigned each host or port state.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 088 · Show state reason

```
nmap --reason -iL targets.txt
```

Displays why Nmap assigned each host or port state.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 089 · Normal output

```
nmap -oN scan.txt scanme.nmap.org
```

Saves human-readable results to scan.txt.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 090 · Normal output

```
nmap -oN scan.txt 192.0.2.10
```

Saves human-readable results to scan.txt.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 091 · Normal output

```
nmap -oN scan.txt 192.0.2.0/28
```

Saves human-readable results to scan.txt.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 092 · Normal output

```
nmap -oN scan.txt -iL targets.txt
```

Saves human-readable results to scan.txt.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 093 · XML output

```
nmap -oX scan.xml scanme.nmap.org
```

Saves structured XML for tools and automation.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 094 · XML output

```
nmap -oX scan.xml 192.0.2.10
```

Saves structured XML for tools and automation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 095 · XML output

```
nmap -oX scan.xml 192.0.2.0/28
```

Saves structured XML for tools and automation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 096 · XML output

```
nmap -oX scan.xml -iL targets.txt
```

Saves structured XML for tools and automation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 097 · All major outputs

```
nmap -oA baseline scanme.nmap.org
```

Writes normal, XML, and grepable files using one basename.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 098 · All major outputs

```
nmap -oA baseline 192.0.2.10
```

Writes normal, XML, and grepable files using one basename.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 099 · All major outputs

```
nmap -oA baseline 192.0.2.0/28
```

Writes normal, XML, and grepable files using one basename.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 100 · All major outputs

```
nmap -oA baseline -iL targets.txt
```

Writes normal, XML, and grepable files using one basename.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 101 · List interfaces and routes

```
nmap --iflist scanme.nmap.org
```

Shows interfaces and routing information before choosing a target.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Basic 102 · List interfaces and routes

```
nmap --iflist 192.0.2.10
```

Shows interfaces and routing information before choosing a target.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 103 · List interfaces and routes

```
nmap --iflist 192.0.2.0/28
```

Shows interfaces and routing information before choosing a target.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Basic 104 · List interfaces and routes

```
nmap --iflist -iL targets.txt
```

Shows interfaces and routing information before choosing a target.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

02

Intermediate — 155 Commands

Service-specific NSE, timing, exclusions and operational control

Intermediate 001 · Measured SYN and version scan

```
nmap -sS -sV -T3 scanme.nmap.org
```

Balances service discovery with moderate timing.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 002 · Measured SYN and version scan

```
nmap -sS -sV -T3 192.0.2.10
```

Balances service discovery with moderate timing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 003 · Measured SYN and version scan

```
nmap -sS -sV -T3 192.0.2.0/28
```

Balances service discovery with moderate timing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 004 · Measured SYN and version scan

```
nmap -sS -sV -T3 198.51.100.0/28
```

Balances service discovery with moderate timing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 005 · Measured SYN and version scan

```
nmap -sS -sV -T3 -iL targets.txt
```

Balances service discovery with moderate timing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 006 · UDP version survey

```
nmap -sU -sV --top-ports 50 scanme.nmap.org
```

Probes common UDP services and their versions.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 007 · UDP version survey

```
nmap -sU -sV --top-ports 50 192.0.2.10
```

Probes common UDP services and their versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 008 · UDP version survey

```
nmap -sU -sV --top-ports 50 192.0.2.0/28
```

Probes common UDP services and their versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 009 · UDP version survey

```
nmap -sU -sV --top-ports 50 198.51.100.0/28
```

Probes common UDP services and their versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 010 · UDP version survey

```
nmap -sU -sV --top-ports 50 -iL targets.txt
```

Probes common UDP services and their versions.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 011 · HTTP title collection

```
nmap -p 80,443 --script http-title scanme.nmap.org
```

Collects page titles from approved web services.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 012 · HTTP title collection

```
nmap -p 80,443 --script http-title 192.0.2.10
```

Collects page titles from approved web services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 013 · HTTP title collection

```
nmap -p 80,443 --script http-title 192.0.2.0/28
```

Collects page titles from approved web services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 014 · HTTP title collection

```
nmap -p 80,443 --script http-title 198.51.100.0/28
```

Collects page titles from approved web services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 015 · HTTP title collection

```
nmap -p 80,443 --script http-title -iL targets.txt
```

Collects page titles from approved web services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 016 · HTTP header review

```
nmap -p 80,443 --script http-headers scanme.nmap.org
```

Retrieves response headers for configuration review.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 017 · HTTP header review

```
nmap -p 80,443 --script http-headers 192.0.2.10
```

Retrieves response headers for configuration review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 018 · HTTP header review

```
nmap -p 80,443 --script http-headers 192.0.2.0/28
```

Retrieves response headers for configuration review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 019 · HTTP header review

```
nmap -p 80,443 --script http-headers 198.51.100.0/28
```

Retrieves response headers for configuration review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 020 · HTTP header review

```
nmap -p 80,443 --script http-headers -iL targets.txt
```

Retrieves response headers for configuration review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 021 · TLS certificate review

```
nmap -p 443 --script ssl-cert scanme.nmap.org
```

Displays certificate subject, issuer, validity, and names.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 022 · TLS certificate review

```
nmap -p 443 --script ssl-cert 192.0.2.10
```

Displays certificate subject, issuer, validity, and names.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 023 · TLS certificate review

```
nmap -p 443 --script ssl-cert 192.0.2.0/28
```

Displays certificate subject, issuer, validity, and names.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 024 · TLS certificate review

```
nmap -p 443 --script ssl-cert 198.51.100.0/28
```

Displays certificate subject, issuer, validity, and names.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 025 · TLS certificate review

```
nmap -p 443 --script ssl-cert -iL targets.txt
```

Displays certificate subject, issuer, validity, and names.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 026 · TLS cipher inventory

```
nmap -p 443 --script ssl-enum-ciphers scanme.nmap.org
```

Enumerates supported TLS protocols and cipher suites.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 027 · TLS cipher inventory

```
nmap -p 443 --script ssl-enum-ciphers 192.0.2.10
```

Enumerates supported TLS protocols and cipher suites.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 028 · TLS cipher inventory

```
nmap -p 443 --script ssl-enum-ciphers 192.0.2.0/28
```

Enumerates supported TLS protocols and cipher suites.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 029 · TLS cipher inventory

```
nmap -p 443 --script ssl-enum-ciphers 198.51.100.0/28
```

Enumerates supported TLS protocols and cipher suites.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 030 · TLS cipher inventory

```
nmap -p 443 --script ssl-enum-ciphers -iL targets.txt
```

