Lab 6: Meterpreter and vncinject

Preliminaries

Refer to lecture slides in Week 6, and some slides in Week 5.

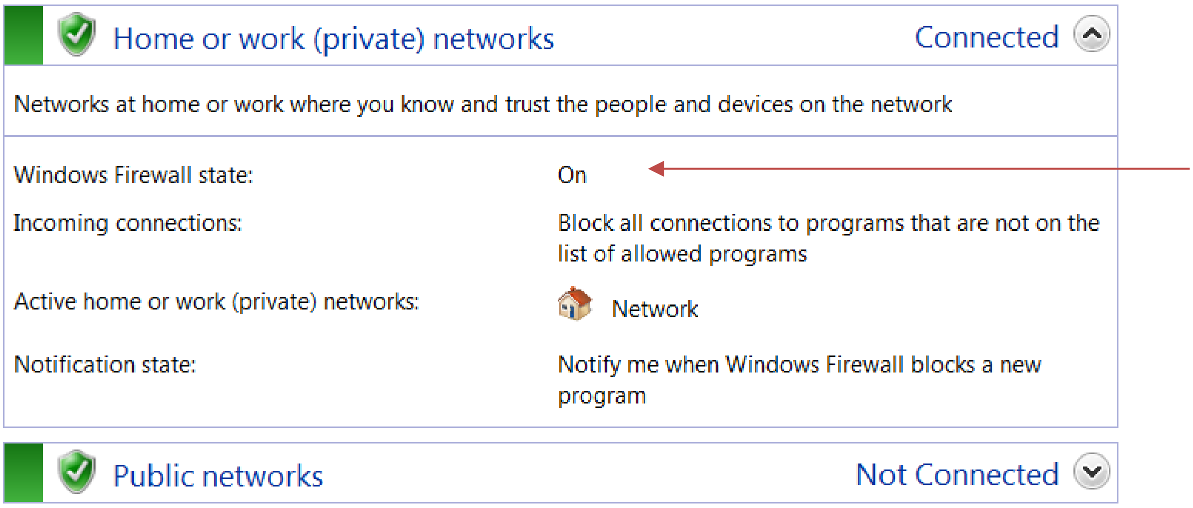
Tasks

Turn on Kali VM and Win7 VM. Log into Kali VM, and start a terminal. Log into Win7 as Admin. Note that to make the Win7 VM vulnerable, we turned its firewall off when creating it.

Complete the following tasks. Write your answers for all questions to your lab report.

1. Meterpreter Basics.

1.1 Turn on 'Windows Firewall' at the Win7 VM as shown in the picture below.



Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

After you have done the above, click the “Allow a program or feature through Windows Firewall” link located in the left column of Control Panel.

a) Based on the info displayed, name at least three programs or services that are allowed to go through the Firewall.

b) "File and Printer Sharing" should be one of the services shown as allowed. This service is provided by the SMB server discussed in the lecture, which mentions that the SMB server in this Win7 VM has a vulnerability. According to the GVM report on the Win7 VM obtained in the last lab, what is the Microsoft Security Update number of this vuln?

1.2 Follow the basic steps in lecture to exploit this vuln, but use 'windows/x64/meterpreter/bind_tcp' as payload. Try to obtain a Meterpreter session to Win7 VM.

a) Are you able to succeed?

b) If not, explain why.

Hint: Refer to lecture slides in Week 5 about 'bind' and 'reverse'. Basically, 'bind_tcp' will wait for a TCP connection at the TCP port 4444 of the target from the attacking machine. Based on this, explain why this connection cannot be established.

1.3 Use 'windows/x64/meterpreter/reverse_tcp' as payload this time. Try to obtain a Meterpreter session to Win7 VM.
   a) Include every step (especially the command line involved) into your lab report.
   b) Include a screenshot on your success. This screenshot should include the results of executing the following commands: 'getuid' and 'pwd'.
   c) Why can you succeed this time?

1.4 Turn off Windows Firewall for 'Home or Work Networks' at the Win7 VM. Grab a screenshot to prove this in your lab report.

1.5 Again use 'windows/x64/meterpreter/bind_tcp' as payload. Try to obtain a Meterpreter session to Win7 VM.
   a) Are you able to succeed this time?
   b) If yes, include a screenshot on your success. This screenshot should include the results of executing the following commands: 'getuid' and 'ipconfig'.
   c) At Kali VM, start a second terminal and issue the command 'sudo ss -antp'. Attach a screenshot on its output. Which TCP connection shown in the output is used by the obtained Meterpreter session? (Give the connection's local IP addr and port number and peer IP addr and port number)

2. Meterpreter In Depth.

2.1 Continue on the Meterpreter shell obtained in Task 1.5. Use a Meterpreter command to find out the PID of the process into which the Meterpreter shell is injected.
   a) What is the Meterpreter command used?
   b) What is the obtained PID?

2.2 Use a Meterpreter command to list all of the processes currently running in the target.
   a) What is the Meterpreter command used?
   b) Scroll the output to examine each process. Which process has the PID obtained in Task 2.1?

   Hint: PPID in the output means Parent Process ID, you can ignore the PPID column from the output.

   c) Which user account the process obtained above is running under?

   Hint: Look at the 'User' column of the process list.

2.3 On the Win7 VM, open a command window and run the 'tasklist' command.
   a) Include a screenshot on the output of ‘tasklist’.
   b) Do you see the same list of processes as seen in Task 2.2?

2.4 a) Is the user account obtained in Task 2.2c the same as the result of 'getuid' in Task 1.5?
   b) Why? (**Hint**: think about the DLL Injection technique)

2.5 Use Meterpreter to log some key strokes without migrating to 'explorer.exe' first. That is,
   i. run 'keyscan_start'
   ii. generate some keystrokes on Win7 VM

iii. run 'keyscan_dump'
iv. run 'keyscan_stop'

a) Did you see some output in the Step iii above?
b) If not, explain why.

Hint: Think about the user account used by Meterpreter.

2.6 Find out the PID of the process 'explorer.exe'.

a) Give your Meterpreter command line for this.
b) Include the result into your lab report.
c) Also, which user account the 'explorer.exe' is running under?

2.7 Migrate Meterpreter to the process 'explorer.exe'.

a) Give your Meterpreter command line for this.
b) Verify the migration is successful with a Meterpreter command and its output. Include a screenshot about this.

2.8 Repeat Task 2.5.

a) Are you successful this time?
b) If yes, include a screenshot to prove this.

3. vncinject.

3.1 Use 'windows/x64/vncinject/reverse_tcp' as payload. Use the default option for 'ViewOnly'. Follow the lecture slides to obtain the desktop of the Win7 VM.

a) Include every step (especially the command line involved) into your lab report.
b) Include a screenshot on your success. This screenshot should have 'TightVNC' in the top bar.
c) Also, are you able to control the target via the obtained desktop? Why?

3.2 Repeat the above task, but set 'ViewOnly' to 'false' this time.

a) Include every step (especially the command line involved) into your lab report.
b) Include a screenshot on your success. This screenshot should have 'TightVNC' in the top bar.
c) Are you able to control the target via the obtained desktop this time? Why?
d) Compare the desktop you obtain and the real desktop. Will they be updated simultaneously upon your actions in either side?
e) Based on the above, why should you be very careful in setting 'ViewOnly' to 'false'?

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.