Name: Ritesh Lakhani

Enrollment No: 22010101099

Metasploit Room

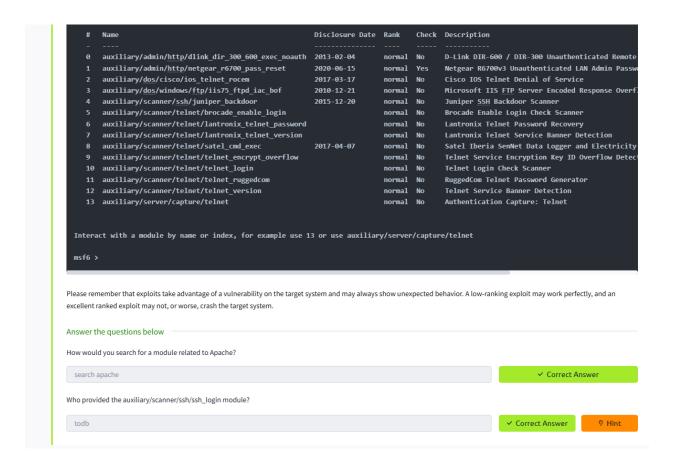
Task 1 Introduction to Metasploit

Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation. . Metasploit Pro: The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI). • Metasploit Framework: The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used The Metasploit Framework is a set of tools that allow information gathering, scanning, exploitation, exploit development, post-exploitation, and more. While the primary usage of the Metasploit Framework focuses on the penetration testing domain, it is also useful for vulnerability research and exploit development. The main components of the Metasploit Framework can be summarized as follows; · msfconsole: The main command-line interface. • Modules: supporting modules such as exploits, scanners, payloads, etc. • Tools: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern, create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this This room will cover the main components of Metasploit while providing you with a solid foundation on how to find relevant exploits, set parameters, and exploit vulnerable services on the target system. Once you have completed this room, you will be able to navigate and use the Metasploit command line comfortably. Press the Start Machine button below. Start the AttackBox by pressing the Start AttackBox button at the top of this page to complete tasks and answer the questions. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue Show Split View button at the top of the page Answer the questions below No answer needed ✓ Correct Answer No answer needed

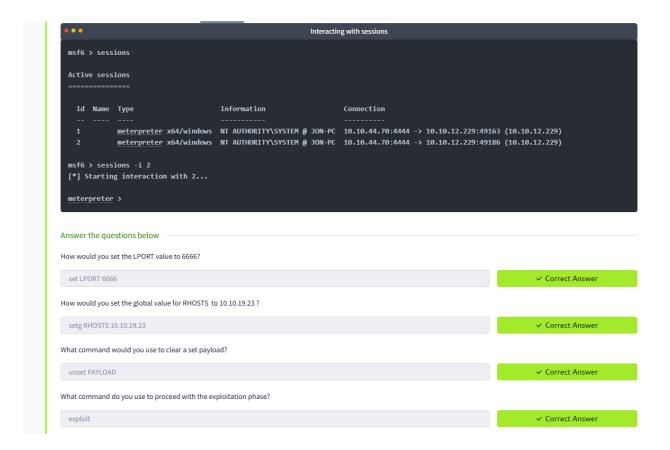
Task 2 Main Components of Metasploit

If you wish to familiarize yourself further with these modules, you can find them under the modules folder of your <u>Metasploit</u> installation. For the AttackBox these are under /opt/ <u>metasploit</u> -framework/embedded/framework/modules	
Answer the questions below	
What is the name of the code taking advantage of a flaw on the target system?	
Exploit	✓ Correct Answer
What is the name of the code that runs on the target system to achieve the attacker's goal?	
Payload	✓ Correct Answer
What are self-contained payloads called?	
Singles	✓ Correct Answer
Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?	
Singles	✓ Correct Answer

Task 3 MfsConsole



Task 4 Working With Modules



Task 5 Summary

