**Metasploit framework**

**What is Metasploit?**

Metasploit is an opensource platform for developing and initializing exploit code. The Metasploit framework is used for research on new exploits. It is a safe way of finding current exploits or creating your own exploits in the Framework.

**Why did I choose Metasploit?**

The Metasploit framework was free and pre-installed on my Kali Linux virtual machine. I enjoyed the simplicity of the system and how everything was plainly laid out. The commands were easy to learn and there was a lot of support available online. Metasploit also had a lot of assistance on their website and there is a lot of media made for Metasploit. Due to this I found it was a lot easier to learn and understand the fundamentals of Metasploit in order for me to create this tutorial.



[This Photo](https://en.wikipedia.org/wiki/Metasploit_Project) by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)



[This Photo](https://sathisharthars.com/2014/08/02/proxying-burpsuite-through-tor-for-anonymity/) by Unknown Author is licensed under [CC BY](https://creativecommons.org/licenses/by/3.0/)

**Why not use Burp Suite?**

Metasploit is a very capable exploit software and the feature that attracted me to the system the most was its ease of use and the available assistance online; I did also appreciate the automation of exploits on Metasploit. I looked into Burp Suite and found the following Pro’s between the systems.

**Pro’s**

* Burp Suite
* Very quick to run web attacks
* Very thorough attacks
* When attacking a website, its spiders the webpage and finds most pages associated with that webpage quickly.
* It allows you to be selective of which web pages you attack, you do not need to attack all that were found in the scan.
* Metasploit
  + Scans networks for new or existing vulnerabilities in systems.
  + Automation of manual tests and exploits.
  + Reduced days’ work into a few hours.
  + Metasploit is an integral part in testing new systems and validating them.

**How did I start?**

I started by opening my virtual machine with Kali Linux on it and went into the search bar and typed Metasploit, this will start the Metasploit infrastructure to run.

**What can Metasploit do?**

Metasploit’s main function is to run exploits and allow the user to create their own exploits using their framework, Metasploit can do many things when used correctly and has the potential to be a very effective security tool. The first thing I would do when using Metasploit is run the command “help”, this will give you a detailed list of many of the things you could use Metasploit for, and what commands would help you achieve what you want. I found that I used the “help“ command on many occasions just to reassure that the command I was about to enter was going to assist me going ahead and not do something I didn’t desire. During my time of using Metasploit I found that the most frequent commands would be “show all“ which will show you all the available modules in the Metasploit framework.

**The frequent commands**

* + “show auxiliary” this command will show the user the auxiliary modules available within Metasploit.
  + Text

    Description automatically generated“show exploits” this command will give the user a list of all exploits within Metasploit.
  + “show payloads” when this command is run it will show you all the available payloads for the exploit that you have chosen to run.
  + “show options” this command needs to be linked to an exploit and will give you all the settings available or required for the chosen exploit.
  + “show targets” this will show you all the available targets associated with your chosen exploit.
  + “show advance” will allow you to further fine tune your exploit by giving you more advanced options and settings.
  + “show encoders” will give you the list of encoders found within the Metasploit framework.
  + ” show nops” this will display the NOP generators stored in the Metasploit framework.
  + “help” command will give you as the user, a lot of assistance as it is very detailed and give a lot of depth into what's going on.
  + “info” will provide more details about the module being used and its suggested to always read this so that you don’t use a module that could do stuff you didn’t expect.
  + “jobs” will inform you of all the modules being run in the background.
  + “kill” will shut down any job as long as you supply the job ID.
  + There are many more commands at your disposal!

**Text

Description automatically generated**

**Auxiliaries**

The auxiliary modules found in the Metasploit framework are able to perform functions like sniffing, scanning and a lot more. These modules are incredibly valuable when it comes to penetration testing a system.

A very common discovery auxiliary module is ARP\_SWEEP, this module is very efficient in discovering more information about the victim system. When the Victim machine and your attacking machine are in the same network this auxiliary module will request your MAC address and IP address and then the scanner will inform you about your victims’ system.

Graphical user interface, text

Description automatically generated

**Exploits**

Text

Description automatically generatedAn exploit is set to release a set of commands that aim to target the vulnerability identified in the victim system. This exploit will provide the attacker with access into the system or desired application. Many exploits contain buffer overflows and code injection. The image below shows me running an exploit that manages the VDMK mount drive in a windows environment.

**Payloads**

The Metasploit framework has three main types of payloads. They are stagers, stages and singles. Due to these different types of payloads, Metasploit is versatile and useful in countless situations. The exploit found in the picture above is an example of a stager and a stage payload.

**MSFENCODE**

This is a great tool that the Metasploit framework will give you access to. This tool creates an environment in which you can encode the exploit you have created to allow you to successfully attack the target and encode the payload to suit the target and work correctly. This tool has been upgraded and is now found in MSFVENOM

**MsfVenom**

This is a command line that utilizes the capabilities of both Msfpayload and Msfencode, msfVenom took over in 2015, this change was made so that only one tool would be needed and that it would increase the overall speed of someone using the Metasploit framework, this also created a new standardized line for the command option.

**Warning!**

Please be careful with how you use this software and remember to hack ethically and be safe. As much as this tool gives you access to certain areas you as the user need to be responsible and not abuse the power, the Metasploit framework is not a toy and misusing it could lead to serious repercussions.

**Common Problem**

A problem I ran into and I think that most people using virtual machines will run into this issue, a lot of the commands require administrative access, I could also tell this because of the $ sign present in my terminal, the administer sign is #.In order to change my access level I used the command “sudu su” this then prompted me to input my password, after that I put the command “Passwd root” which allowed me to create a new password for an admin user. Text

Description automatically generated

Works cited

* https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/
* https://www.offensive-security.com/metasploit-unleashed/msfconsole/
* https://www.offensive-security.com/metasploit-unleashed/metasploit-fundamentals/
* https://youtu.be/aRwxsn9ZEQw
* http://robwillis.info/2016/08/metasploit-framework-basics-on-kali-linux-owning-a-windows-server/
* https://www.offensive-security.com/metasploit-unleashed/scanner-discovery-auxiliary-modules/
* https://www.offensive-security.com/metasploit-unleashed/payloads/#:~:text=A%20payload%20in%20Metasploit%20refers,Singles%2C%20Stagers%2C%20and%20Stages.&text=For%20example%2C%20windows%2Fshell\_bind\_tcp%20is,and%20a%20stage%20(shell).
* https://www.offensive-security.com/metasploit-unleashed/msfencode/
* https://www.offensive-security.com/metasploit-unleashed/msfvenom/