OSCP Notes: Identifying Target OS Type Using Nmap

✅ 1. Initial Nmap Scan (Fast)

bash

CopyEdit

nmap -T4 -p- --min-rate=1000 -v <IP>

- Scans all 65535 ports quickly
- Helps find web ports, RDP/SSH, custom ports

✅ 2. Detailed Scan on Open Ports

bash

CopyEdit

nmap -sCV -p <open-ports> <IP> -oN scan.txt

- -sC → default scripts
- -sV → version detection
- -oN → saves to file

🔍 Identify the Machine Type:

🖥️ Windows Clues

Port/Service	Clue
135, 139, 445	SMB/NetBIOS = likely Windows
3389	RDP = definitely Windows
WinRM (5985/5986)	Windows remote mgmt
Hostname includes WIN-	Common Windows pattern

bash

CopyEdit

nmap -p 445 --script smb-os-discovery <IP>

🐧 Linux Clues

Port/Service	Clue
22	SSH with OpenSSH banner
111	RPCbind (NFS) common on Linux
631	CUPS web printing (Linux)
Apache, Samba	Often used on Linux

bash

CopyEdit

nmap -p 22 --script ssh-hostkey <IP>

🌐 **Web Server (Linux or Windows)**

Port	Check
80, 443, 8080 etc	HTTP(S) → check manually

bash

CopyEdit

whatweb http://<IP>

bash

CopyEdit

curl -I http://<IP>

Look for:

- Server: Apache → Linux
- Server: Microsoft-IIS → Windows

□ Pro Tip:

Add this to your flow:

bash

CopyEdit

nmap -sV -sC -O <IP>

- -O → OS detection (not always accurate, but helpful)