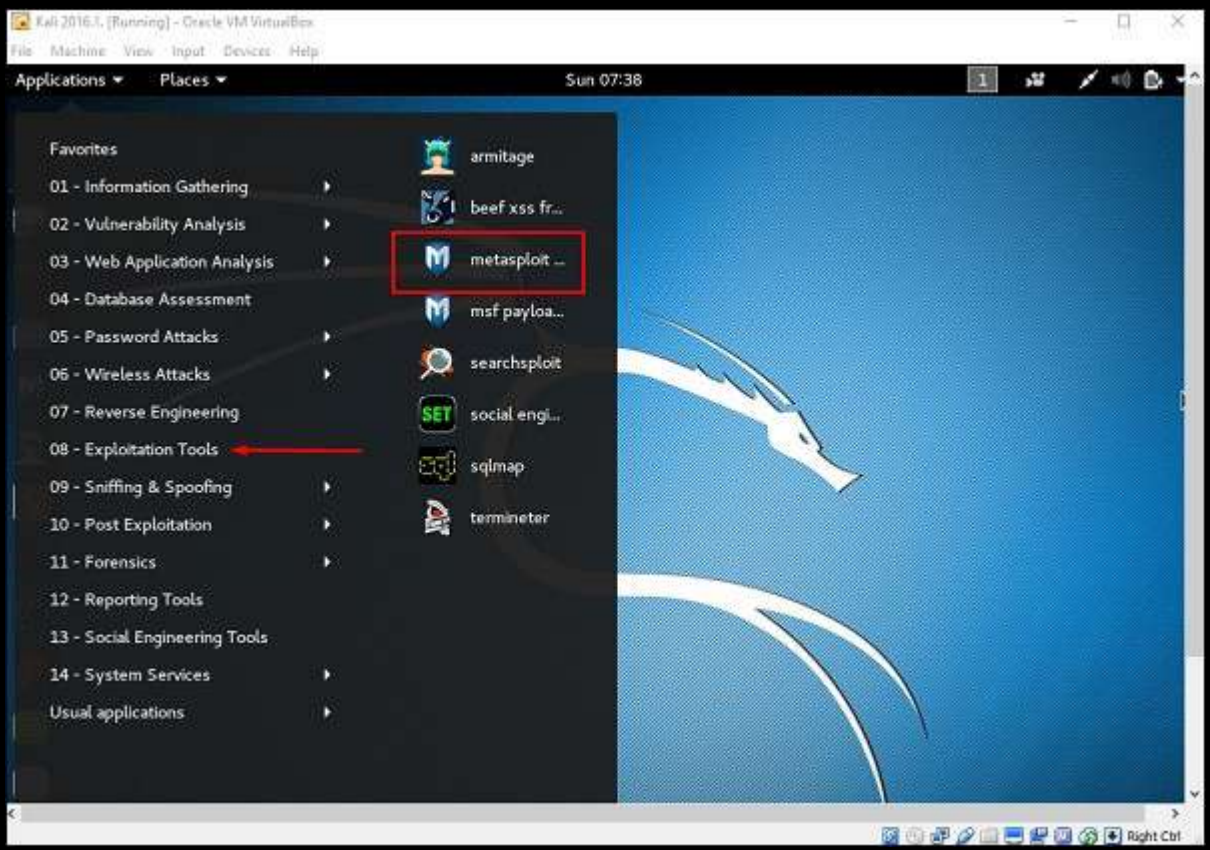
*Exploitation Tools-*Metasploit

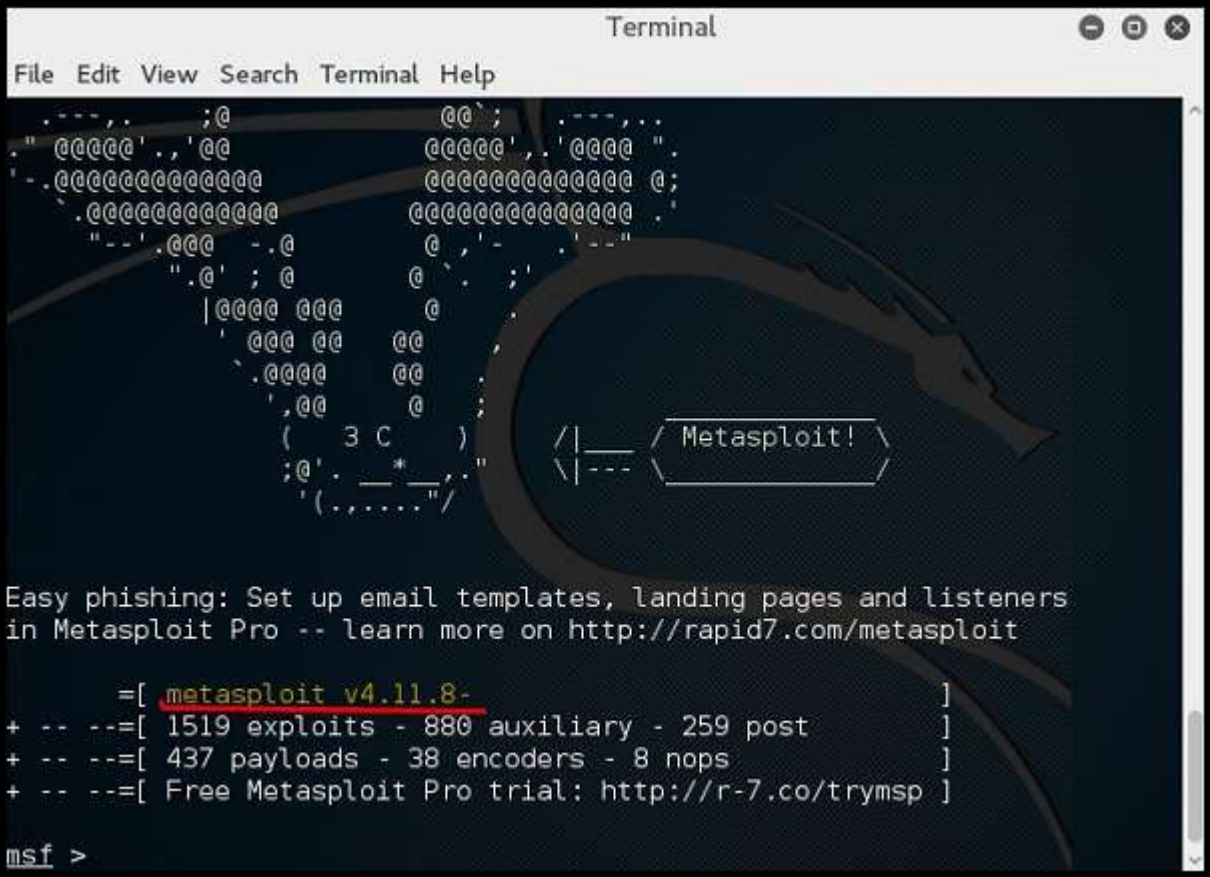
As we mentioned before, Metasploit is a product of Rapid7 and most of the resources can be found on their web page www.metasploit.com. It is available in two versions - commercial and free edition. The differences between these two versions is not much hence, in this case we will be using the Community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

As an Ethical Hacker, you will be using "Kali Ditribution" 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.

