CYSE 301: Cybersecurity Technique and Operations

Assignment: Ethical Hacking (Windows Server 2008)

In this assignment, each student will be familiar with the basic usage of the Metasploit framework and try different exploits against the target Windows Server.

You will be using the following VMs in the Module 1 blueprint.

- Windows Server 2008 (Target)
- pfSense VM (power on only)
- External Kali (attacker)

Task A. Select your exploits

1. Use Nessus to find all FIVE critical security issues in the target Windows Server 2008.
2. Search for an exploit that targets a security issue other than MS17-010.
3. Discuss the exploit you select, such as how it works and the required configurations, etc.

Task B. ms17_010_eternalblue

Use **ms17_010_eternalblue** and reverse_tcp as the exploit and payload to launch the attack. You need to use the following configuration for the reverse shell.

1. Listening Port: Use **30123** as the listening port number.
2. Background your meterpreter session. Then display the list of your active session(s) with connection peers.

Task C. Basic Information harvesting

Once you have established the reverse shell connection to the target Windows Server 2008, complete the following tasks in your meterpreter shell:

1. Take a screenshot of the target machine, then display it.
2. Create a text file on the External Kali named "IMadeIT-**YourMIDAS**.txt" (replace **YourMIDAS** with your university MIDAS ID) and put “This is XXX, hello pumpkin!” in the file. Then, upload this file to the target's desktop (Windows Server 2008). Then log in to Windows Server 2008 and check if the file exists. You need to show me the command that uploads the file.
3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot/”.
4. Access the Windows Command Prompt via the meterpreter shell, then create a malicious user, YourMIDAS, with admin privilege in the Windows Server 2008. Please replace XXX with your MIDAS ID.
5. Remote access to the malicious account created in the previous step and browse the files belonging to the other users in the RDP.

Task D. Extra Credit (10 points each)

- Other than the plain reverse_tcp payload, we can find a list of other payloads with different features. Let's try to use a new payload in Task B with RC4 encryption.
- Use Wireshark on External Kali to explore the difference between a traditional reverse_tcp payload and reverse_tcp payload with RC4 encryption. Show me your analysis.