**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

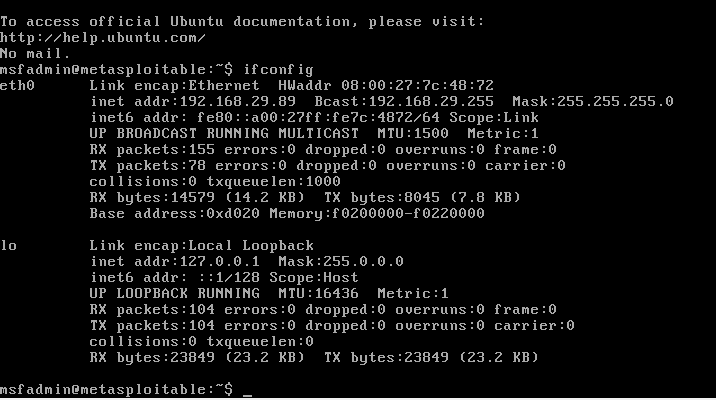
● msfvenom is a combination of msfpayload and msfencode Use msfvenom -h to get an overview Pre-requisites

● 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.



**Launch msfconsole on Kali Linux.**

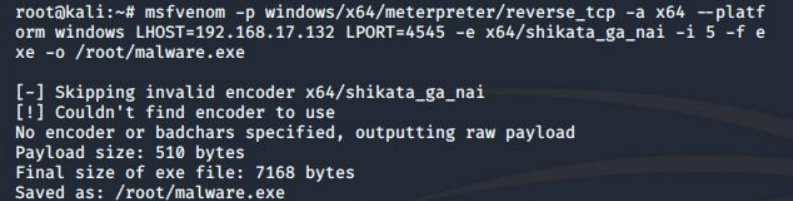
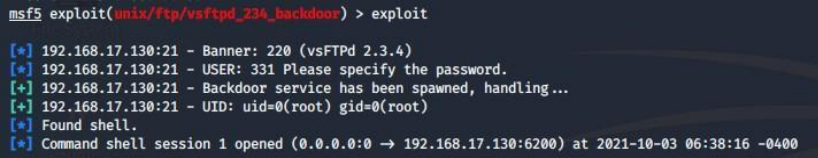


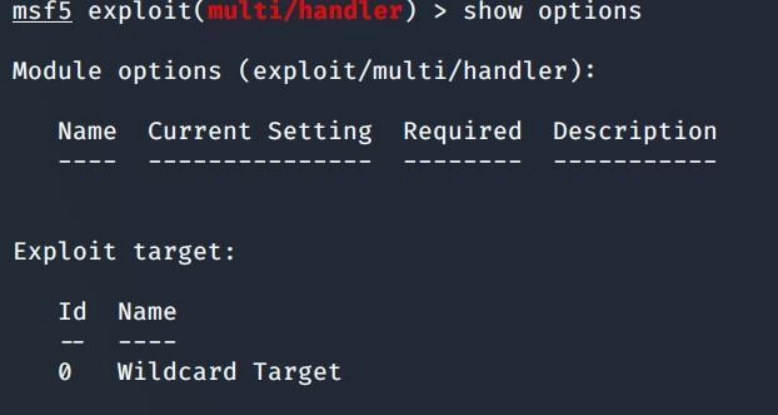
FTP Backdoor Exploit

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

**Set Hosts by accessing vsftpd\_234\_backdoor.**

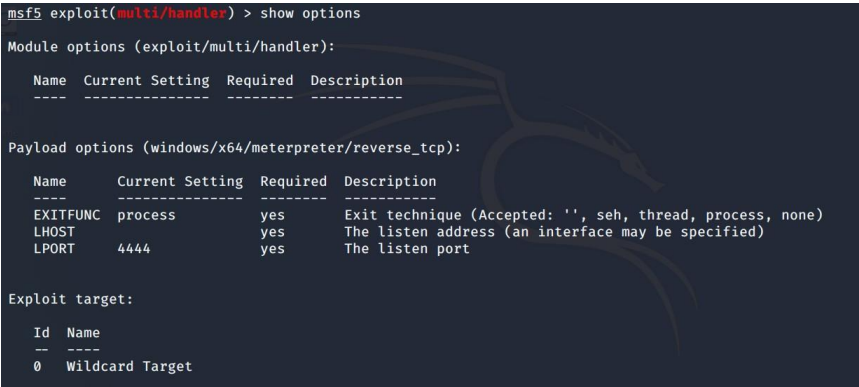


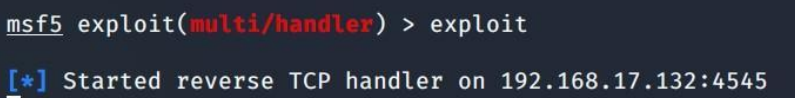
**Exploit the Machine.**

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

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

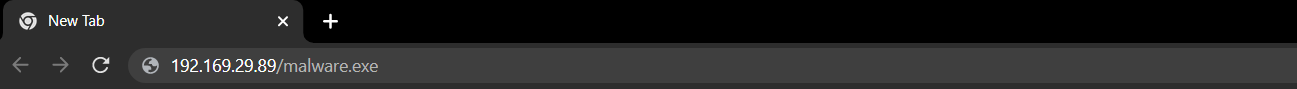






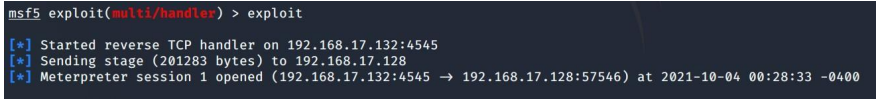
**Set the ports and exploit.**

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





**Check the terminal after opening the .exe file.**



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.