Nmap Port Scanning Guide (Step-by-Step) – Target: 10.0.3.4 (Windows)

Lab-focused walkthrough for discovering open ports and identifying services with Nmap.

Scanner	***Kali Linux (VirtualBox)***
Tool	*Nmap*
Target host	*Windows PC*
Target IP	*10.0.3.4*
Goal	*Identify open TCP/UDP ports, confirm services/versions, and save scan outputs*

1. Prerequisites

- Network connectivity between Kali and the Windows target (same network / routed path).
- Nmap installed on Kali (usually preinstalled).
- Sudo privileges on Kali for SYN scans (-sS) and OS detection (-O).
- Windows firewall or security controls may cause ports to appear filtered; that is still a valid finding.

Optional sanity checks:

- `ip a` - Confirm your Kali IP/interface.
- `ip r` - Confirm route to the 10.0.3.0/24 network.
- `ping -c 3 10.0.3.4` - Quick reachability test (ICMP may be blocked; a failed ping does not always mean host is down).

2. Identify the target and verify it is up

If you are not 100% sure the host is online, start with host discovery. In a lab, you might also scan the whole /24 to confirm the IP is correct.

2.1 Host discovery (ping scan)

Scan the local subnet for live hosts (no port scan):

```
nmap -sn 10.0.3.0/24
```

```
nmap -sn -PE -PP -PM 10.0.3.0/24  # try multiple ICMP probes
```

If the target blocks ICMP, use -Pn to skip host discovery and scan anyway:

```
nmap -Pn 10.0.3.4
```

3. Basic TCP port scan (quick view)

This scans the 1,000 most common TCP ports and provides a quick baseline.

```
nmap -Pn -n 10.0.3.4
```

Flags explained:

- -Pn: treat host as up (useful if ICMP is blocked).
- -n: do not resolve DNS names (faster and cleaner output).

4. Full TCP port scan (all 65,535 ports)

For a comprehensive port inventory, scan all TCP ports. This can take longer but is the most complete.

```
sudo nmap -Pn -n -sS -p- --open --reason 10.0.3.4
```

Recommended options:

- -sS: SYN scan (requires sudo).
- -p-: scan all 1-65535 ports.
- --open: show only open ports (reduces noise).
- --reason: explain why Nmap marked a port as open/closed/filtered.

5. Service and version detection

Once you know which ports are open, identify what is running on them.

```
sudo nmap -Pn -n -sS -sV --version-all --open 10.0.3.4
```

Tip: If you already found open ports, scan only those ports to save time:

```
sudo nmap -Pn -n -sS -sV -p 135,139,445,3389 10.0.3.4  # example ports
```

6. Default scripts and OS detection (safe enumeration)

Nmap scripting can do safe service enumeration. The default scripts (-sC) are generally non-intrusive. OS detection (-O) can help confirm the target OS, but it requires sudo and works best when at least one open and one closed port are found.

```
sudo nmap -Pn -n -sS -sV -sC -O 10.0.3.4
```

All-in-one (aggressive) scan (more traffic; use carefully in a lab):

```
sudo nmap -Pn -n -A 10.0.3.4
```

What -A includes:

- OS detection (-O)
- Version detection (-sV)
- Default scripts (-sC)
- Traceroute

7. UDP port scanning (optional but important)

UDP scanning is slower and more error-prone because many UDP services do not reply. Start with the most common UDP ports, then expand if needed.

```
sudo nmap -Pn -n -sU --top-ports 200 10.0.3.4
```

Or target specific UDP ports commonly found in Windows environments (adjust to your lab):

```
sudo nmap -Pn -n -sU -p 53,67,68,69,123,137,138,161,162,500,1900 10.0.3.4
```

8. Save your results (recommended for reports)

Always save scan output so you can compare scans and attach evidence to reports.

Save in normal text format:

```
nmap -Pn -n 10.0.3.4 -oN nmap_10.0.3.4_basic.txt
```

Save in all formats (normal, grepable, XML):

```
sudo nmap -Pn -n -sS -sV -sC -O 10.0.3.4 -oA nmap_10.0.3.4_full
```

If you want to import into other tools, XML is best:

```
sudo nmap -Pn -n -sS -sV 10.0.3.4 -oX nmap_10.0.3.4.xml
```

9. Interpret the output

Key port states:

- open: an application accepted the probe (service likely reachable).
- closed: no service is listening on that port, but the host responded.
- filtered: a firewall or network device likely blocked the probe (no clear response).

In Windows vulnerability labs, common ports you may see:

- 135/tcp (MSRPC)
- 139/tcp and 445/tcp (SMB/CIFS)
- 3389/tcp (RDP)
- 5985/tcp (WinRM HTTP) and 5986/tcp (WinRM HTTPS)
- 80/443 (web services) if installed

10. Troubleshooting tips

- If everything shows filtered, check Windows Firewall and any security software on the target.
- Verify both VMs are on the same VirtualBox network mode (Host-only, Internal Network, or Bridged). NAT typically prevents inbound scanning to another guest unless configured.
- Try a slower timing template (-T2) if the network is unstable, or a faster one (-T4) in a controlled lab.
- If OS detection fails, ensure you have at least one open port and one closed port; consider scanning a wider port range.

11. Suggested scan workflow

Run these in order for a clean, report-ready workflow:

1. `nmap -sn 10.0.3.0/24`

2. `nmap -Pn -n 10.0.3.4`

3. `sudo nmap -Pn -n -sS -p- --open --reason 10.0.3.4`

4. `sudo nmap -Pn -n -sS -sV -sC -O --open 10.0.3.4 -oA nmap_10.0.3.4_full`

5. `sudo nmap -Pn -n -sU --top-ports 200 10.0.3.4 -oN nmap_10.0.3.4_udp_top200.txt`