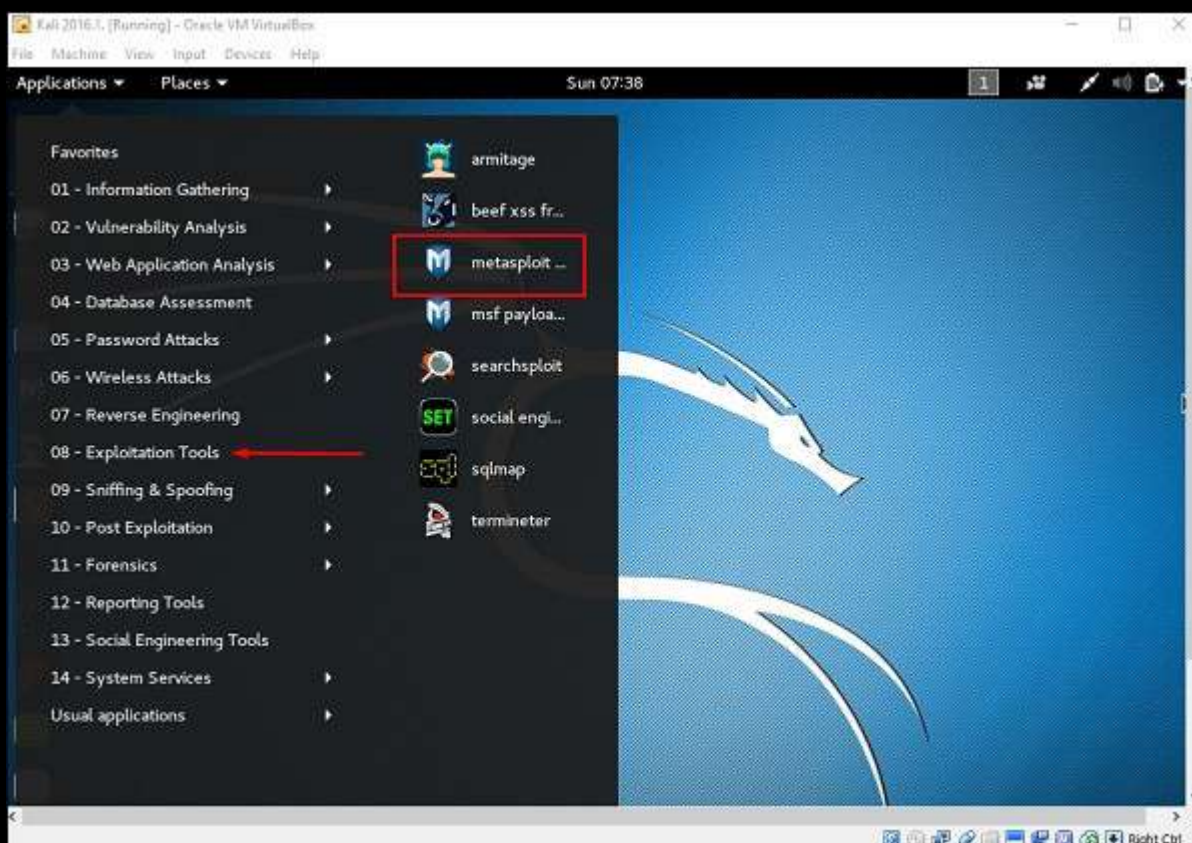


Exploitation Tools-Metasploit

As we mentioned before, Metasploit is a product of Rapid7 and most of the resources can be found on their web page www.metasploit.com. It is available in two versions - commercial and free edition. The differences between these two versions is not much hence, in this case we will be using the Community version (free).

As an Ethical Hacker, you will be using “Kali Distribution” which has the Metasploit community version embedded, along with other ethical hacking tools which are very comfortable by saving time of installation. However, if you want to install as a separate tool it is an application that can be installed in the operating systems like Linux, Windows and OS X.

First, open the Metasploit Console in Kali. Then, go to Applications → Exploitation Tools → Metasploit.



After it starts, you will see the following screen, where the version of Metasploit is underlined in red.

The screenshot shows a terminal window titled "Terminal". The main content is an ASCII art representation of a dragon's head, facing right. To the right of the dragon's head, there is a box containing the text "Metasploit!". Below the ASCII art, there is a promotional message: "Easy phishing: Set up email templates, landing pages and listeners in Metasploit Pro -- learn more on http://rapid7.com/metasploit". At the bottom, there is a list of statistics for Metasploit v4.11.8:

```
= [ metasploit v4.11.8- ]  
+ -- ==[ 1519 exploits - 880 auxiliary - 259 post ]  
+ -- ==[ 437 payloads - 38 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

The prompt "msf >" is visible at the bottom left.

In the console, if you use help or ? symbol, it will show you a list with the commands of MSP along with their description. You can choose based on your needs and what you will use.

