Lab 7: Netcat and Client-side Exploitation

Preliminaries

- Refer to Lecture 7 slides.
- For your convenience, the nc program is installed in Win7 VM in our school cloud and added to the system path already.

Tasks

Turn on all three VMs. Log into Kali VM, and start a terminal. Log into Win7 as Admin, and make sure the Windows Firewall is turned off. Then, complete the following tasks. Write your answers for all questions to your lab report.

1. Netcat.
   1.1 Use netcat to perform a banner grabbing on the SSH service on the Metasploitable VM.
      a) Type the command line used into your lab report.
      Hint: find out the port number used by the SSH service first.
      b) Based on the output, what is the SSH server software used on Metasploitable?
      c) What is the OpenSSH version number?
      d) Grab a screenshot to support your above answers.

   1.2 Use netcat to perform a banner grabbing on the MySQL service on the Metasploitable VM.
      a) Type your command line into the lab report.
      Hint: find out the port number used by the MySQL service first.
      b) Based on the output, what is the MySQL server version number?
      c) Grab a screenshot to support your answer.

   1.3 On the Win7 VM, use Notepad to create a text file with words "Genius is one percent inspiration and ninety-nine percent perspiration", and name it 'genius.txt', and save it under the 'Documents' folder. Use netcat to transfer this file to Kali VM and store it in '/home/kali/Downloads'. In doing so, you should run netcat in server mode on Kali VM.
      a) What are the command lines run in Kali VM?
      b) What are the command lines run in Win7 VM?
      c) Include a screenshot on your success. This screenshot should include the results of executing the command 'ls -l' on the '/home/kali/Downloads' folder.

   1.4 On the Win7 VM, create another text file with words "Whoever is happy will make others happy too", and name it 'happy.txt', and save it under the 'Documents' folder. Use netcat to transfer this file to Kali VM and store it in '/home/kali/Downloads'. This time, you should run netcat in server mode on Win7 VM.
      a) What are the command lines run in Kali VM?
      b) What are the command lines run in Win7 VM?
      c) Include a screenshot on your success. This screenshot should include the results of executing the command 'ls -l' on the '/home/kali/Downloads' folder.

Note: In accomplishing 1.3 and 1.4 above, you may destroy those two text files accidentally. If you see their sizes are of 0 byte, then they are destroyed. If so, you should restore their contents before trying to transfer them.

2. Browser Exploitation.
   2.1 Follow the lecture slides to exploit IE 8. In this exploitation, you should set those advanced options that will enable the injected Meterpreter session to migrate to a new 'explorer.exe' process. Moreover, after the exploitation, you should manually migrate the Meterpreter session to the true 'explorer.exe' process.
      a) Include all command lines to achieve the above in your lab report.
      b) Include a screenshot to prove your success. This screenshot should include the results of executing the following commands 'getuid', 'getpid', and 'ps -S explorer' after you have completed the exploitation required above.
      c) Don't exit from the meterpreter session obtained. It is needed in the task 2.2 below.

   2.2 On the Kali VM, start a new terminal other than the one used for exploiting IE. Run the command 'sudo ss -antp'.
      a) Include a screenshot on the output of the above commend.
      b) Based on the output, explain which established TCP connection is used by the meterpreter session obtained in Task 2.1 (specifically, you should give the IP address and port number at Kali side, and the IP address and port number at Win7 side for this TCP connection).

3. Adobe Reader Exploitation.
   3.1 Follow the lecture slides to exploit the Adobe Reader on Win7 VM. In this exploitation, you should set those advanced options that will enable the injected Meterpreter session to migrate to a new 'explorer.exe' process. Also, after the exploitation, you should manually migrate the Meterpreter session to the true 'explorer.exe' process.

   During the above exploitation, you should upload the generated malicious PDF file to the 'Documents' folder of Admin. You should do this using the netcat program as you have practised in Task 1.
      a) Include all command lines to achieve the above in your lab report.
      b) Include a screenshot to prove your success. This screenshot should include the results of executing the following commands 'pwd', 'getpid', and 'ps -S explorer' after you have completed the exploitation required above.

   3.2 Use the Meterpreter session obtained above to grab a screenshot of the remote Win7 desktop. The Meterpreter command to use can be found in Lecture 6 slides. By default, this screenshot picture will be saved to the '/home/kali' directory.
      a) What's the Meterpreter command line for this?
      b) Send this picture by email to you, and then insert this picture to your lab report.

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.