Enumerates supported TLS protocols and cipher suites.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 031 · SSH algorithm inventory

```
nmap -p 22 --script ssh2-enum-algos scanme.nmap.org
```

Lists supported SSH algorithms for hardening review.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 032 · SSH algorithm inventory

```
nmap -p 22 --script ssh2-enum-algos 192.0.2.10
```

Lists supported SSH algorithms for hardening review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 033 · SSH algorithm inventory

```
nmap -p 22 --script ssh2-enum-algos 192.0.2.0/28
```

Lists supported SSH algorithms for hardening review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 034 · SSH algorithm inventory

```
nmap -p 22 --script ssh2-enum-algos 198.51.100.0/28
```

Lists supported SSH algorithms for hardening review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 035 · SSH algorithm inventory

```
nmap -p 22 --script ssh2-enum-algos -iL targets.txt
```

Lists supported SSH algorithms for hardening review.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 036 · Anonymous FTP check

```
nmap -p 21 --script ftp-anon scanme.nmap.org
```

Checks whether an FTP service permits anonymous login.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 037 · Anonymous FTP check

```
nmap -p 21 --script ftp-anon 192.0.2.10
```

Checks whether an FTP service permits anonymous login.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 038 · Anonymous FTP check

```
nmap -p 21 --script ftp-anon 192.0.2.0/28
```

Checks whether an FTP service permits anonymous login.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 039 · Anonymous FTP check

```
nmap -p 21 --script ftp-anon 198.51.100.0/28
```

Checks whether an FTP service permits anonymous login.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 040 · Anonymous FTP check

```
nmap -p 21 --script ftp-anon -iL targets.txt
```

Checks whether an FTP service permits anonymous login.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 041 · SMB protocol review

```
nmap -p 445 --script smb-protocols scanme.nmap.org
```

Identifies supported SMB dialects.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 042 · SMB protocol review

```
nmap -p 445 --script smb-protocols 192.0.2.10
```

Identifies supported SMB dialects.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 043 · SMB protocol review

```
nmap -p 445 --script smb-protocols 192.0.2.0/28
```

Identifies supported SMB dialects.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 044 · SMB protocol review

```
nmap -p 445 --script smb-protocols 198.51.100.0/28
```

Identifies supported SMB dialects.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 045 · SMB protocol review

```
nmap -p 445 --script smb-protocols -iL targets.txt
```

Identifies supported SMB dialects.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 046 · SMB signing review

```
nmap -p 445 --script smb2-security-mode scanme.nmap.org
```

Checks SMB2 signing configuration.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 047 · SMB signing review

```
nmap -p 445 --script smb2-security-mode 192.0.2.10
```

Checks SMB2 signing configuration.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 048 · SMB signing review

```
nmap -p 445 --script smb2-security-mode 192.0.2.0/28
```

Checks SMB2 signing configuration.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 049 · SMB signing review

```
nmap -p 445 --script smb2-security-mode 198.51.100.0/28
```

Checks SMB2 signing configuration.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 050 · SMB signing review

```
nmap -p 445 --script smb2-security-mode -iL targets.txt
```

Checks SMB2 signing configuration.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 051 · DNS recursion review

```
nmap -p 53 --script dns-recursion scanme.nmap.org
```

Checks whether a DNS server appears to allow recursion.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 052 · DNS recursion review

```
nmap -p 53 --script dns-recursion 192.0.2.10
```

Checks whether a DNS server appears to allow recursion.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 053 · DNS recursion review

```
nmap -p 53 --script dns-recursion 192.0.2.0/28
```

Checks whether a DNS server appears to allow recursion.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 054 · DNS recursion review

```
nmap -p 53 --script dns-recursion 198.51.100.0/28
```

Checks whether a DNS server appears to allow recursion.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 055 · DNS recursion review

```
nmap -p 53 --script dns-recursion -iL targets.txt
```

Checks whether a DNS server appears to allow recursion.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 056 · SMTP capability review

```
nmap -p 25 --script smtp-commands scanme.nmap.org
```

Enumerates advertised SMTP commands.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 057 · SMTP capability review

```
nmap -p 25 --script smtp-commands 192.0.2.10
```

Enumerates advertised SMTP commands.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 058 · SMTP capability review

```
nmap -p 25 --script smtp-commands 192.0.2.0/28
```

Enumerates advertised SMTP commands.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 059 · SMTP capability review

```
nmap -p 25 --script smtp-commands 198.51.100.0/28
```

Enumerates advertised SMTP commands.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 060 · SMTP capability review

```
nmap -p 25 --script smtp-commands -iL targets.txt
```

Enumerates advertised SMTP commands.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 061 · Mail banner collection

```
nmap -p 110,143,993,995 --script banner scanme.nmap.org
```

Collects service banners from common mail ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 062 · Mail banner collection

```
nmap -p 110,143,993,995 --script banner 192.0.2.10
```

Collects service banners from common mail ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 063 · Mail banner collection

```
nmap -p 110,143,993,995 --script banner 192.0.2.0/28
```

Collects service banners from common mail ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 064 · Mail banner collection

```
nmap -p 110,143,993,995 --script banner 198.51.100.0/28
```

Collects service banners from common mail ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 065 · Mail banner collection

```
nmap -p 110,143,993,995 --script banner -iL targets.txt
```

Collects service banners from common mail ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 066 · Light version detection

```
nmap -sV --version-light scanme.nmap.org
```

Uses fewer probes to reduce time and traffic.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 067 · Light version detection

```
nmap -sV --version-light 192.0.2.10
```

Uses fewer probes to reduce time and traffic.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 068 · Light version detection

```
nmap -sV --version-light 192.0.2.0/28
```

Uses fewer probes to reduce time and traffic.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 069 · Light version detection

```
nmap -sV --version-light 198.51.100.0/28
```

Uses fewer probes to reduce time and traffic.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 070 · Light version detection

```
nmap -sV --version-light -iL targets.txt
```

Uses fewer probes to reduce time and traffic.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 071 · Full version detection

```
nmap -sV --version-all scanme.nmap.org
```

Uses every version probe for difficult services.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 072 · Full version detection

```
nmap -sV --version-all 192.0.2.10
```

Uses every version probe for difficult services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 073 · Full version detection

```
nmap -sV --version-all 192.0.2.0/28
```

Uses every version probe for difficult services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 074 · Full version detection

```
nmap -sV --version-all 198.51.100.0/28
```

Uses every version probe for difficult services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 075 · Full version detection

```
nmap -sV --version-all -iL targets.txt
```

Uses every version probe for difficult services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 076 · Balanced version intensity

```
nmap -sV --version-intensity 5 scanme.nmap.org
```

Controls how many probes service detection attempts.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 077 · Balanced version intensity

```
nmap -sV --version-intensity 5 192.0.2.10
```

