Lab 8: Post Exploitation

Preliminaries

Refer to Lectures 7, 8 and 9 slides.

Tasks

Turn on Kali VM and Windows 7 VM. You should keep Metasploitable2 turned off, which is not needed in this lab.

Log into Kali VM, and start a terminal. Log into Win7 initially as 'Alex' (password: alex123). Then, complete the following tasks. Write your answers for all questions to your lab report.

1. **Privilege Escalation.**
   1.1 Follow Lecture 7 client-side exploitation slides to exploit the IE on Win7 VM to obtain a Meterpreter shell. Since you log into Win7 with the account 'Alex', the Meterpreter shell you get should also has the privilege of 'Alex'. Grab a screenshot to prove this. The screenshot should show the result of executing the following commands: 'getuid' and 'hashdump'. Note that the 'hashdump' command should not be successful, as it needs SYSTEM privilege to run.

   1.2 Follow Lecture 8 slides to escalate the privilege to 'NT Authority/System'. You should use a local exploit to achieve this. The difference from the lecture is that you should use 'ms18_8120_win32k_privesc' as the local exploit instead.
   a) Type all command lines to achieve the above into your lab report.
   b) Grab a screenshot to prove your success. The screenshot should show the result of executing the following commands: 'getuid', 'pwd', and 'hashdump'

   1.3 Follow Lecture 8 slides to kill the Meterpreter session obtained in Task 1.1, while keeping the session obtained in Task 1.2.
   a) Type all command lines to achieve the above into your lab report.
   b) Grab a screenshot to prove your success. This screenshot should include the result of executing the command 'sessions' under msfconsole.

2. **Information Gathering.**
   2.1 Get back to the Meterpreter session left in Task 1.3, and enter the command 'sysinfo'.
   a) Grab a screenshot showing the output of ‘sysinfo’.
   b) Explain each line of the output in your own words.

   2.2 Enter another Meterpreter command 'hashdump'.
   a) Grab a screenshot showing the output of ‘hashdump’.
   b) Based on this output, how many users accounts are currently available on the Win7 VM? (Hint: count the number of lines in the output)
   c) What are their account names? (Hint: the user name appears in the first column of each line, with columns separated by ‘:’).

3. **Installing backdoors.**

3.1 Exit msfconsole and start it again, such that all previous handlers and Meterpreter sessions die. Then, follow Lecture 6 slides to exploit the SMB vuln on Win7 VM to obtain a reverse Meterpreter shell with user account 'NT Authority/System'. Based on this Meterpreter session, install a netcat backdoor at Win7 VM. **This netcat backdoor should run in client mode**. Follow the sketchy steps mentioned in Lecture 9 slides on alternative method to complete this.

a) Include all your command lines to achieve the above in your lab report.

b) Reboot the Win7 VM and login with 'Admin' account. Then, grab a screenshot on Kali terminal to prove your backdoor has connected to Kali successfully. This screenshot should show the following:

- The client-mode netcat (bound with cmd.exe) connects to the server-mode netcat at Kali.
- The result of executing the command:
  reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run

3.2 Suppose in the netcat session above, you have done all the pentesting jobs, and lastly you want to remove the netcat backdoor. Here you need to accomplish the following two items. First, remove the nc.exe from the C:\Windows\System32 folder. Second, remove the entry in Windows Registry to start nc automatically.

a) Include your command lines for completing these two items in your lab report.

b) Confirm the registry entry is successfully removed by executing:
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
And include the screenshot on the output of the above command in your lab report.

4. **Removing traces.**

4.1 In a Kali terminal, enter 'cd /var/log', where the log files are located.

a) How many files with the extension '.log' are under this directory?
(Hint: you can use '*ls -l *.log*' and then count the number of files, or use
'*ls -l *.log | wc -l*' to count it for you.)

b) When you use '*ls -l*' to list files in a directory, which option you should add to it in order to sort the list of files by the time of modification?
(Hint: you can use 'man ls' to find out.)

c) Use the option you figure out in b) to list all the '.log' files in /var/log, sorted by the time of modification. Grab a screenshot to prove the correctness of your command line.

4.2 In Win7 VM, login as Admin. Use 'Event Viewer' to examine the events of the 'System' and 'Application' categories under the 'Windows Logs' respectively.

a) How many events are logged under each category?

b) Grab a screenshot of each of them to prove your answer.

Note: To start Event Viewer, click 'Start' → 'Run' → enter 'eventvwr'

4.3 In Kali VM, use a Meterpreter session as described in Task 3.1 to execute the 'clearev' command. Grab a screenshot of the output of this command.

4.4 In Win7 VM, use 'Event Viewer' to examine the events under the 'System' and 'Application' categories again.
   a) How many events are present under each category now?
   b) Grab a screenshot of each of them to prove your answer.

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.