LINUX MACHINE (No credentials yet)

🔍 **Step 1: Service Enumeration**

bash

CopyEdit

nmap -sC -sV -p- <IP>

Look for:

- **SSH (22)** → Skip for now, unless bruteforce is justified
- **FTP (21)** → Check for anonymous login:

bash

CopyEdit

ftp <IP>

Name: anonymous

- **HTTP (80, 8080)** → Web enumeration

bash

CopyEdit

gobuster dir -u http://<IP> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

whatweb http://<IP>

- **NFS (111/2049)** → List shares:

bash

CopyEdit

showmount -e <IP>

mount -t nfs <IP>:/share /mnt/nfs

- **SMTP (25)** → User enumeration:

bash

CopyEdit

smtp-user-enum -M VRFY -U users.txt -t <IP>

🎯 **Step 2: Exploit or Find Credentials**

- **Check for exposed files via web or FTP** (e.g., config.php with DB creds).
- **Bruteforce only if it makes sense**, and allowed in the lab or exam.

bash

CopyEdit

hydra -l user -P rockyou.txt ssh://<IP>

- **RCE via web upload / LFI → reverse shell**

□ WINDOWS MACHINE (No credentials yet)

🔍 **Step 1: Service Enumeration**

bash

CopyEdit

nmap -sC -sV -p- <IP>

Look for:

- **SMB (139/445)** → Try null sessions:

bash

CopyEdit

smbclient -L //<IP> -N

enum4linux-ng <IP>

- **WinRM (5985/5986)** → Useful **after** you get creds
- **HTTP (IIS)** → Same as Linux, check for exposed web services

bash

CopyEdit

gobuster dir -u http://<IP> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

- **RDP (3389)** → Not useful until you have valid credentials

---

🎯 **Step 2: Exploit or Leak Credentials**

- SMB shares may contain .txt, .xml, .ps1, or .config files with hardcoded creds.
- If it's a web app:
    - Check for **default creds** (admin:admin, guest:guest)
    - Look for **SQLi** or **command injection**
- Use **Responder** if you're in a position to poison responses (rare on standalone)

□ Other Entry Points:

- **Misconfigured services**

- **Known exploits** from banners
- **Leakage from file disclosure**
- **Database access via web + creds reuse**
- **Shellshock / Apache exploits / CVEs** matching version info

---

Once You Get Initial Access:

- On Linux: Check ~/.ssh, /etc/passwd, cron jobs, sudo perms
- On Windows: Enumerate with winPEAS, PowerView (if allowed), look for user.txt

---

TL;DR: No creds? Try these paths:

Path	Try On
FTP anonymous login	Linux
SMB null session	Windows
Web-based RCE/LFI	Both
Exposed config files	Both
NFS mounting	Linux
Hydra SSH bruteforce	(only if justified)
HTTP auth default creds	Both
Gobuster / Nikto / WhatWeb	Both

Step-by-Step Plan — No AD Creds Given

---

1. Identify the DC and AD Scope

Run Nmap on all IPs:

bash

CopyEdit

nmap -sC -sV -Pn -oN <ip>.txt <ip>

Look for:

- DC: ports 88, 389, 445, 135, 3268
- Other Windows hosts: usually only 445, 135, 5985, etc.

Label boxes:

diff

CopyEdit

- DC: likely domain controller

- Clients: other Windows members

🎯 **2. Start With Likely Foothold Machine (Non-DC)**

- Pick a Windows machine **not the DC**
- Look for:
    - SMB shares
    - Web services (port 80/443/8080)
    - WinRM (5985)
    - Local privilege escalation path

This is your likely **foothold target**.

□ 3. Enumerate SMB Shares Without Creds

bash

CopyEdit

smbclient -L //<ip> -N

or

bash

CopyEdit

crackmapexec smb <ip>

If anonymous login works, try:

bash

CopyEdit

smbclient //<ip>/sharename -N

Look for:

- Leaked password

- Public scripts
- Configs or backups with creds

🌐 4. Enumerate Web Services

If you find a website:

- Try gobuster, nikto, manual browsing
- Look for login forms or file uploads
- Try default creds (admin:admin, etc.)

□ 5. Exploit a Local Vulnerability

If you get a **shell as low-priv user**, try:

- Privilege escalation to SYSTEM
- Dumping hashes or tickets
- Reuse creds across other machines

□ 6. Pivot to Domain with Looted Creds

Once you escalate on a machine:

- Dump credentials (e.g., mimikatz, lsass, sam)
- Use them to:
    - Access other machines
    - Query the domain
    - Use evil-winrm, crackmapexec, etc.

🚫 Don't:

Mistake	Why It's Bad
Start with the DC	Usually patched, fewer footholds
Ignore SMB/Web	Most common initial access
Skip manual recon	Auto tools miss things
Assume creds will come later	You might need to find them early

---

□ Mindset:

Without creds = **recon is everything**
→ Look for misconfigs, leaks, weak shares, or exposed apps.

✅ **TL;DR – "No AD Creds" Action Plan:**

Step	Action
🔎 1	Identify DC + likely clients
□ 2	Enum SMB for anon access or misconfigs
🌐 3	Check all web ports for low-hanging fruit
□ 4	Exploit user → escalate privileges
🔓 5	Dump creds → lateral movement
□ 6	Use dumped creds to pivot into AD