Controls how many probes service detection attempts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 078 · Balanced version intensity

```
nmap -sV --version-intensity 5 192.0.2.0/28
```

Controls how many probes service detection attempts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 079 · Balanced version intensity

```
nmap -sV --version-intensity 5 198.51.100.0/28
```

Controls how many probes service detection attempts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 080 · Balanced version intensity

```
nmap -sV --version-intensity 5 -iL targets.txt
```

Controls how many probes service detection attempts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 081 · Polite timing

```
nmap -T2 scanme.nmap.org
```

Reduces scan speed and network load.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 082 · Polite timing

```
nmap -T2 192.0.2.10
```

Reduces scan speed and network load.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 083 · Polite timing

```
nmap -T2 192.0.2.0/28
```

Reduces scan speed and network load.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 084 · Polite timing

```
nmap -T2 198.51.100.0/28
```

Reduces scan speed and network load.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 085 · Polite timing

```
nmap -T2 -iL targets.txt
```

Reduces scan speed and network load.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 086 · Normal timing

```
nmap -T3 scanme.nmap.org
```

Uses a balanced timing profile.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 087 · Normal timing

```
nmap -T3 192.0.2.10
```

Uses a balanced timing profile.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 088 · Normal timing

```
nmap -T3 192.0.2.0/28
```

Uses a balanced timing profile.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 089 · Normal timing

```
nmap -T3 198.51.100.0/28
```

Uses a balanced timing profile.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 090 · Normal timing

```
nmap -T3 -iL targets.txt
```

Uses a balanced timing profile.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 091 · Faster timing

```
nmap -T4 scanme.nmap.org
```

Uses aggressive timing on reliable authorized networks.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 092 · Faster timing

```
nmap -T4 192.0.2.10
```

Uses aggressive timing on reliable authorized networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 093 · Faster timing

```
nmap -T4 192.0.2.0/28
```

Uses aggressive timing on reliable authorized networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 094 · Faster timing

```
nmap -T4 198.51.100.0/28
```

Uses aggressive timing on reliable authorized networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 095 · Faster timing

```
nmap -T4 -iL targets.txt
```

Uses aggressive timing on reliable authorized networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 096 · Cap packet rate

```
nmap --max-rate 100 scanme.nmap.org
```

Limits packets per second to reduce impact.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 097 · Cap packet rate

```
nmap --max-rate 100 192.0.2.10
```

Limits packets per second to reduce impact.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 098 · Cap packet rate

```
nmap --max-rate 100 192.0.2.0/28
```

Limits packets per second to reduce impact.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 099 · Cap packet rate

```
nmap --max-rate 100 198.51.100.0/28
```

Limits packets per second to reduce impact.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 100 · Cap packet rate

```
nmap --max-rate 100 -iL targets.txt
```

Limits packets per second to reduce impact.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 101 · Minimum packet rate

```
nmap --min-rate 50 scanme.nmap.org
```

Requests a minimum send rate on stable lab networks.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 102 · Minimum packet rate

```
nmap --min-rate 50 192.0.2.10
```

Requests a minimum send rate on stable lab networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 103 · Minimum packet rate

```
nmap --min-rate 50 192.0.2.0/28
```

Requests a minimum send rate on stable lab networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 104 · Minimum packet rate

```
nmap --min-rate 50 198.51.100.0/28
```

Requests a minimum send rate on stable lab networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 105 · Minimum packet rate

```
nmap --min-rate 50 -iL targets.txt
```

Requests a minimum send rate on stable lab networks.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 106 · Limit retries

```
nmap --max-retries 2 scanme.nmap.org
```

Reduces repeat probes when speed matters.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 107 · Limit retries

```
nmap --max-retries 2 192.0.2.10
```

Reduces repeat probes when speed matters.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 108 · Limit retries

```
nmap --max-retries 2 192.0.2.0/28
```

Reduces repeat probes when speed matters.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 109 · Limit retries

```
nmap --max-retries 2 198.51.100.0/28
```

Reduces repeat probes when speed matters.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 110 · Limit retries

```
nmap --max-retries 2 -iL targets.txt
```

Reduces repeat probes when speed matters.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 111 · Per-host timeout

```
nmap --host-timeout 5m scanme.nmap.org
```

Stops spending time on a host after five minutes.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 112 · Per-host timeout

```
nmap --host-timeout 5m 192.0.2.10
```

Stops spending time on a host after five minutes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 113 · Per-host timeout

```
nmap --host-timeout 5m 192.0.2.0/28
```

Stops spending time on a host after five minutes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 114 · Per-host timeout

```
nmap --host-timeout 5m 198.51.100.0/28
```

Stops spending time on a host after five minutes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 115 · Per-host timeout

```
nmap --host-timeout 5m -iL targets.txt
```

Stops spending time on a host after five minutes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 116 · Delay probes

```
nmap --scan-delay 200ms scanme.nmap.org
```

Adds a delay between probes for fragile services.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 117 · Delay probes

```
nmap --scan-delay 200ms 192.0.2.10
```

Adds a delay between probes for fragile services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 118 · Delay probes

```
nmap --scan-delay 200ms 192.0.2.0/28
```

Adds a delay between probes for fragile services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 119 · Delay probes

```
nmap --scan-delay 200ms 198.51.100.0/28
```

Adds a delay between probes for fragile services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 120 · Delay probes

```
nmap --scan-delay 200ms -iL targets.txt
```

Adds a delay between probes for fragile services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 121 · Exclude one host

```
nmap --exclude 192.0.2.5 scanme.nmap.org
```

Keeps an explicitly excluded system out of the scan.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 122 · Exclude one host

```
nmap --exclude 192.0.2.5 192.0.2.10
```

Keeps an explicitly excluded system out of the scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 123 · Exclude one host

```
nmap --exclude 192.0.2.5 192.0.2.0/28
```

Keeps an explicitly excluded system out of the scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 124 · Exclude one host

```
nmap --exclude 192.0.2.5 198.51.100.0/28
```

Keeps an explicitly excluded system out of the scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 125 · Exclude one host

```
nmap --exclude 192.0.2.5 -iL targets.txt
```

Keeps an explicitly excluded system out of the scan.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 126 · Exclude host list

```
nmap --exclude 192.0.2.5,192.0.2.6 scanme.nmap.org
```

Protects multiple out-of-scope systems.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 127 · Exclude host list

```
nmap --exclude 192.0.2.5,192.0.2.6 192.0.2.10
```

Protects multiple out-of-scope systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 128 · Exclude host list

```
nmap --exclude 192.0.2.5,192.0.2.6 192.0.2.0/28
```

