ESOF 422 HW 5: Metasploit (WIP)

Assigned Friday April 4th.

Due Wednesday April 16th

On this assignment, you will get hands on experience with Metasploit, one of the most popular frameworks for ethical hacking and exploiting vulnerabilities. You will answer several questions as you are gathering information, looking at vulnerabilities, and exploiting the system. As you are working through the assignment, please be typing your answers in a word document that you will eventually submit to Brightspace. You are allowed to work with one partner on this assignment.

Part I: Getting Started and setting up your machines

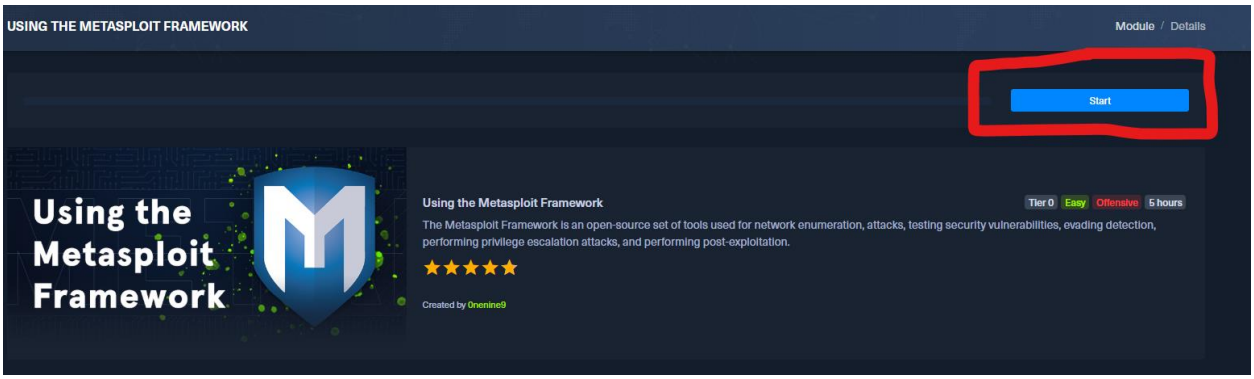
We need to have access to a machine that has the Metasploit framework installed, and access to a separate, vulnerable machine. Instead of setting up this environment ourselves, we will leverage a cybersecurity learning platform called **HackTheBox.** HackTheBox is an online platform that will summon a unique, vulnerable machine for you to attack, and provides you with all the hacking tools that you will need. The machines it creates for you are only active for two hours before they reset, so make sure you have adequate time to start this assignment.

HackTheBox is completely free, but you will need to register for an account. With normal account, there are some restrictions that may give you a headache if you are not being careful. For example, you are only able to create one machine to attack per day. Therefore, you should not wait until the very last night to start this assignment. You can pay for a premium account to get around these restrictions, which is $8 per month for students.

When your account is created, please navigate to the following link:

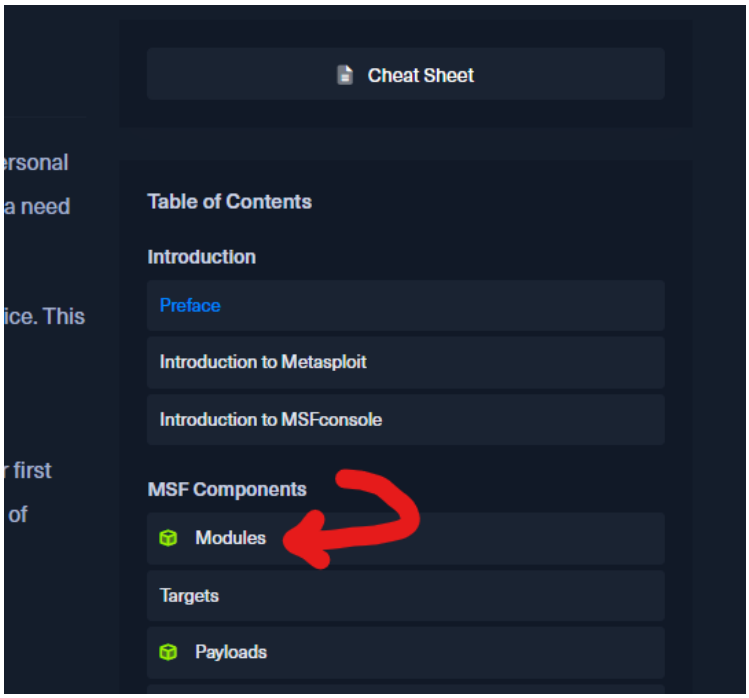
https://academy.hackthebox.com/

At the top, there should be a search bar. Search for "Metasploit". There should be a learning module that appears called "*Using the Metasploit Framework*". Select this option, and then press the **start** button on the top right:

