Assignment 3

New Attempt

- Due Oct 1, 2024 by 11:59pm
- Points 100
- Submitting a file upload
- File Types pdf

Due: Tuesday, October 1, 2024 (11:59 PM). Please submit your assignment on Canvas as a PDF.

Post Exploitation

In this assignment, you will explore the options regarding post-exploitation concepts. We assume that you have a successful Meterpreter session throughout the entire assignment.

The commands in Metasploit that you are going to use in this assignment are identical to those in the previous assignment. Also all of the exploits you are going to use reside under `post/windows/…` path in Metasploit. The keyword `post` in Metasploit indicates post-exploitation.

1 Process Migration (20%)

The first step towards a successful Meterpreter post exploitation is to migrate the Meterpreter's process to a core Windows process so that the user at the target machine is not able to "kill" the Meterpreter session.

Task 1: Using Meterpreter's command `ps` find a **suitable** process to migrate to. What process did you choose and why? What is the ID of this process?

Task 2: Force to background the current Meterpreter sessions and find the **proper** post exploit to use for process migration. What exploit did you select?

Hint: Search exploits under post/windows.

Task 3: Perform the exploit and report the commands/options you used.

2 Killing the Antivirus (10%)

After migrating Meterpreter to another process the next step is to kill the antivirus system.

Task 4: Select the proper exploit to kill the antivirus system of the target machine (if any). What exploit did you use?

Task 5: Report the commands/options of the post exploit you used to kill the antivirus.

3 Obtaining System Privilege (20%)

The following tasks are about getting system privileges on the target machine.

Task 6: What is the Meterpreter command to check the privilege level of the current Meterpreter session?

Task 7 What is the proper post exploit to escalate the privilege to the system level? Please note that this exploit does not always work. Perform the exploit and report the commands/options you used.

4 Persistence (20%)

In successful Meterpreter exploitation, after migrating to the process, killing the antivirus, and escalating to system privilege, the last step is to make Meterpreter **persistent**. If the Meterpreter becomes persistent, then, it starts after every boot of the target system.

Task 8: What is the **proper** post exploit to perform the persistence?

Task 9 Perform the exploit and report the commands/options you used.

Hint: You may need to use MSFVenom to create the payload. Use a port different from the port you used to initiate the current session.

Use the multi/handler module to run a Meterpreter exploit handler so that the persisted payload can connect back to you. Restart the victim machine.

Task 10: Confirm that a Meterpreter session is created when you log in back into the Windows machine. Report the commands you used to set up the multi/handler module and a screenshot of the current Meterpreter session that has been opened.

5 Credentials (30%)

Task 11: What is the Meterpreter command to get the hashes of all the user passwords on the system? Report the command and output with a screenshot. What is the hash format?

Task 12: What are the credentials for `admin` user? Explain the steps you used to extract the password with screenshots.

Task 13: Change the credentials for `admin` user. Explain the steps you used to change the password with screenshots. Verify the password changed using the steps from Tasks 11 and 12.

Task 14: How can these credentials be used to log in to the Windows 7 machine as admin?