

**Information Security proposal**

**Performing Reverse\_tcp Attack(using Metasploit)**

**Syed Ali Hamza Ghaznavi**

**22-11091**

**Muhammad Umar Ali**

**22-10507**

**Hamza Ayub**

**22-11085**

**Ali Afzal**

**21-10321**

**Coding and Screenshots**

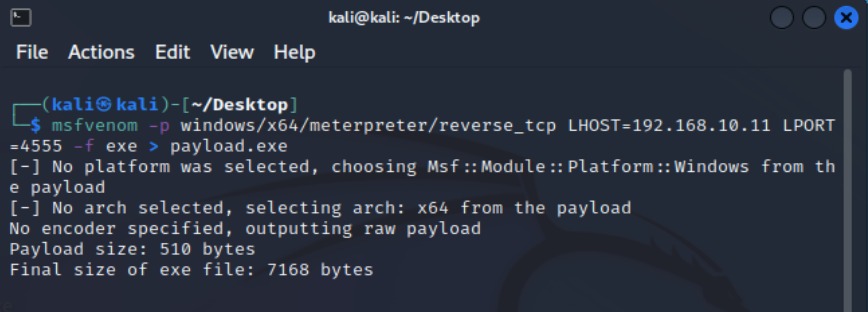
The First step we did was to find out the IP of host/attacker machine. Then we checked which port is available on the Public IP of machine. We then accessed advanced router settings to enable port forwarding on the port we have selected previously. We the use msfvenom to create a payload. We started a http server on kali machine because all our command execution will be through http server. The payload is downloaded on victim machine using windows cmd. We set up handler using msfconsole to listen and once the payload.exe is opened on victim machine and the directory can be assessed. Then commands can be executed. They are also chances the windows defender can detect Exe file and block it. Files can be downloaded. Webcam can be accessed. Screenshots can be taken. Files can be edited and corrupted and further other manipulation of data can be done.

**Creating payload**

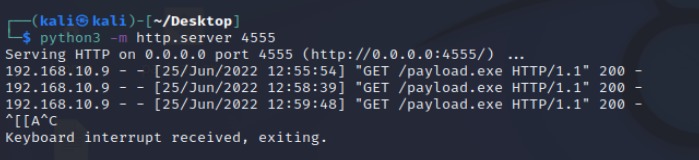
We require

* architecture of victim machine(windows 64 bit)
* type of shell(reverse tcp)
* IP address of attacker/Kali machine (192.168.10.11)
* PORT for forwarding(4555)

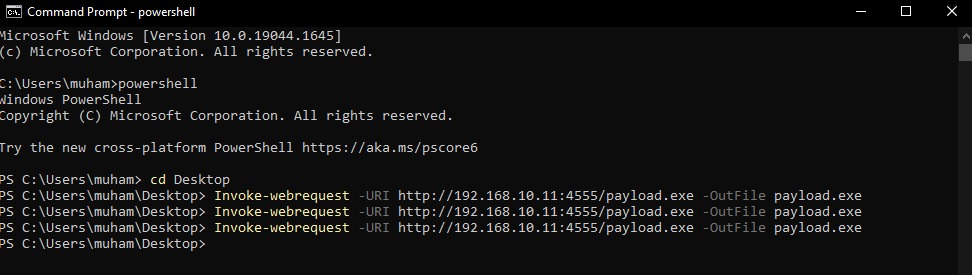
payload.exe is created



**Starting an HTTP server**



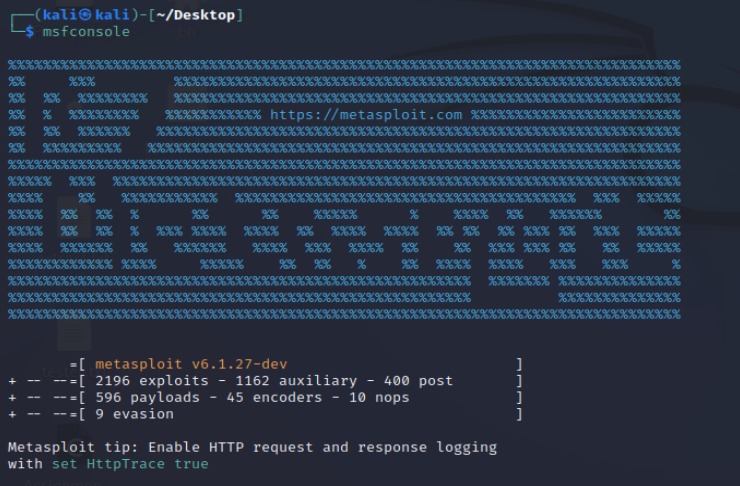
**Downloading payload on victim machine via CMD**



