CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Penetration Testing in Microsoft Windows

At the end of this module, each student must submit a report indicating the completion of the following tasks. **Make sure you take screenshots as proof**.
You need to power on and start the following VMs for this assignment.

- **Internal Kali**
- pfSense VM (power on only) -Optional, as Internal Kali is used as attacker VM here in this assignment)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

Task A. Exploit SMB vulnerability on Windows XP using Metasploit framework (30 pts)

Please activate Windows XP clock by following the document posted under Module-3 or demonstrated in class.

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. **(2 pts)** Network Scanning: Run an Nmap scan against the target machine to find
    - open ports
    - running services
    - Smb vulnerabilities

    Submit the screenshot of the Nmap command used with the relevant scan results

2. **(3 pts)** Identify the SMB port number (default: 445) to confirm that it is open. Briefly explain (2–3 sentences) of what MS08–067 is and why was it severe?

3. **(2 pts)** Launch Metasploit Framework and ***Search for the module related to MS08-067***
4. **(2 pts)** ***Select:*** exploit/windows/smb/ms08_067_netapi
5. **(2 pts) Set payload:** windows/meterpreter/reverse_tcp
6. **(2 pts) Configure:** RHOSTS, LHOST and LPORT
7. **(2 pts)** Display the configurations and screenshot of "show options"
8. **(5 pts)** Run exploit and confirm Meterpreter session
9. **(5 pts)** Explain why the exploit succeeded (or did not succeed)
10. [Post-exploitation] **(5 pts):**
    a. Capture screenshot
    b. Display system's local date/time
    c. Retrieve SID
    d. Identify current process ID
    e. Gather system information

----------End of Task -A----------

Task B. Testing Eternal Blue (MS17-010) Against Windows Server 2022 (10 pts)

In this task, try to exploit the **EternalBlue** vulnerability on Windows Server 2022. You **may or may not** establish a reverse shell connection to Windows Server 2022.

- **(5 pt)** Show your results and configuration.
- **(5 pt)** Explain why EternalBlue typically fails against Windows Server 2022.

NOTE: You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

----------End of Task-B----------

Task C. Exploit Windows 7 with a deliverable payload (60 pts).

In this task, you need to create an executable payload in **Internal Kali** with the required configurations below.

1. **Generate Executable Payload (5 *2pts = 20 pts)**

[Submit the screenshot for each step]

a. Create a Windows executable payload
b. Use reverse_tcp
c. LPORT = 4444 (you may change it)
d. LHOST = Internal Kali IP
e. Payload filename = Your MIDAS ID.exe (for example, **svatsa.exe**)

2. **Host and Deliver Payload (5* 2 pts = 10 pts)**

[Submit the screenshot for each step]

a. Start a web server on Internal Kali
b. Upload payload to web root (Apache or python http server)
c. Download payload from Windows 7
d. Configure Metasploit handler
e. Execute payload on target

3. **Post-Exploitation (10 pts)**

[Submit the screenshot for each step]

After the session is established, i**n Meterpreter**:

a. **(2 pt) E**xecute the command to take a screenshot of the target machine if the exploit is successful.
b. **(4 pt)** Create a text file with the name as **YourMIDAS**.txt (for example, **svatsa.txt**) and put the current timestamp in the file.
c. **(2 pt)** Upload the above text file (YourMIDAS.txt) to the Windows 7 Desktop folder
d. **(2 pt)** Log in to Windows 7 and verify if the file exists

HINT: To learn about the command used in Meterpreter, type '?' and hit "Enter" or "Return" key.

[Privilege escalation]

4. Gain Administrator Privileges (5 pts)
[Submit the screenshot for each step]

a. Background the current session

b. Attempt privilege escalation (gain administrator-level privileges)

c. Regain elevated session

5. Create Malicious Admin Account (5 * 2 pts =10 pts)
[Submit the screenshot for each step]

Since you have now gained the elevated privilege, in the Meterpreter shell running on the attacker side (Internal Kali),

a. **(2 pts)** Create a new user account (use your real name) with a valid password (do not use your real password)

b. **(2 pts)** Add this user account to the Administrators group
c. **(2 pts)** Create three additional users with their passwords
d. **(2 pts)** Display the password hashes using correct command in meterpreter shell
e. (2 pts) Redirect/copy those password hashes, of all the users created, in a new text file named as, **winHash.txt. Display the contents of the file, WinHash.txt**

[Remote Access via RDP]

6. (3 pts) In a new terminal in Internal Kali, enable RDP and log in using the malicious account created in the previous step.

7. **(2 pts)** Browse user folders in Windows 7

----------End of Task-C----------