Protects multiple out-of-scope systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 129 · Exclude host list

```
nmap --exclude 192.0.2.5,192.0.2.6 198.51.100.0/28
```

Protects multiple out-of-scope systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 130 · Exclude host list

```
nmap --exclude 192.0.2.5,192.0.2.6 -iL targets.txt
```

Protects multiple out-of-scope systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 131 · Trace network path

```
nmap --traceroute scanme.nmap.org
```

Adds route information after scanning.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 132 · Trace network path

```
nmap --traceroute 192.0.2.10
```

Adds route information after scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 133 · Trace network path

```
nmap --traceroute 192.0.2.0/28
```

Adds route information after scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 134 · Trace network path

```
nmap --traceroute 198.51.100.0/28
```

Adds route information after scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 135 · Trace network path

```
nmap --traceroute -iL targets.txt
```

Adds route information after scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 136 · IPv6 scan

```
nmap -6 scanme.nmap.org
```

Enables scanning of IPv6 targets.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 137 · IPv6 scan

```
nmap -6 192.0.2.10
```

Enables scanning of IPv6 targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 138 · IPv6 scan

```
nmap -6 192.0.2.0/28
```

Enables scanning of IPv6 targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 139 · IPv6 scan

```
nmap -6 198.51.100.0/28
```

Enables scanning of IPv6 targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 140 · IPv6 scan

```
nmap -6 -iL targets.txt
```

Enables scanning of IPv6 targets.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 141 · Choose interface

```
nmap -e eth0 scanme.nmap.org
```

Sends probes using a specified local interface.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 142 · Choose interface

```
nmap -e eth0 192.0.2.10
```

Sends probes using a specified local interface.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 143 · Choose interface

```
nmap -e eth0 192.0.2.0/28
```

Sends probes using a specified local interface.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 144 · Choose interface

```
nmap -e eth0 198.51.100.0/28
```

Sends probes using a specified local interface.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 145 · Choose interface

```
nmap -e eth0 -iL targets.txt
```

Sends probes using a specified local interface.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 146 · Choose DNS resolver

```
nmap --dns-servers 192.0.2.53 scanme.nmap.org
```

Uses an approved resolver for DNS lookups.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 147 · Choose DNS resolver

```
nmap --dns-servers 192.0.2.53 192.0.2.10
```

Uses an approved resolver for DNS lookups.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 148 · Choose DNS resolver

```
nmap --dns-servers 192.0.2.53 192.0.2.0/28
```

Uses an approved resolver for DNS lookups.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 149 · Choose DNS resolver

```
nmap --dns-servers 192.0.2.53 198.51.100.0/28
```

Uses an approved resolver for DNS lookups.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 150 · Choose DNS resolver

```
nmap --dns-servers 192.0.2.53 -iL targets.txt
```

Uses an approved resolver for DNS lookups.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 151 · Periodic progress

```
nmap --stats-every 15s scanme.nmap.org
```

Prints scan statistics every fifteen seconds.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Intermediate 152 · Periodic progress

```
nmap --stats-every 15s 192.0.2.10
```

Prints scan statistics every fifteen seconds.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 153 · Periodic progress

```
nmap --stats-every 15s 192.0.2.0/28
```

Prints scan statistics every fifteen seconds.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 154 · Periodic progress

```
nmap --stats-every 15s 198.51.100.0/28
```

Prints scan statistics every fifteen seconds.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Intermediate 155 · Periodic progress

```
nmap --stats-every 15s -iL targets.txt
```

Prints scan statistics every fifteen seconds.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

03

Expert — 205 Commands

Advanced scan types, packet behavior, NSE selection and audit workflows

Expert 001 · Mixed TCP and UDP scan

```
nmap -sS -sU -p T:22,80,443,U:53,161 scanme.nmap.org
```

Scans explicit TCP and UDP services in one run.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 002 · Mixed TCP and UDP scan

```
nmap -sS -sU -p T:22,80,443,U:53,161 192.0.2.10
```

Scans explicit TCP and UDP services in one run.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 003 · Mixed TCP and UDP scan

```
nmap -sS -sU -p T:22,80,443,U:53,161 192.0.2.0/28
```

Scans explicit TCP and UDP services in one run.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 004 · Mixed TCP and UDP scan

```
nmap -sS -sU -p T:22,80,443,U:53,161 198.51.100.0/28
```

Scans explicit TCP and UDP services in one run.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 005 · Mixed TCP and UDP scan

```
nmap -sS -sU -p T:22,80,443,U:53,161 -iL targets.txt
```

Scans explicit TCP and UDP services in one run.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 006 · TCP ACK scan

```
nmap -sA scanme.nmap.org
```

Maps filtering behavior; it does not identify open ports directly.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 007 · TCP ACK scan

```
nmap -sA 192.0.2.10
```

Maps filtering behavior; it does not identify open ports directly.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 008 · TCP ACK scan

```
nmap -sA 192.0.2.0/28
```

Maps filtering behavior; it does not identify open ports directly.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 009 · TCP ACK scan

```
nmap -sA 198.51.100.0/28
```

Maps filtering behavior; it does not identify open ports directly.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 010 · TCP ACK scan

```
nmap -sA -iL targets.txt
```

Maps filtering behavior; it does not identify open ports directly.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 011 · TCP window scan

```
nmap -sW scanme.nmap.org
```

Uses TCP window differences where supported to infer states.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 012 · TCP window scan

```
nmap -sW 192.0.2.10
```

Uses TCP window differences where supported to infer states.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 013 · TCP window scan

```
nmap -sW 192.0.2.0/28
```

Uses TCP window differences where supported to infer states.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 014 · TCP window scan

```
nmap -sW 198.51.100.0/28
```

Uses TCP window differences where supported to infer states.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 015 · TCP window scan

```
nmap -sW -iL targets.txt
```

Uses TCP window differences where supported to infer states.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 016 · TCP Maimon scan

```
nmap -sM scanme.nmap.org
```

Uses FIN/ACK probes for specialized firewall research.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 017 · TCP Maimon scan

```
nmap -sM 192.0.2.10
```

Uses FIN/ACK probes for specialized firewall research.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 018 · TCP Maimon scan

```
nmap -sM 192.0.2.0/28
```

Uses FIN/ACK probes for specialized firewall research.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 019 · TCP Maimon scan

```
nmap -sM 198.51.100.0/28
```

Uses FIN/ACK probes for specialized firewall research.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 020 · TCP Maimon scan

```
nmap -sM -iL targets.txt
```

Uses FIN/ACK probes for specialized firewall research.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 021 · TCP null scan

```
nmap -sN scanme.nmap.org
```

Sends packets with no TCP flags for RFC-based state inference.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 022 · TCP null scan

```
nmap -sN 192.0.2.10
```

