**8. Lateral Movement Simulation**

Step 1: Enable File Sharing on the Victim Windows Machine

1. On your target Windows machine (the one being accessed), create a shared folder:
   * Create a folder: C:\Shared
   * Right-click > Properties > Sharing tab > Share...
   * Share with “Everyone” (read/write) for testing purposes (adjust later for security)
2. Get the Windows VM's IP address:
3. ipconfig

Step 2: Access Shared Folder from the Attacker Machine

From Another Windows VM:

Open File Explorer > type:

\\192.168.100.10\Shared

OR in PowerShell:

net use Z: \\192.168.100.10\Shared

copy Z:\example.exe C:\Users\Attacker\Desktop\

From Kali Linux:

Use the smbclient tool:

smbclient //192.168.100.10/Shared -U <username>

Then use commands like:

get somefile.exe

put evil.exe

Step 3: Analyze Logs on the Victim Windows Machine

Open Event Viewer and go to:

Windows Logs > Security

Look for:

|  |  |
| --- | --- |
| Event ID | Meaning |
| 4624 | Successful logon |
| 5140 | A network share was accessed |
| 5145 | A file was accessed over SMB |
| 4663 | Object access (if auditing is enabled) |

Enable object access auditing if needed:

* Local Security Policy > Advanced Audit Policy Configuration > Object Access > Audit File System