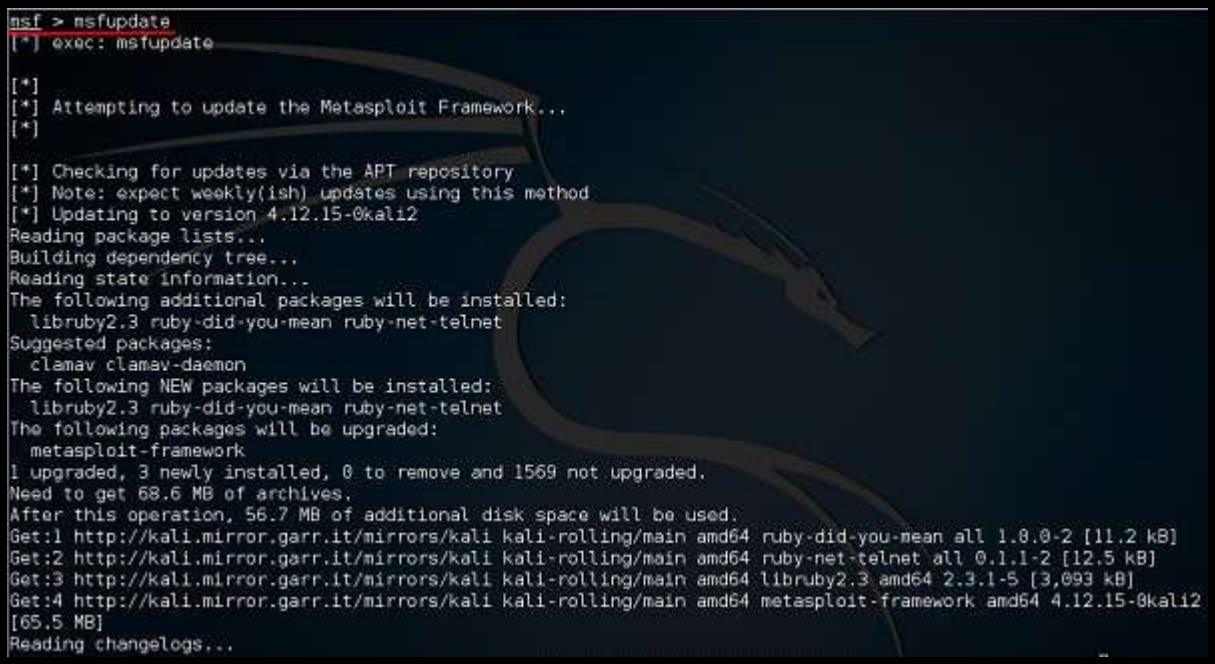


After it starts, you will see the following screen, where the version of Metasploit is underlined in red.



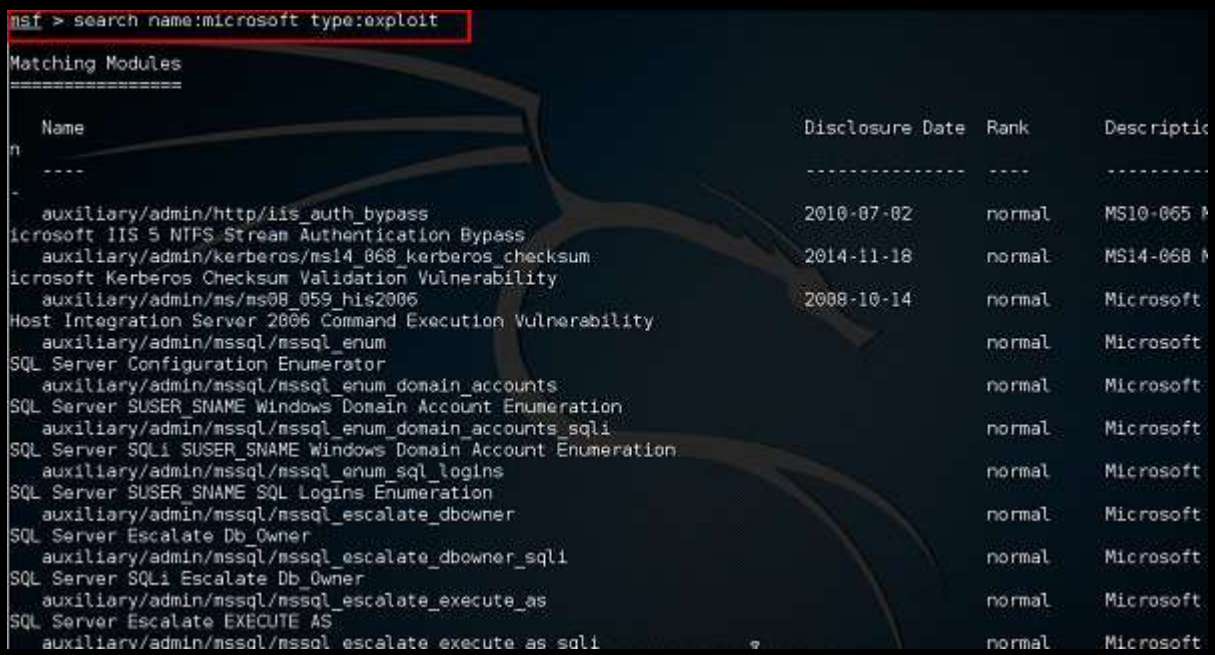
In the console, if you use help or ? symbol, it will show you a list with the commands of MSP along with their description. You can choose based on your needs and what you will use.

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.



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.



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

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

sic 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

scription:
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.

ferences:
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
```