Sends packets with no TCP flags for RFC-based state inference.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 023 · TCP null scan

```
nmap -sN 192.0.2.0/28
```

Sends packets with no TCP flags for RFC-based state inference.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 024 · TCP null scan

```
nmap -sN 198.51.100.0/28
```

Sends packets with no TCP flags for RFC-based state inference.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 025 · TCP null scan

```
nmap -sN -iL targets.txt
```

Sends packets with no TCP flags for RFC-based state inference.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 026 · TCP FIN scan

```
nmap -sF scanme.nmap.org
```

Uses FIN probes; behavior varies across operating systems.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 027 · TCP FIN scan

```
nmap -sF 192.0.2.10
```

Uses FIN probes; behavior varies across operating systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 028 · TCP FIN scan

```
nmap -sF 192.0.2.0/28
```

Uses FIN probes; behavior varies across operating systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 029 · TCP FIN scan

```
nmap -sF 198.51.100.0/28
```

Uses FIN probes; behavior varies across operating systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 030 · TCP FIN scan

```
nmap -sF -iL targets.txt
```

Uses FIN probes; behavior varies across operating systems.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 031 · TCP Xmas scan

```
nmap -sX scanme.nmap.org
```

Sets FIN, PSH, and URG flags for stack-response analysis.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 032 · TCP Xmas scan

```
nmap -sX 192.0.2.10
```

Sets FIN, PSH, and URG flags for stack-response analysis.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 033 · TCP Xmas scan

```
nmap -sX 192.0.2.0/28
```

Sets FIN, PSH, and URG flags for stack-response analysis.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 034 · TCP Xmas scan

```
nmap -sX 198.51.100.0/28
```

Sets FIN, PSH, and URG flags for stack-response analysis.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 035 · TCP Xmas scan

```
nmap -sX -iL targets.txt
```

Sets FIN, PSH, and URG flags for stack-response analysis.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 036 · Idle scan

```
nmap -sI zombie.example:80 scanme.nmap.org
```

Uses an approved idle host to perform specialized blind scanning.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 037 · Idle scan

```
nmap -sI zombie.example:80 192.0.2.10
```

Uses an approved idle host to perform specialized blind scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 038 · Idle scan

```
nmap -sI zombie.example:80 192.0.2.0/28
```

Uses an approved idle host to perform specialized blind scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 039 · Idle scan

```
nmap -sI zombie.example:80 198.51.100.0/28
```

Uses an approved idle host to perform specialized blind scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 040 · Idle scan

```
nmap -sI zombie.example:80 -iL targets.txt
```

Uses an approved idle host to perform specialized blind scanning.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 041 · IP protocol scan

```
nmap -sO scanme.nmap.org
```

Identifies supported IP protocols rather than transport ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 042 · IP protocol scan

```
nmap -sO 192.0.2.10
```

Identifies supported IP protocols rather than transport ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 043 · IP protocol scan

```
nmap -sO 192.0.2.0/28
```

Identifies supported IP protocols rather than transport ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 044 · IP protocol scan

```
nmap -sO 198.51.100.0/28
```

Identifies supported IP protocols rather than transport ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 045 · IP protocol scan

```
nmap -sO -iL targets.txt
```

Identifies supported IP protocols rather than transport ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 046 · ARP discovery

```
nmap -PR -sn scanme.nmap.org
```

Uses ARP for local Ethernet host discovery.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 047 · ARP discovery

```
nmap -PR -sn 192.0.2.10
```

Uses ARP for local Ethernet host discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 048 · ARP discovery

```
nmap -PR -sn 192.0.2.0/28
```

Uses ARP for local Ethernet host discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 049 · ARP discovery

```
nmap -PR -sn 198.51.100.0/28
```

Uses ARP for local Ethernet host discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 050 · ARP discovery

```
nmap -PR -sn -iL targets.txt
```

Uses ARP for local Ethernet host discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 051 · ICMP echo discovery

```
nmap -PE -sn scanme.nmap.org
```

Uses ICMP echo requests for discovery.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 052 · ICMP echo discovery

```
nmap -PE -sn 192.0.2.10
```

Uses ICMP echo requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 053 · ICMP echo discovery

```
nmap -PE -sn 192.0.2.0/28
```

Uses ICMP echo requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 054 · ICMP echo discovery

```
nmap -PE -sn 198.51.100.0/28
```

Uses ICMP echo requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 055 · ICMP echo discovery

```
nmap -PE -sn -iL targets.txt
```

Uses ICMP echo requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 056 · ICMP timestamp discovery

```
nmap -PP -sn scanme.nmap.org
```

Uses ICMP timestamp requests for discovery.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 057 · ICMP timestamp discovery

```
nmap -PP -sn 192.0.2.10
```

Uses ICMP timestamp requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 058 · ICMP timestamp discovery

```
nmap -PP -sn 192.0.2.0/28
```

Uses ICMP timestamp requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 059 · ICMP timestamp discovery

```
nmap -PP -sn 198.51.100.0/28
```

Uses ICMP timestamp requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 060 · ICMP timestamp discovery

```
nmap -PP -sn -iL targets.txt
```

Uses ICMP timestamp requests for discovery.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 061 · TCP SYN discovery

```
nmap -PS22,80,443 -sn scanme.nmap.org
```

Discovers hosts using SYN probes to selected ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 062 · TCP SYN discovery

```
nmap -PS22,80,443 -sn 192.0.2.10
```

Discovers hosts using SYN probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 063 · TCP SYN discovery

```
nmap -PS22,80,443 -sn 192.0.2.0/28
```

Discovers hosts using SYN probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 064 · TCP SYN discovery

```
nmap -PS22,80,443 -sn 198.51.100.0/28
```

Discovers hosts using SYN probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 065 · TCP SYN discovery

```
nmap -PS22,80,443 -sn -iL targets.txt
```

Discovers hosts using SYN probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 066 · TCP ACK discovery

```
nmap -PA80,443 -sn scanme.nmap.org
```

Discovers hosts using ACK probes to selected ports.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 067 · TCP ACK discovery

```
nmap -PA80,443 -sn 192.0.2.10
```

Discovers hosts using ACK probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 068 · TCP ACK discovery

```
nmap -PA80,443 -sn 192.0.2.0/28
```

Discovers hosts using ACK probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 069 · TCP ACK discovery

```
nmap -PA80,443 -sn 198.51.100.0/28
```

Discovers hosts using ACK probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 070 · TCP ACK discovery

```
nmap -PA80,443 -sn -iL targets.txt
```

