CTF Lab Guide (2026)

Nmap Recon Sprint

Host Discovery → Port Discovery → Service & OS Fingerprinting

Difficulty	Beginner → Intermediate (Recon fundamentals)
Primary tool	Nmap (latest stable recommended)
Goal	Produce a clear Recon Report that enables next-stage enumeration
Safety	Run ONLY in the authorized classroom/CTF lab network

Learning outcomes

• Discover live hosts using multiple probe types and explain the evidence with **--reason**.
• Enumerate open TCP ports reliably (**-p-**) and interpret **open / closed / filtered** states.
• Identify service versions (**-sV**) and infer OS traits (**-O**) with appropriate confidence.
• Deliver a Recon Report that another person can use immediately for deeper enumeration.

Rules of engagement

Use these techniques only inside the authorized lab/CTF environment. Scanning production or third-party networks without explicit written permission is not allowed.

Preflight checklist

Before scanning, confirm you are on the correct network and that your tools behave predictably.

1) Verify your interface and routing

```
ip a
ip route
```

2) Run Nmap with appropriate privileges

SYN scans, ARP discovery, and OS detection work best with root privileges.

```
sudo -v
```

3) Confirm the target range

In this lab we will use an example subnet and a sample target. Replace these with the instructor-provided values.

```
Example subnet: 192.168.1.0/24
Example host:   192.168.1.7
```

Phase 1 — Host Discovery (Ping Sweeping)

Objective: identify which hosts are alive and record **why** Nmap believes they are up using **--reason**.

Key flags

• **-sn**: host discovery only (no port scan)
• **--reason**: prints evidence (ARP reply, ICMP reply, TCP response, etc.)
• **--send-ip**: sends probes using raw IP sockets (useful in some environments; not always required)

1A) ARP ping scan (best on local LAN)

Use ARP discovery when you are on the same Layer-2 network as the targets (same LAN/VLAN).

```
nmap -sn -PR --reason --send-ip 192.168.1.7
```

What to observe: a reason like *arp-response* is strong evidence the host is up.

1B) Fast local sweep (no port scan)

```
nmap -sn --send-ip --reason 192.168.1.0/24
```

Record the IPs that respond and the evidence shown by **--reason**.

1C) TCP-based discovery (useful when ICMP is blocked)

These probes can confirm reachability even if classic ping is filtered.

```
# SYN ping scan
nmap -sn -PS --send-ip --reason 192.168.1.0/24

# ACK ping scan
nmap -sn -PA --send-ip --reason 192.168.1.0/24
```

Interpretation hint: TCP responses (SYN-ACK or RST) often prove the host is reachable.

1D) UDP ping scan (fast but silence is ambiguous)

UDP discovery sometimes marks hosts up via ICMP errors. No response does not automatically mean down.

```
nmap -sn -PU --send-ip --reason --data-string m4dm4n 192.168.1.7
```

1E) SCTP INIT ping (optional)

SCTP discovery uses INIT probes. It is less common, but useful to understand alternate protocols.

```
nmap -sn -PY --send-ip --reason 192.168.1.7
```

1F) ICMP discovery variants

```
# ICMP echo request (type 8) expecting echo reply (type 0)
nmap -sn -PE --send-ip --reason 192.168.1.7

# ICMP timestamp (type 13) expecting timestamp reply (type 14)
nmap -sn -PP --send-ip --reason 192.168.1.7

# ICMP address mask (type 17) expecting address mask reply (type 18)
nmap -sn -PM --send-ip --reason 192.168.1.7
```

Note: ICMP is frequently filtered; always validate with TCP-based discovery when in doubt.

Phase 1 deliverable — Host Discovery Evidence Log

For at least 3 hosts, submit:

- IP address
- Probe type used (ARP / SYN / ACK / UDP / ICMP / SCTP)
- Result (up/down)
- Evidence line(s) from --reason
- One-sentence interpretation (e.g., “ICMP blocked, but TCP RST confirms host is reachable”)

Phase 2 — Port Discovery (TCP)

Objective: discover open TCP ports and understand open/closed/filtered outcomes.

Why -Pn?

If host discovery is unreliable or filtered, **-Pn** tells Nmap to assume the host is up and proceed directly to port scanning.

2A) Full TCP SYN scan (preferred when you have privileges)

```
nmap -Pn -sS -p- -T3 --reason 192.168.1.7
```

- **-sS** SYN scan (fast, typical default when privileged)
- **-p-** scans all 65535 TCP ports
- **-T3** balanced timing for stable results in classrooms
- **--reason** helps you explain each result

2B) Full TCP Connect scan (works without raw privileges)

```
nmap -Pn -sT -p- -T3 --reason 192.168.1.7
```

Use **-sT** when SYN scan is not possible (permissions or environment constraints).

Phase 2 deliverable — Open Ports List

Submit:

- Target IP
- Scan type used (-sS or -sT)
- List of open ports (top 10 or all if fewer than 10)
- For each open port: state and the key evidence from --reason

Phase 3 — Service & OS Detection

Objective: identify what is running behind each open port, and infer OS traits responsibly.

3A) Version detection + OS fingerprinting (all ports)

```
nmap -Pn -sS -sV -O -p- -T3 --reason 192.168.1.7
```

How to interpret results

• **-sV** uses additional probes to guess service names and versions. Treat as “likely” until confirmed with deeper enumeration.
• **-O** is probabilistic. Confidence improves when multiple ports are reachable and responses are consistent.
• If OS detection is low confidence, record it as a hypothesis and focus on service-level evidence.

Phase 3 deliverable — Service Fingerprinting Snapshot

• For each open port: service, version guess, and a confidence note
• OS guess (if provided) and your confidence (high/medium/low)
• Two next-step enumeration ideas based on what you found (e.g., HTTP content discovery, SSH policy checks, SMB share enumeration)

Advanced topics (defender perspective)

You may see references online to techniques such as packet fragmentation, decoys, and indirect scanning. These topics are primarily discussed here as **defensive visibility testing**: how to validate that your monitoring, firewalls, and detection tools can correctly observe and log unusual scan patterns. For this course, we focus on accurate recon and evidence-based reporting.

In a blue-team lab, your goal is to answer questions like:

• Do our sensors capture the true source IP and scan intent?
• Do fragments get reassembled and logged correctly?
• Do alerts correlate across multiple probe styles (ICMP, TCP, UDP)?

If the instructor assigns a blue-team validation exercise, follow the provided lab instructions and monitoring checklist.

Final Submission — Recon Report Template

Your final writeup must be readable by someone who did not run the scans. Keep it evidence-based and concise: what you observed, why you believe it, and what it implies.

Recon Report — Target: _____

1) Host discovery summary

• Methods attempted:
• Final conclusion (up/down):
• Best evidence (paste one --reason line):
• Short interpretation:

2) Port discovery summary

• Scan type used (-sS or -sT):
• Open ports found:
• Any filtered behavior (yes/no + one sentence):

3) Service & OS snapshot

• Services table (port → service → version):
• OS guess and confidence:
• Two next-step enumeration ideas (based on services):

Service Notes Table (optional)

Port/Proto	State	Service	Version guess	Evidence / Notes

References (for further study)

Nmap Reference Guide and Nmap Book (official documentation): nmap.org/book/ • Nmap downloads: nmap.org/dist/