



Introduction about Metasploite

Metasploit is a popular and powerful framework used for penetration testing, exploiting vulnerabilities, and security research. It contains a wide range of tools and modules for various tasks in the security testing process. Below are some of the main components and contents of the Metasploit Framework

History of Metasploite :

The Metasploit Framework is a popular open-source tool for developing and executing exploits against a target system. It was first developed by HD Moore in 2003 as a portable network tool using Perl, and has since evolved into a full-featured exploit development platform written in Ruby.

Metasploit Content

Modules :-

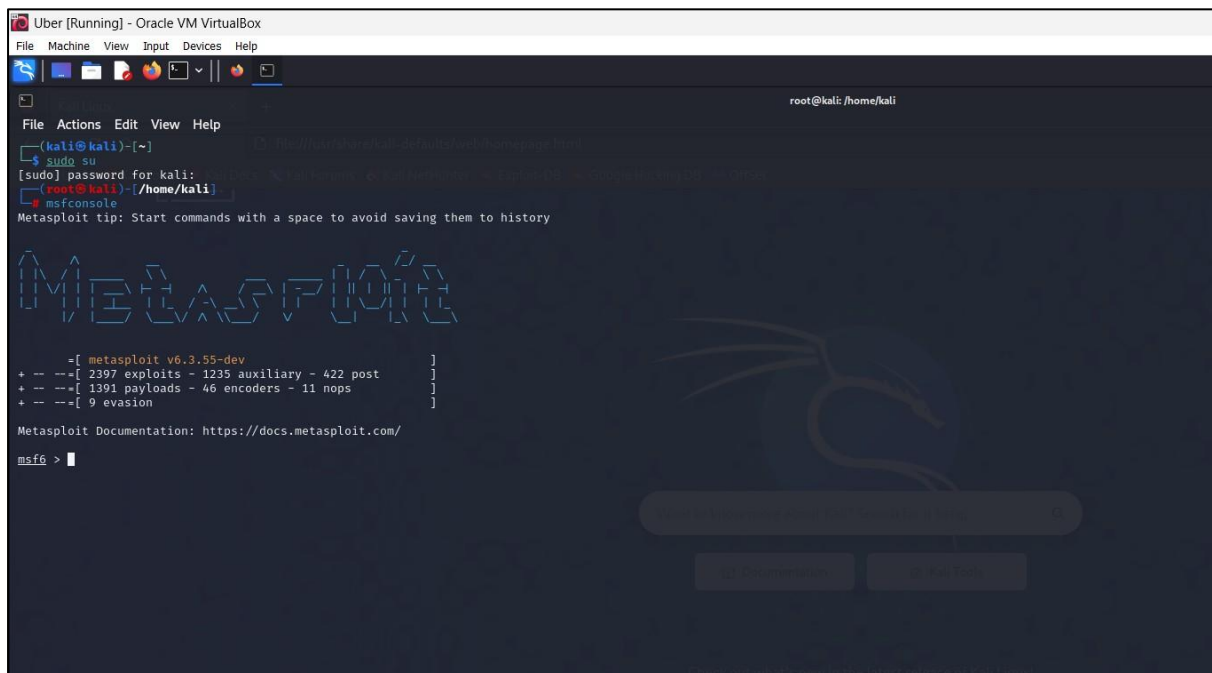
1. **Exploit Modules:** These modules are used to take advantage of vulnerabilities in target systems. Each exploit module is designed for a specific vulnerability in software or hardware.
2. **Payload Modules:** Payloads are the code that is executed after a successful exploit. These can range from simple commands to complex shells and reverse shells.
3. **Auxiliary Modules:** These modules are used for various tasks other than exploitation, such as scanning, fuzzing, DoS (Denial of Service), and enumeration.
4. **Post-Exploitation Modules:** These modules are used after successfully exploiting a target, helping gather information, escalate privileges, and maintain access.
5. **Encoders:** Used to modify payloads to bypass security mechanisms, like antivirus software, by encoding them in different ways.
6. **Nops:** Used to insert "no-op" (NOP) instructions in the payload to ensure it runs successfully, especially when dealing with buffer overflow exploits.
7. **Evasion:** A category used to avoid detection by firewalls, intrusion detection systems (IDS), and antivirus software.