Discovers hosts using ACK probes to selected ports.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 071 · UDP discovery

```
nmap -PU53,161 -sn scanme.nmap.org
```

Discovers hosts using UDP probes to selected services.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 072 · UDP discovery

```
nmap -PU53,161 -sn 192.0.2.10
```

Discovers hosts using UDP probes to selected services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 073 · UDP discovery

```
nmap -PU53,161 -sn 192.0.2.0/28
```

Discovers hosts using UDP probes to selected services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 074 · UDP discovery

```
nmap -PU53,161 -sn 198.51.100.0/28
```

Discovers hosts using UDP probes to selected services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 075 · UDP discovery

```
nmap -PU53,161 -sn -iL targets.txt
```

Discovers hosts using UDP probes to selected services.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 076 · Decoy scan lab

```
nmap -D RND:5 scanme.nmap.org
```

Adds random decoy sources for controlled detection testing.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 077 · Decoy scan lab

```
nmap -D RND:5 192.0.2.10
```

Adds random decoy sources for controlled detection testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 078 · Decoy scan lab

```
nmap -D RND:5 192.0.2.0/28
```

Adds random decoy sources for controlled detection testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 079 · Decoy scan lab

```
nmap -D RND:5 198.51.100.0/28
```

Adds random decoy sources for controlled detection testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 080 · Decoy scan lab

```
nmap -D RND:5 -iL targets.txt
```

Adds random decoy sources for controlled detection testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 081 · Specify source address

```
nmap -S 192.0.2.20 scanme.nmap.org
```

Sets the source address when routing and authorization permit it.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 082 · Specify source address

```
nmap -S 192.0.2.20 192.0.2.10
```

Sets the source address when routing and authorization permit it.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 083 · Specify source address

```
nmap -S 192.0.2.20 192.0.2.0/28
```

Sets the source address when routing and authorization permit it.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 084 · Specify source address

```
nmap -S 192.0.2.20 198.51.100.0/28
```

Sets the source address when routing and authorization permit it.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 085 · Specify source address

```
nmap -S 192.0.2.20 -iL targets.txt
```

Sets the source address when routing and authorization permit it.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 086 · Specify source port

```
nmap -g 53 scanme.nmap.org
```

Uses a selected source port for firewall-rule validation.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 087 · Specify source port

```
nmap -g 53 192.0.2.10
```

Uses a selected source port for firewall-rule validation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 088 · Specify source port

```
nmap -g 53 192.0.2.0/28
```

Uses a selected source port for firewall-rule validation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 089 · Specify source port

```
nmap -g 53 198.51.100.0/28
```

Uses a selected source port for firewall-rule validation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 090 · Specify source port

```
nmap -g 53 -iL targets.txt
```

Uses a selected source port for firewall-rule validation.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 091 · Fragment probes

```
nmap -f scanme.nmap.org
```

Fragments IP packets for controlled IDS and firewall testing.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 092 · Fragment probes

```
nmap -f 192.0.2.10
```

Fragments IP packets for controlled IDS and firewall testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 093 · Fragment probes

```
nmap -f 192.0.2.0/28
```

Fragments IP packets for controlled IDS and firewall testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 094 · Fragment probes

```
nmap -f 198.51.100.0/28
```

Fragments IP packets for controlled IDS and firewall testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 095 · Fragment probes

```
nmap -f -iL targets.txt
```

Fragments IP packets for controlled IDS and firewall testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 096 · Custom fragment size

```
nmap --mtu 24 scanme.nmap.org
```

Uses a multiple-of-eight MTU for fragmentation testing.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 097 · Custom fragment size

```
nmap --mtu 24 192.0.2.10
```

Uses a multiple-of-eight MTU for fragmentation testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 098 · Custom fragment size

```
nmap --mtu 24 192.0.2.0/28
```

Uses a multiple-of-eight MTU for fragmentation testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 099 · Custom fragment size

```
nmap --mtu 24 198.51.100.0/28
```

Uses a multiple-of-eight MTU for fragmentation testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 100 · Custom fragment size

```
nmap --mtu 24 -iL targets.txt
```

Uses a multiple-of-eight MTU for fragmentation testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 101 · Append random data

```
nmap --data-length 32 scanme.nmap.org
```

Adds payload bytes to probes for signature testing.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 102 · Append random data

```
nmap --data-length 32 192.0.2.10
```

Adds payload bytes to probes for signature testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 103 · Append random data

```
nmap --data-length 32 192.0.2.0/28
```

Adds payload bytes to probes for signature testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 104 · Append random data

```
nmap --data-length 32 198.51.100.0/28
```

Adds payload bytes to probes for signature testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 105 · Append random data

```
nmap --data-length 32 -iL targets.txt
```

Adds payload bytes to probes for signature testing.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 106 · Set IP TTL

```
nmap --ttl 32 scanme.nmap.org
```

Controls probe lifetime for routing experiments.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 107 · Set IP TTL

```
nmap --ttl 32 192.0.2.10
```

Controls probe lifetime for routing experiments.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 108 · Set IP TTL

```
nmap --ttl 32 192.0.2.0/28
```

Controls probe lifetime for routing experiments.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 109 · Set IP TTL

```
nmap --ttl 32 198.51.100.0/28
```

Controls probe lifetime for routing experiments.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 110 · Set IP TTL

```
nmap --ttl 32 -iL targets.txt
```

Controls probe lifetime for routing experiments.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 111 · Randomize MAC address

```
nmap --spoof-mac 0 scanme.nmap.org
```

Uses a random MAC on an authorized local test network.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 112 · Randomize MAC address

```
nmap --spoof-mac 0 192.0.2.10
```

Uses a random MAC on an authorized local test network.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 113 · Randomize MAC address

```
nmap --spoof-mac 0 192.0.2.0/28
```

Uses a random MAC on an authorized local test network.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 114 · Randomize MAC address

```
nmap --spoof-mac 0 198.51.100.0/28
```

Uses a random MAC on an authorized local test network.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 115 · Randomize MAC address

```
nmap --spoof-mac 0 -iL targets.txt
```

Uses a random MAC on an authorized local test network.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 116 · Invalid checksums

```
nmap --badsum scanme.nmap.org
```

Sends invalid checksums to study firewall and IDS behavior.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 117 · Invalid checksums

```
nmap --badsum 192.0.2.10
```

Sends invalid checksums to study firewall and IDS behavior.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 118 · Invalid checksums

```
nmap --badsum 192.0.2.0/28
```

Sends invalid checksums to study firewall and IDS behavior.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 119 · Invalid checksums

```
nmap --badsum 198.51.100.0/28
```

Sends invalid checksums to study firewall and IDS behavior.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 120 · Invalid checksums

```
nmap --badsum -iL targets.txt
```

Sends invalid checksums to study firewall and IDS behavior.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 121 · Packet trace

```
nmap --packet-trace scanme.nmap.org
```

Shows sent and received packets for troubleshooting.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 122 · Packet trace

```
nmap --packet-trace 192.0.2.10
```

Shows sent and received packets for troubleshooting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 123 · Packet trace

```
nmap --packet-trace 192.0.2.0/28
```

Shows sent and received packets for troubleshooting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 124 · Packet trace

```
nmap --packet-trace 198.51.100.0/28
```

Shows sent and received packets for troubleshooting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 125 · Packet trace

```
nmap --packet-trace -iL targets.txt
```

Shows sent and received packets for troubleshooting.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 126 · Safe NSE category

```
nmap --script safe scanme.nmap.org
```

Runs scripts categorized as safe.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 127 · Safe NSE category

```
nmap --script safe 192.0.2.10
```

Runs scripts categorized as safe.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 128 · Safe NSE category

```
nmap --script safe 192.0.2.0/28
```

Runs scripts categorized as safe.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 129 · Safe NSE category

```
nmap --script safe 198.51.100.0/28
```

Runs scripts categorized as safe.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 130 · Safe NSE category

```
nmap --script safe -iL targets.txt
```

Runs scripts categorized as safe.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 131 · Discovery NSE category

```
nmap --script discovery scanme.nmap.org
```

Runs scripts that collect additional service information.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 132 · Discovery NSE category

```
nmap --script discovery 192.0.2.10
```

Runs scripts that collect additional service information.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 133 · Discovery NSE category

```
nmap --script discovery 192.0.2.0/28
```

Runs scripts that collect additional service information.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 134 · Discovery NSE category

```
nmap --script discovery 198.51.100.0/28
```

Runs scripts that collect additional service information.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 135 · Discovery NSE category

```
nmap --script discovery -iL targets.txt
```

Runs scripts that collect additional service information.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 136 · Version NSE category

```
nmap --script version scanme.nmap.org
```

Runs scripts used during version detection.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 137 · Version NSE category

```
nmap --script version 192.0.2.10
```

Runs scripts used during version detection.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 138 · Version NSE category

```
nmap --script version 192.0.2.0/28
```

Runs scripts used during version detection.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 139 · Version NSE category

```
nmap --script version 198.51.100.0/28
```

Runs scripts used during version detection.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 140 · Version NSE category

```
nmap --script version -iL targets.txt
```

Runs scripts used during version detection.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 141 · NSE boolean selection

```
nmap --script "default and safe" scanme.nmap.org
```

Runs scripts matching both default and safe categories.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 142 · NSE boolean selection

```
nmap --script "default and safe" 192.0.2.10
```

Runs scripts matching both default and safe categories.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 143 · NSE boolean selection

```
nmap --script "default and safe" 192.0.2.0/28
```

Runs scripts matching both default and safe categories.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 144 · NSE boolean selection

```
nmap --script "default and safe" 198.51.100.0/28
```

Runs scripts matching both default and safe categories.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 145 · NSE boolean selection

```
nmap --script "default and safe" -iL targets.txt
```

Runs scripts matching both default and safe categories.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 146 · Safe HTTP NSE scripts

```
nmap --script "http-* and safe" scanme.nmap.org
```

Runs safe scripts whose names begin with http-.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 147 · Safe HTTP NSE scripts

```
nmap --script "http-* and safe" 192.0.2.10
```

Runs safe scripts whose names begin with http-.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 148 · Safe HTTP NSE scripts

```
nmap --script "http-* and safe" 192.0.2.0/28
```

Runs safe scripts whose names begin with http-.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 149 · Safe HTTP NSE scripts

```
nmap --script "http-* and safe" 198.51.100.0/28
```

Runs safe scripts whose names begin with http-.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 150 · Safe HTTP NSE scripts

```
nmap --script "http-* and safe" -iL targets.txt
```

Runs safe scripts whose names begin with http-.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 151 · NSE help

```
nmap --script-help "http-*" scanme.nmap.org
```

Displays descriptions and categories for matching scripts.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 152 · NSE help

```
nmap --script-help "http-*" 192.0.2.10
```

Displays descriptions and categories for matching scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 153 · NSE help

```
nmap --script-help "http-*" 192.0.2.0/28
```

Displays descriptions and categories for matching scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 154 · NSE help

```
nmap --script-help "http-*" 198.51.100.0/28
```

Displays descriptions and categories for matching scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 155 · NSE help

```
nmap --script-help "http-*" -iL targets.txt
```

Displays descriptions and categories for matching scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 156 · Refresh NSE database

```
nmap --script-updatedb scanme.nmap.org
```

Rebuilds the local NSE script index after script changes.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 157 · Refresh NSE database

```
nmap --script-updatedb 192.0.2.10
```

Rebuilds the local NSE script index after script changes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 158 · Refresh NSE database

```
nmap --script-updatedb 192.0.2.0/28
```

Rebuilds the local NSE script index after script changes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 159 · Refresh NSE database

```
nmap --script-updatedb 198.51.100.0/28
```

Rebuilds the local NSE script index after script changes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 160 · Refresh NSE database

```
nmap --script-updatedb -iL targets.txt
```

Rebuilds the local NSE script index after script changes.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 161 · Trace NSE traffic

```
nmap --script-trace scanme.nmap.org
```

Shows network traffic produced by NSE scripts.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 162 · Trace NSE traffic

```
nmap --script-trace 192.0.2.10
```

Shows network traffic produced by NSE scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 163 · Trace NSE traffic

```
nmap --script-trace 192.0.2.0/28
```

Shows network traffic produced by NSE scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 164 · Trace NSE traffic

```
nmap --script-trace 198.51.100.0/28
```

Shows network traffic produced by NSE scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 165 · Trace NSE traffic

```
nmap --script-trace -iL targets.txt
```

Shows network traffic produced by NSE scripts.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 166 · NSE arguments file

```
nmap --script-args-file nse-args.txt scanme.nmap.org
```

Loads script arguments from a controlled file.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 167 · NSE arguments file

```
nmap --script-args-file nse-args.txt 192.0.2.10
```

Loads script arguments from a controlled file.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 168 · NSE arguments file

```
nmap --script-args-file nse-args.txt 192.0.2.0/28
```

Loads script arguments from a controlled file.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 169 · NSE arguments file

```
nmap --script-args-file nse-args.txt 198.51.100.0/28
```

Loads script arguments from a controlled file.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 170 · NSE arguments file

```
nmap --script-args-file nse-args.txt -iL targets.txt
```

Loads script arguments from a controlled file.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 171 · HTTP method review

```
nmap -p 80 --script http-methods --script-args http-methods.retest scanme.nmap.org
```

