PREVIEW COPY

CyberWithMadhav

2026 EDITION

```
$ nmap -sV --open 192.168.56.101
```

# Nmap Field Guide

From Zero to Confident Scanner. A practical, ethics-first guide for Indian beginners and students starting in cybersecurity.

```
# your first real scan, on your own lab
$ nmap -sn 192.168.56.0/24
$ sudo nmap -sS -sV -p 22,80 192.168.56.101
$ nmap -oA my-first-scan 192.168.56.101
```

**Madhav Pandya**
CyberWithMadhav | cyberwithmadhav.com

10 HANDS-ON LABS
1 PAGE CHEAT SHEET
DEFENDER FIRST

Preview only. Get the full 30 page Nmap Field Guide with 10 labs and a cheat sheet at cyberwithmadhav.com

PREVIEW
CyberWithMadhav

PREVIEW COPY

STOP. READ THIS FIRST

# Scan only what you own, or have written permission to scan.

Nmap is a legal, free, respected tool. **How** you use it decides whether it is a skill or a crime. Even the Nmap documentation advises asking permission before scanning a network at all. Madhav ka tip: **pehle permission, phir scan.**

## You may scan

YES **Your own lab.** Your laptop ( `127.0.0.1` ), your own VMs on a host-only network (chapter 1).

YES **Your own home devices** (your router, your phone, your smart TV), when the people who share that network know.

YES **scanme.nmap.org**, only as the Nmap project allows. Their page says you are authorised to scan that machine, that a few scans in a day is fine, and not to hammer it 100 times a day or use it to test password cracking.

YES **Anything with written permission** from the owner: a signed scope with IP ranges, dates and what is allowed.

## You may not scan

NO College, office, hostel, PG, café or hotel Wi-Fi, unless the network owner has allowed it in writing.

NO Websites, servers or IPs of companies, banks, government bodies or neighbours, "just to check".

NO Random internet addresses. Never use `-iR` to pick targets.

NO A target that is outside the scope you were given, even if it sits next to one you were allowed to test.

WHAT THE LAW SAYS (INDIA)

The **Information Technology Act, 2000** is the main law. **Section 43** says that if a person, *without permission of the owner or any other person who is in charge of a computer, computer system or computer network*, accesses or secures access to it, or does other listed acts such as copying data, introducing a virus, disrupting or denying access, they are liable to pay compensation to the affected person. **Section 66** says that if a person, *dishonestly or fraudulently*, does any act referred to in Section 43, they are punishable with imprisonment up to **three years**, or a fine up to **₹5 lakh**, or both.

Whether a bare port scan counts as "access" is something you never want to find out in court. Treat every unauthorised scan as risky. Other laws, and the rules of your college, employer or ISP, may also apply.

Wording summarised from the IT Act as published on India Code (indiacode.nic.in). Laws get amended: always read the current text yourself. This is education, not legal advice.

YOUR 5 GOLDEN RULES

1. **Own it or have it in writing.** "My friend said okay on WhatsApp" is not a scope document.
2. **Stay in scope.** Only the IPs, ports and times you were given.
3. **Start gentle.** Default timing, few ports, no "intrusive" scripts on systems you do not control.
4. **Keep notes and outputs.** Save with `-oA` . Good habits protect you and your client.
5. **Report responsibly.** If you find something on a system you own or are authorised to test, fix it or report it to the owner privately.

Preview only. Get the full 30 page Nmap Field Guide with 10 labs and a cheat sheet at cyberwithmadhav.com

PREVIEW COPY

# Contents

Ethics first, then tools, then labs.


| | | |
|---|---|---|
| | Copyright and licence | 2 |
| | Read this first: ethics and law | 3 |
| 01 | Build Your Lab | 5 |
| 02 | What Nmap Is and How It Works | 6 |
| 03 | Installing Nmap | 8 |
| 04 | Host Discovery | 9 |
| 05 | Scan Types | 10 |
| 06 | Choosing Ports | 12 |
| 07 | Reading the Results | 14 |
| 08 | Service and Version Detection | 15 |
| 09 | OS Detection | 16 |
| 10 | Timing and Performance | 17 |
| 11 | Output Formats | 18 |
| 12 | The Nmap Scripting Engine (NSE) | 19 |
| 13 | Firewalls and IDS: The Defender's View | 21 |
| 14 | Nmap as a Defender's Tool | 23 |
| 15 | Ten Hands-On Labs | 24 |
| 16 | One-Page Cheat Sheet | 27 |
| 17 | Common Mistakes | 28 |
| 18 | Next Steps: Your Learning Path | 28 |
| 19 | Glossary | 29 |


Preview only. Get the full 30 page Nmap Field Guide with 10 labs and a cheat sheet at cyberwithmadhav.com



PREVIEW
CyberWithMadhav

## -sS: SYN scan

The SYN scan sends a SYN. If a SYN/ACK comes back the port is open, if RST the port is closed, and if nothing comes back (or an ICMP “unreachable” error does) the port is filtered. It is called *half-open* because it does not finish the handshake, which makes it quick and relatively unobtrusive. It is still visible to firewalls and intrusion detection, so never treat it as invisible.

```
$ sudo nmap -sS 192.168.56.101
```

EXAMPLE OUTPUT: LAB IP 192.168.56.101

```
Nmap scan report for 192.168.56.101
Host is up (0.00041s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:3A:5C:9E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

## -sT: connect scan

When you cannot send raw packets, Nmap asks your operating system to open real connections. It works everywhere, but because the handshake completes, the target's service may log each connection, so it is noisier at the application level.

```
$ nmap -sT -p 22,80,8000,8080 127.0.0.1
```

EXAMPLE OUTPUT: REAL RUN ON 127.0.0.1, NMAP 7.95

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000059s latency).

PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   closed http
8000/tcp open   http-alt
8080/tcp open   http-proxy
```

Notice the closed ports are listed here because we asked for specific ports. Also notice the difference in the reason Nmap gives for closed ports in a bigger scan: `conn-refused` for a connect scan, `reset` for a SYN scan. Use `--reason` to see it.

## -sU: UDP scan

UDP has no handshake, so a quiet port tells Nmap very little. A closed UDP port usually answers with an ICMP “port unreachable”, but many systems rate-limit those replies. The reference guide says Linux and Solaris are particularly strict, with a Linux-style limit of one reply per second as its example. Result: UDP scans are **slow**, so scan a handful of top ports first.

Preview only. Get the full 30 page Nmap Field Guide with 10 labs and a cheat sheet at cyberwithmadhav.com