A picture containing text

Description automatically generated

**Starting up msfconsole**



**Setting up handler**



**Setting up payload architecture**

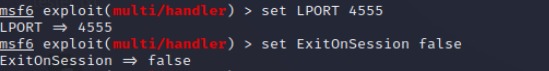


**Setting up LHOST, LPORT and Exit session condition**

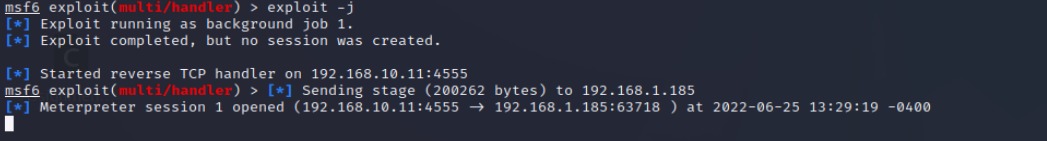
**LHOST**



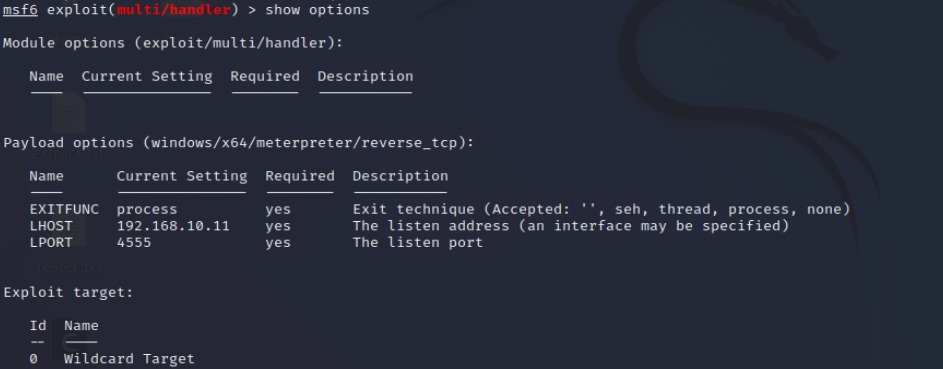
**LPORT**



**Executing payload**

****

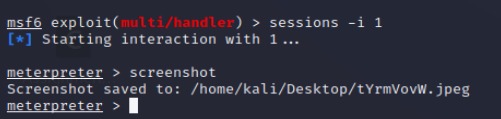
**Interactive session**



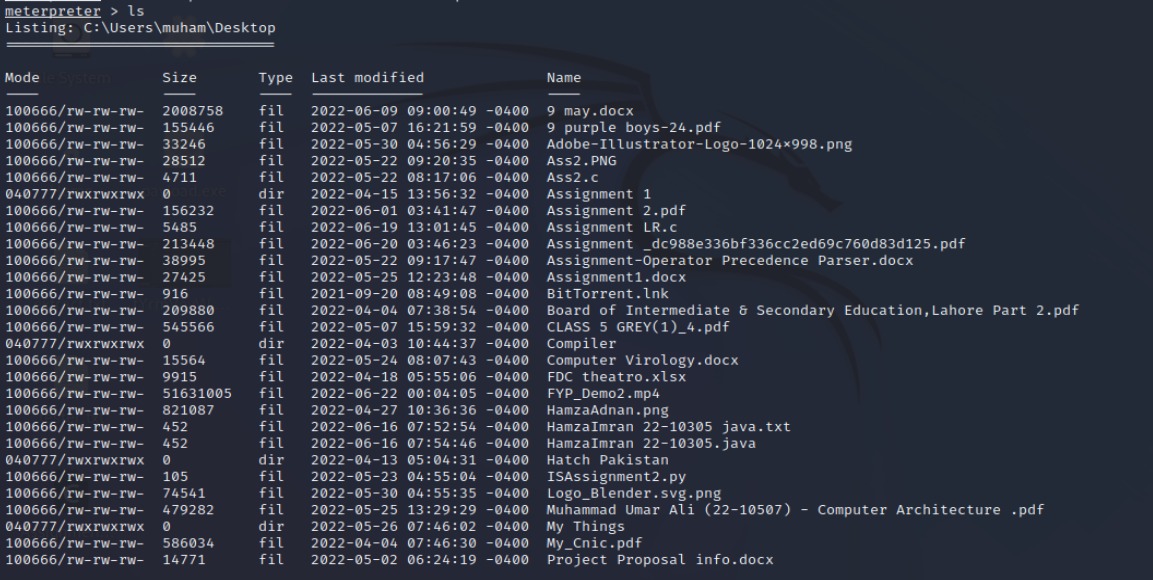
**Commands**

**Help is typed to see what commands are available to start exploiting.**

1. **Taking screenshot of windows machine**



1. **Seeing files in the directory by using ls**

****

1. **Reading file named Passwords with extension.txt**

**Text

Description automatically generated**

1. **Downloading file named Passwords with extension.txt**

Text

Description automatically generated

**Kali machine has downloaded the files on desktop**

**Graphical user interface

Description automatically generated with medium confidence**