Enumerates methods and optionally retests flagged methods.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 172 · HTTP method review

```
nmap -p 80 --script http-methods --script-args http-methods.retest 192.0.2.10
```

Enumerates methods and optionally retests flagged methods.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 173 · HTTP method review

```
nmap -p 80 --script http-methods --script-args http-methods.retest 192.0.2.0/28
```

Enumerates methods and optionally retests flagged methods.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 174 · HTTP method review

```
nmap -p 80 --script http-methods --script-args http-methods.retest 198.51.100.0/28
```

Enumerates methods and optionally retests flagged methods.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 175 · HTTP method review

```
nmap -p 80 --script http-methods --script-args http-methods.retest -iL targets.txt
```

Enumerates methods and optionally retests flagged methods.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 176 · TLS DH parameter review

```
nmap -p 443 --script ssl-dh-params scanme.nmap.org
```

Checks Diffie-Hellman parameter strength.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 177 · TLS DH parameter review

```
nmap -p 443 --script ssl-dh-params 192.0.2.10
```

Checks Diffie-Hellman parameter strength.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 178 · TLS DH parameter review

```
nmap -p 443 --script ssl-dh-params 192.0.2.0/28
```

Checks Diffie-Hellman parameter strength.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 179 · TLS DH parameter review

```
nmap -p 443 --script ssl-dh-params 198.51.100.0/28
```

Checks Diffie-Hellman parameter strength.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 180 · TLS DH parameter review

```
nmap -p 443 --script ssl-dh-params -iL targets.txt
```

Checks Diffie-Hellman parameter strength.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 181 · SMB share inventory

```
nmap -p 445 --script smb-enum-shares scanme.nmap.org
```

Enumerates shares using authorized credentials or permitted guest access.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 182 · SMB share inventory

```
nmap -p 445 --script smb-enum-shares 192.0.2.10
```

Enumerates shares using authorized credentials or permitted guest access.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 183 · SMB share inventory

```
nmap -p 445 --script smb-enum-shares 192.0.2.0/28
```

Enumerates shares using authorized credentials or permitted guest access.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 184 · SMB share inventory

```
nmap -p 445 --script smb-enum-shares 198.51.100.0/28
```

Enumerates shares using authorized credentials or permitted guest access.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 185 · SMB share inventory

```
nmap -p 445 --script smb-enum-shares -iL targets.txt
```

Enumerates shares using authorized credentials or permitted guest access.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 186 · RDP encryption review

```
nmap -p 3389 --script rdp-enum-encryption scanme.nmap.org
```

Enumerates RDP security and encryption settings.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 187 · RDP encryption review

```
nmap -p 3389 --script rdp-enum-encryption 192.0.2.10
```

Enumerates RDP security and encryption settings.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 188 · RDP encryption review

```
nmap -p 3389 --script rdp-enum-encryption 192.0.2.0/28
```

Enumerates RDP security and encryption settings.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 189 · RDP encryption review

```
nmap -p 3389 --script rdp-enum-encryption 198.51.100.0/28
```

Enumerates RDP security and encryption settings.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 190 · RDP encryption review

```
nmap -p 3389 --script rdp-enum-encryption -iL targets.txt
```

Enumerates RDP security and encryption settings.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 191 · SNMP information review

```
nmap -p 161 --script snmp-info scanme.nmap.org
```

Collects basic information when authorized community access is configured.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 192 · SNMP information review

```
nmap -p 161 --script snmp-info 192.0.2.10
```

Collects basic information when authorized community access is configured.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 193 · SNMP information review

```
nmap -p 161 --script snmp-info 192.0.2.0/28
```

Collects basic information when authorized community access is configured.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 194 · SNMP information review

```
nmap -p 161 --script snmp-info 198.51.100.0/28
```

Collects basic information when authorized community access is configured.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 195 · SNMP information review

```
nmap -p 161 --script snmp-info -iL targets.txt
```

Collects basic information when authorized community access is configured.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 196 · DNS transfer validation

```
nmap -p 53 --script dns-zone-transfer scanme.nmap.org
```

Tests whether an approved DNS server permits AXFR.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 197 · DNS transfer validation

```
nmap -p 53 --script dns-zone-transfer 192.0.2.10
```

Tests whether an approved DNS server permits AXFR.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 198 · DNS transfer validation

```
nmap -p 53 --script dns-zone-transfer 192.0.2.0/28
```

Tests whether an approved DNS server permits AXFR.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 199 · DNS transfer validation

```
nmap -p 53 --script dns-zone-transfer 198.51.100.0/28
```

Tests whether an approved DNS server permits AXFR.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 200 · DNS transfer validation

```
nmap -p 53 --script dns-zone-transfer -iL targets.txt
```

Tests whether an approved DNS server permits AXFR.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 201 · Security header review

```
nmap -p 80,443 --script http-security-headers scanme.nmap.org
```

Checks common HTTP response security headers.

Note: Nmap permits scanning scanme.nmap.org for learning; still keep traffic reasonable.

Expert 202 · Security header review

```
nmap -p 80,443 --script http-security-headers 192.0.2.10
```

Checks common HTTP response security headers.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 203 · Security header review

```
nmap -p 80,443 --script http-security-headers 192.0.2.0/28
```

Checks common HTTP response security headers.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 204 · Security header review

```
nmap -p 80,443 --script http-security-headers 198.51.100.0/28
```

Checks common HTTP response security headers.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

Expert 205 · Security header review

```
nmap -p 80,443 --script http-security-headers -iL targets.txt
```

Checks common HTTP response security headers.

Note: Use documentation ranges/placeholders and replace them only with authorized targets.

04

Flag Decoder & Workflow

How to build a safe scan plan

1 · Discover

Start with `-sn` and approved discovery probes. Confirm the asset list before port scanning.

2 · Enumerate

Use selected ports, `-sV`, and protocol-specific safe scripts.

3 · Control

Set timing, rate limits, retries, exclusions, and timeouts for the environment.

4 · Record

Use `-oA`, timestamps, source IPs, and scope notes for reproducible evidence.

05

Official References

Primary documentation used for validation

Nmap Reference Guide
https://nmap.org/book/man.html

NSE Usage
https://nmap.org/book/nse-usage.html

NSE Script Index
https://nmap.org/nsedoc/

Keep learning safely

Website
https://mnatech.in/

Instagram
@mna_tech_academy

Call / WhatsApp
+91 9216110094

Practice rule
Only test systems you own or have written authorization to assess.

© 2026 MNA Tech Academy. All rights reserved.
Original educational reference. Product names and trademarks belong to their respective owners. Commands may vary by version and operating system; verify with official documentation before production use.