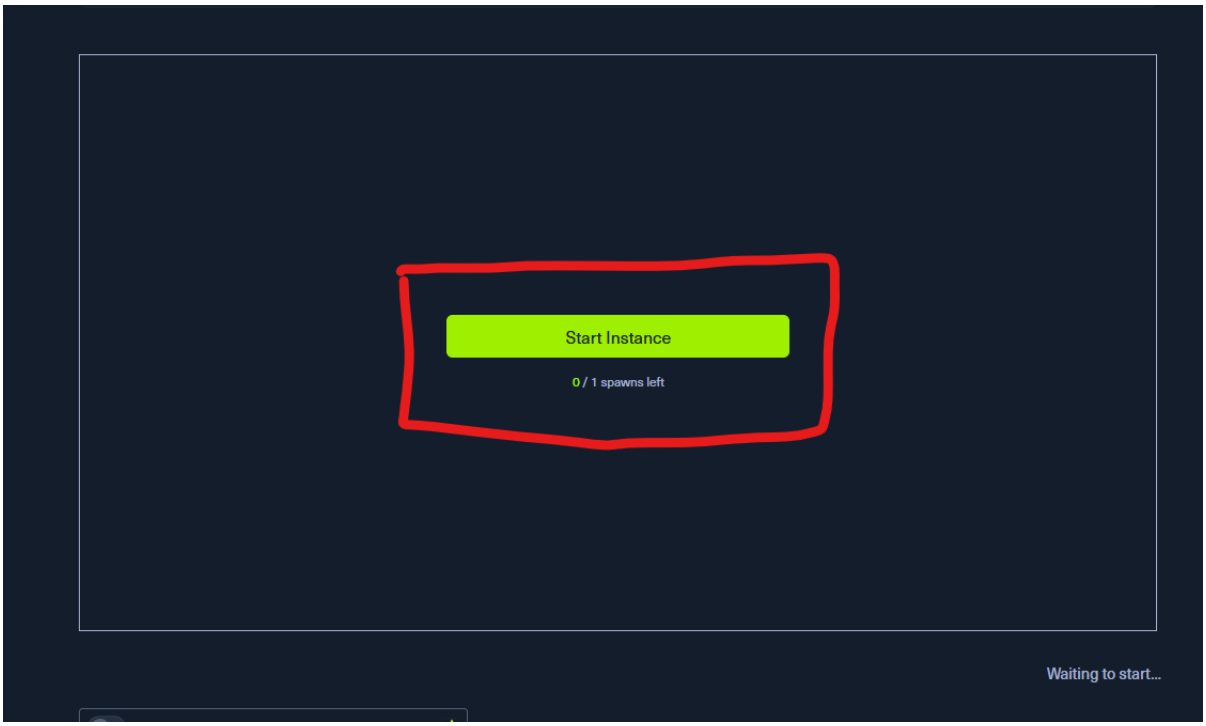


HackTheBox has a lot of information here, but we are really only concerned about using their infrastructure. The questions that I will be asking you are not the same questions that HackTheBox will ask you.

On the table of contents, let's skip ahead to the "**Modules**" section.



Scroll to the bottom of the page. This is where we are going to create the machines to use for this assignment. We will create the attacker's instance, which will have all the Metasploit tools installed.

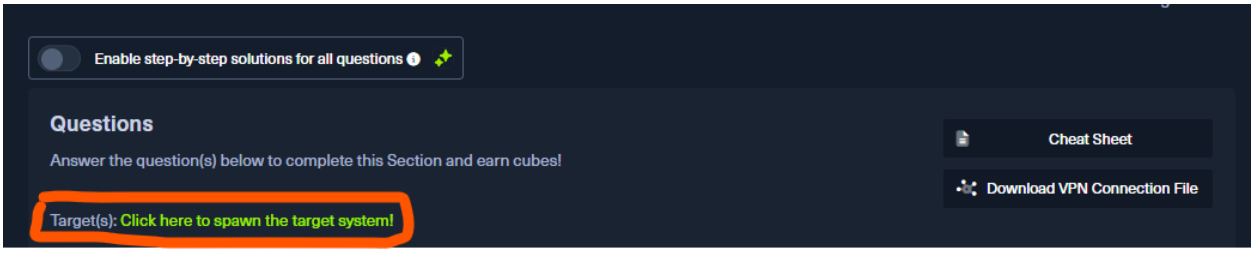


This may take several seconds to boot up. This will be a Parrot Linux VM, which is very similar to Kali Linux. This machine will only stay running for two hours. After two hours, the machine will terminate, and you will likely need to wait until the next day to restart it.