Interfaces:

- Metasploite has different interfaces to ease our tasks

1. MSFconsole :

msfconsole is the primary command-line interface (CLI) for interacting with the **Metasploit Framework**. It is the most commonly used interface for penetration testers and ethical hackers when performing penetration testing, exploiting vulnerabilities, and post-exploitation activities.



```
Uber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /home/kali

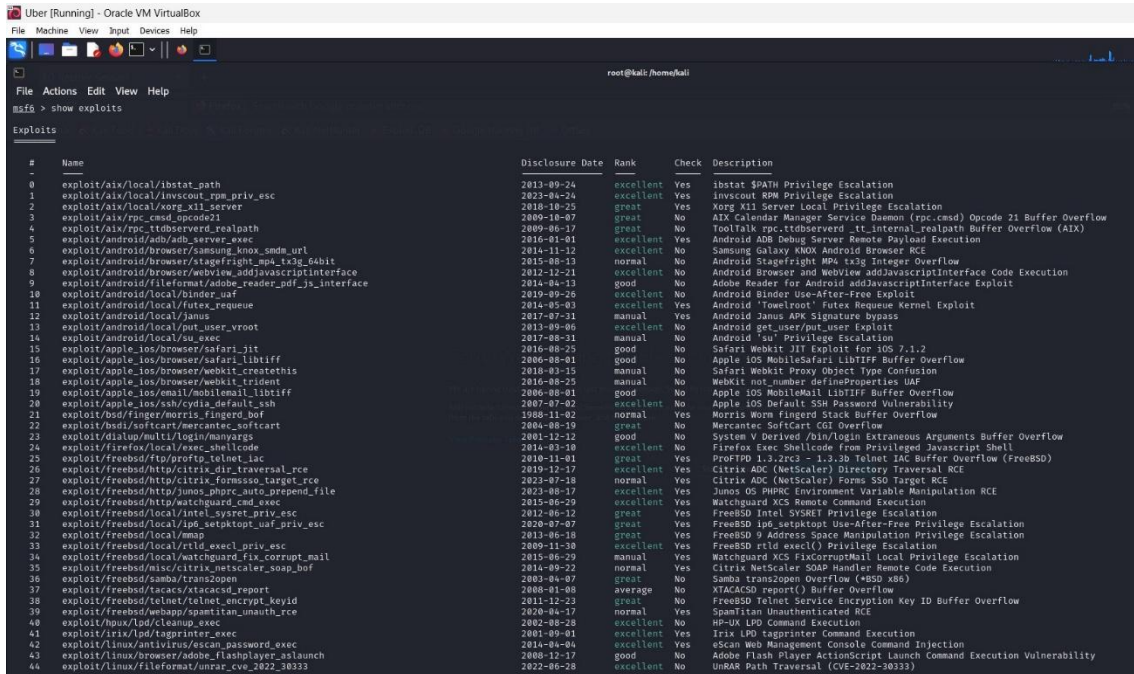
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

Metasploit

+ -- --[ metasploit v6.3.55-dev ]
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

1. Exploit Module:



#	Name	Disclosure Date	Rank	Check	Description
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat \$PATH Privilege Escalation
1	exploit/aix/local/invscout_rpm_priv_esc	2023-04-24	excellent	Yes	invscout RPM Privilege Escalation
2	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Privilege Escalation
3	exploit/aix/rpc_cmsd_rpcand21	2009-10-07	great	No	AIX Calendar Manager Service Daemon (rpc_cmsd) Opcode 21 Buffer Overflow
4	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd -it_internal_realpath Buffer Overflow (AIX)
5	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
6	exploit/android/browser/samsung_knox_smdm_url	2016-11-12	excellent	No	Samsung Galaxy Knox Android Browser RCE
7	exploit/android/browser/stagefright_mp4_tn3g_64bit	2015-08-11	normal	No	Android Stagefright MP4 tns3 Integer Overflow
8	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavaScriptInterface Code Execution
9	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-15	good	No	Adobe Reader for Android addJavaScriptInterface Exploit
10	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit
11	exploit/android/local/futex_reqqueue	2014-05-03	excellent	Yes	Android 'Towelroot' futex Reqqueue Kernel Exploit
12	exploit/android/local/Janus	2017-07-31	manual	Yes	Android Janus APK Signature bypass
13	exploit/android/local/pmt_user_vroot	2013-09-06	excellent	No	Android get-user/out-user Exploit
14	exploit/android/local/su_exec	2017-08-31	manual	No	Android 'su' Privilege Escalation
15	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No	Safari Webkit JIT Exploit for iOS 7.1.2
16	exploit/apple_ios/browser/safari_libtiff	2006-08-01	good	No	Apple iOS MobileSafari LibTIFF Buffer Overflow
17	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No	Safari Webkit Proxy Object Type Confusion
18	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No	Webkit not_number_defineProperties UAF
19	exploit/apple_ios/email/mobilemail_libtiff	2006-08-01	good	No	Apple iOS MobileMail LibTIFF Buffer Overflow
20	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
21	exploit/bsd/finger/morris_fingerd_bof	1988-11-02	normal	Yes	Morris Worm fingerd Stack Buffer Overflow
22	exploit/bsd/softcart/mecartec_softcart	2004-06-19	great	No	Mercantec SoftCart CGI Overflow
23	exploit/dialup/multi/login/manysys	2001-12-12	good	No	System V Derived /bin/login Extraneous Arguments Buffer Overflow
24	exploit/firefox/local/exec_shellcode	2014-03-10	excellent	No	Firefox Exec Shellcode from Privileged Javascript Shell
25	exploit/freebsd/ftp/proftpd_telnet_isc	2010-11-01	great	Yes	PROFTPD 1.3.4rc2 - 1.3.30 Telnet IAC Buffer Overflow (FreeBSD)
26	exploit/freebsd/http/citrix_dir_traversal_rce	2019-12-17	excellent	Yes	Citrix ADC (NetScaler) Directory Traversal RCE