```
+ -- --=[ 43/ payloads - 8 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > help

Core Commands
=====

Command      Description
-----
?            Help menu
advanced     Displays advanced options for one or more modules
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
edit         Edit the current module with $VISUAL or $EDITOR
exit         Exit the console
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
info         Displays information about one or more modules
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath     Searches for and loads modules from a path
makerc       Save commands entered since start to a file
options      Displays global options or for one or more modules
popm         Pops the latest module off the stack and makes it active
previous     Sets the previously loaded module as the current module
pushm        Pushes the active or list of modules onto the module stack
quit         Exit the console
```


Another important administration command is **msfupdate** which helps to update the metasploit with the latest vulnerability exploits. After running this command in the console, you will have to wait several minutes until the update is complete.

```
msf > msfupdate
[*] exec: msfupdate

[*]
[*] Attempting to update the Metasploit Framework...
[*]

[*] Checking for updates via the APT repository
[*] Note: expect weekly(ish) updates using this method
[*] Updating to version 4.12.15-0kali2
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
Suggested packages:
  clamav clamav-daemon
The following NEW packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 3 newly installed, 0 to remove and 1569 not upgraded.
Need to get 68.6 MB of archives.
After this operation, 56.7 MB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-did-you-mean all 1.0.0-2 [11.2 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-net-telnet all 0.1.1-2 [12.5 kB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 libruby2.3 amd64 2.3.1-5 [3,093 kB]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 metasploit-framework amd64 4.12.15-0kali2
[65.5 MB]
Reading changelogs...
```

It has a good command called “Search” which you can use to find what you want as shown in the following screenshot. For example, I want to find exploits related to Microsoft and the command can be **msf >search name:Microsoft type:exploit**.

Where “search” is the command, “name” is the name of the object that we are looking for, and “type” is what kind of script we are looking for.

```
msf > search name:microsoft type:exploit

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
auxiliary/admin/http/iis_auth_bypass	2010-07-02	normal	MS10-065 P
Microsoft IIS 5 NTFS Stream Authentication Bypass			
auxiliary/admin/kerberos/ms14_068_kerberos_checksum	2014-11-18	normal	MS14-068 P
Microsoft Kerberos Checksum Validation Vulnerability			
auxiliary/admin/ms/ms08_059_his2006	2008-10-14	normal	Microsoft
Host Integration Server 2006 Command Execution Vulnerability			
auxiliary/admin/mssql/mssql_enum		normal	Microsoft
SQL Server Configuration Enumerator			
auxiliary/admin/mssql/mssql_enum_domain_accounts		normal	Microsoft
SQL Server SUSER_SNAME Windows Domain Account Enumeration			
auxiliary/admin/mssql/mssql_enum_domain_accounts_sql		normal	Microsoft
SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration			
auxiliary/admin/mssql/mssql_enum_sql_logins		normal	Microsoft
SQL Server SUSER_SNAME SQL Logins Enumeration			
auxiliary/admin/mssql/mssql_escalate_dbowner		normal	Microsoft
SQL Server Escalate Db Owner			
auxiliary/admin/mssql/mssql_escalate_dbowner_sql		normal	Microsoft
SQL Server SQLi Escalate Db Owner			
auxiliary/admin/mssql/mssql_escalate_execute_as		normal	Microsoft
SQL Server Escalate EXECUTE AS			
auxiliary/admin/mssql/mssql_escalate_execute_as_sql		normal	Microsoft

Another command is “info”. It provides the information regarding a module or platform where it is used, who is the author, vulnerability reference, and the payload restriction that this can have.

```
f auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass
```

Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
Module: auxiliary/admin/http/iis_auth_bypass
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2010-07-02

Provided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

Basic options:

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOST		yes	The target address
RPORT	80	yes	The target port
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The URI directory where basic auth is enabled
VHOST		no	HTTP server virtual host

Description:

This module bypasses basic authentication for Internet Information Services (IIS). By appending the NTFS stream name to the directory name in a request, it is possible to bypass authentication.

References:

<http://cvedetails.com/cve/2010-2731/>
<http://www.osvdb.org/66160>
<http://technet.microsoft.com/en-us/security/bulletin/MS10-065>
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation