Challenge: **Hack, Grab, and Stay – The Blue Server Takeover**

Challenge: Hack, Grab, and Stay – The Blue Server Takeover

Recreate the full attack chain on the vulnerable "Blue" machine — from scan to persistence.

Task 1: Discover the Target Machine

Objective: Identify the IP address of the vulnerable Windows ("Blue") VM on your network.
Instructions:
Use a network discovery tool to find live hosts.
Commands:
`netdiscover` `nmap`
Expected Output:
An IP address belonging to a Windows 7 machine (e.g., `192.168.1.50`).
Validation:

> Submit the target IP: `___________`

Task 2: Scan for SMB Services

Objective: Confirm that SMB ports (139 and 445) are open on the target.
Instructions:
Run an Nmap scan targeting SMB ports.
`namp <ports> <options> <IP Address>`
Expected Output:
Both ports should be in `open` state.
Validation:

> Are ports 139 and 445 open? ☐ Yes ☐ No

Hint: SMB is used for file sharing in Windows—and is the entry point for EternalBlue.

Task 3: Check for MS17-010 Vulnerability

Objective: Verify that the target is vulnerable to EternalBlue (CVE-2017-0144).
Instructions:
Use Nmap's vulnerability script.
`namp <ports> <options> <IP Address>`
Expected Output:
Output should include: `VULNERABLE` or `The target is vulnerable`.
Validation:

> Does the scan confirm the MS17-010 vulnerability? ☐ Yes ☐ No

Hint: This flaw affects unpatched Windows 7/Server 2008 machines.

Task 4: Exploit Using EternalBlue

Objective: Gain remote access to the Blue machine using Metasploit.
Instructions:
Launch the EternalBlue exploit in Metasploit.
`msfconsole`
Expected Output:
A `meterpreter >` shell prompt.
Validation:

> Did you get a Meterpreter session? ☐ Yes ☐ No

Hint: Ensure your Kali IP (`LHOST`) is correct and the VMs can communicate.

Task 6: Establish Persistence

Objective: Configure the system to reconnect to you after reboot.
Instructions:
Use Meterpreter's built-in persistence script.

Expected Output:
Message confirming a registry-based backdoor (e.g., in `HKCU\...\Run`).
Validation:

> Screenshot or note the name of the registry value created (e.g., `jUxPvQ`): `__________`

Hint: Persistence ensures long-term access—common in real attacks.

Task 7: Submit Your report and findings!

Objective: Prove you completed the full attack chain.
Instructions:
Submit both secret codes to your instructor or automated validator.
Required Submission:

- 1 : Open Ports
- 2 : Vulneribilities Found
- 3 : Access Gained
- 4 : Access Persisted

Congratulations! You've ethically recreated a real-world attack—from scan to persistence!