27	exploit/freebsd/http/citrix_formssso_target_rce	2023-07-18	normal	Yes	Citrix ADC (NetScaler) Forms SSO Target RCE
28	exploit/freebsd/http/junos_phpnc_auto_prepend_file	2023-06-17	excellent	Yes	Junos OS PHPNC Environment variable Manipulation RCE
29	exploit/freebsd/http/watchguard_cmd_exec	2015-06-20	excellent	Yes	Watchguard XCS Remote Command Execution
30	exploit/freebsd/local/intel_sysret_priv_esc	2012-06-12	great	Yes	FreeBSD Intel SYSRET Privilege Escalation
31	exploit/freebsd/local/ipd_setptkopt_uaf_priv_esc	2020-07-07	great	Yes	FreeBSD ipd_setptkopt User-After-Free Privilege Escalation
32	exploit/freebsd/local/mmp	2013-06-18	great	Yes	FreeBSD 9 Address Space Manipulation Privilege Escalation
33	exploit/freebsd/local/rtdl_exec_priv_esc	2009-11-30	excellent	Yes	FreeBSD rtdl exec() Privilege Escalation
34	exploit/freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual	Yes	Watchguard XCS FixCorruptMail Local Privilege Escalation
35	exploit/freebsd/misc/citrix_netscaler_xssp_bof	2014-09-22	normal	Yes	Citrix NetScaler SOAP Handler Remote Code Execution
36	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (MSD x86)
37	exploit/freebsd/tacacs/tacacs_report	2008-01-08	average	No	XTACACS report() Buffer Overflow
38	exploit/freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	No	FreeBSD Telnet Service Encryption Key ID Buffer Overflow
39	exploit/freebsd/webapp/spannitan_unauth_rce	2020-04-17	normal	Yes	Spannitan Unauthenticated RCE
40	exploit/hpux/lpd/cleanup_exec	2002-08-28	excellent	No	HP-UX LPD Command Execution
41	exploit/ixis/lpd/tagprinter_exec	2001-09-01	excellent	Yes	Irix LPD tagprinter Command Execution
42	exploit/linux/antivirus/escan_password_exec	2014-04-04	excellent	Yes	eScan Web Management Console Command Injection
43	exploit/linux/browser/adobe_flashplayer_aslaunch	2008-12-17	good	No	Adobe Flash Player ActionScript Launch Command Execution Vulnerability
44	exploit/linux/fileformat/unrar_cve_2022_38333	2022-06-28	excellent	No	unRAR Path Traversal (CVE-2022-38333)

➤ An exploit executes a sequence of commands that target a specific vulnerability found in a system

- Use a Particular exploits :

```
msf6 > use exploit/windows/misc/bopup_comm
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/bopup_comm) >
```

- **Show Options in Exploits :**

```

Uber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /home/kali

msf6 exploit(windows/misc/bopup_comm) > show options

Module options (exploit/windows/misc/bopup_comm):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.0.10     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     4444             yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.140   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Bopup Communications Server 3.2.26.5460

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

msf6 exploit(windows/misc/bopup_comm) > set RHOSTS 192.168.74.128
RHOSTS => 192.168.74.128
msf6 exploit(windows/misc/bopup_comm) >
  
```

Usage :

Open

1. Terminal – msfconsole -q

2. msf6 – show exploits (It displays various options)

3. msf6 > use exploit/windows/misc/bopup_comm

msf6 exploit (windows/misc/bopup_comm) > show options [It displays various option in this exploit]

4. msf6 exploit (windows/misc/bopup_comm) > set RHOSTS = 192.168.74.128

RHOSTS is a remote host , we should type the victim's ip address