In the top right corner of this machine, it should display the IP address of the attacker's machine.

1. What is the IP address of your attacker machine?

Next, let's create the victim machine that we will be targeting. The button for creating the victim machine can be found right under the window for the attacker's machine.



It may take several seconds to boot up. Once it's created, it should display the IP address for the victim machine.

2. What is the IP address of the victim machine?

Congratulations! Your environment is set up, and you are ready to hack some things!

Part 2: Reconnaissance

To exploit a machine, we need to find a vulnerability of some kind. A great way to scan for potentially vulnerable services or ports on a target machine is with **`nmap`**.

The **`-A`** flag will try to identify services that are running on an open port, and the versions of those services.

3. Use **`nmap`** with the **`-A`** flag to see which ports are open on the victim machine. This may take 30-60 seconds to complete. Please take a screenshot of the output of your **`nmap`** command

4. There should be four ports that are open. What are the four ports?

5. Look at port 445 of your **`nmap`** output. The service on the port is a commonly-used network file sharing communication protocol. What is the communication protocol that this service is associated with? You may need to use Google here.

Part 3: Vulnerability Analysis

`nmap` should have told you the specific version of the service. Do a little bit of Googling and see if there is a known vulnerability for this specific version. Microsoft has a naming scheme for Microsoft-based vulnerabilities that they disclose in yearly security bulletins. This naming scheme is called a *Bulletin Number*. Bulletin numbers typically have the following format: **`MS__-___`** . From Google, you should be able to find a critical vulnerability, and one of the top results should be a "Learn Microsoft" security bulletin web page. Answer the following questions:

6. What is the Security Bulletin number for this vulnerability?

7. When was this vulnerability published?

8. What CVEs is the vulnerability linked to?

9. What does the vulnerability allow an attacker to do?

10. Nmap should have told you the operating system of the victim machine. Is the victim machine's OS vulnerable to this CVE?

Part 4: Exploitation and Metasploit

11. Google the bulletin number, and you should find the name of the **exploit** for this vulnerability. It might go by a few different names, but the first part is always the same for each name. What is the name of the exploit for this vulnerability?

12. This exploit achieves a **Write-What-Where** condition. What is the CWE for the Write-What-Where condition?

13. What is a Write-What-Where condition?

On the attacker's box, let's boot up the Metasploit console with **`msfconsole`**. You can search the exploit catalog for specific keywords. Search for the bulletin number with the **`search`** command, and you should find an exploit module that ends with **`psexec`.** Select the correct module with the **`use`** keyword, and you should now have the exploit loaded. Run the command **`show options`** to see more information about the exploit and payload.

14. What is the Metasploit payload that will be sent by the exploit? (this will be the default configuration).

15. What is the purpose of this payload? (ie. what is so great about it?)

16. Run the **`info`** command while the exploit is still loaded. In this exploit, we also achieve an **escalation of privilege**. How is that achieved with this exploit? Your answer for question 11 will be helpful here.

We are now ready to run our exploit. Metasploit will need the remote IP address of the victim machine (`RHOSTS`) and the local IP address of the Attacker's machine (`LHOST`). You can set these values with the **`setg`** or **`set`** commands. Make sure to use the IP addresses that you determined at the beginning of this lab.

When those values are set. Use the **`exploit`** command or **`run`** command to run the exploit and send the payload to the victim machine.

Part 5: Post Exploitation

Your attack should be successful! You should now be in a **`meterpreter`** shell, which is essentially our Admin-level reverse shell on the victim's Windows machine. We can now run any Metasploit post-exploitation command (see the **`help`** command for more info)

17. Take a screenshot that clearly shows an active **`meterpreter`** shell.

18. Run the **`getuid`** command. What is the username of the server?

19. Navigate to the **`Desktop`** folder of the Administrator account. Make an empty file on the desktop called **`yougothacked.txt`**. Take a screenshot that shows the file was successfully created and is in the Desktop folder. You may need to look at Metasploit documentation or **`help`** for how to do this task.

20. On the desktop, there should be an existing file called **`flag.txt`**. Suppose this was some secret company secret that we wanted to steal. What is the secret string that is in the file?

Congratulations! You have successfully exploited vulnerability using Metasploit and are an elite h4ck3r.

Submission

Please type up your answers in the word document and include screenshot for the questions that requested them. Please clearly label each question so that we understand your answers. If you worked with a partner, include your names at the top of your report. Both partners will submit to Brightspace. Save your word document as a PDF, and submit to the HW5 Brightspace submission box.