Full Name : Saurav Gajanan Patil

Gmail ID : sauravpatil0506@gmail.com

College / Organization Name : MVP's KBTCOE ,Nashik

Metasploit intro:-

1.Introduction

This module provided a comprehensive deep dive into the **Metasploit Framework (MSF)**, the world's most used penetration testing framework. Throughout the lab, I progressed from understanding the architecture of the framework to actively configuring exploits and managing payloads in a simulated attack environment.

2.Main Components of Metasploit :

The first phase of the lab involved defining the "language" of Metasploit. I learned to distinguish between the various parts of the framework:

- **msfconsole:** The primary, centralized command-line interface.
- **Exploit:** The specific code used to take advantage of a vulnerability.
- **Payload:** The code that runs *after* a successful exploit to achieve the attacker's objective (e.g., a shell).
    - **Singles:** Self-contained payloads (e.g., windows/x64/pingback_reverse_tcp).
    - **Staged:** Payloads that are sent in two parts to save space.
- **Encoders:** Used to obfuscate payloads to bypass Signature-based Antivirus (AV) detection.

3.msfconsole:

I successfully demonstrated the standard operational workflow required for a penetration test:

A. Information Gathering & Searching

I learned that the search command is the gateway to the framework's database.

- **Command: search apache**
- **Observation: This returns a ranked list of modules (Excellent, Great, Good).**
- **Command: info [module_name]**
- **Learning: The info command reveals the author (e.g., todb for the SSH login scanner) and the specific CVEs the module addresses.**

B. Module Contexts & Prompts

A critical skill I developed was identifying my "location" within the framework by looking at the terminal prompt:

1. **msf6 >: The general console (no module selected).**
2. **msf6 exploit(...) >: The Context Prompt, where specific parameters are set.**
3. **meterpreter >: An advanced, post-exploitation shell running in the target's memory.**
4. **C:\Windows\System32>: A standard OS shell on the target system.**

C. Parameter Configuration

I mastered the configuration of the environment using the show options menu.

- **RHOSTS: The "Remote Host" or target IP/range.**
- **LHOST: The "Local Host" (my AttackBox IP) for receiving reverse connections.**
- **Set vs. Setg: I learned that set only applies to the current module, while setg (Set Global) carries the value across all modules, significantly speeding up the workflow.**

5. **Question/Answers**

Question	Answer	Reason
What is the name of the code taking advantage of a flaw on the target system?	Exploit	It is the delivery vehicle for the attack.

Question	Answer	Reason
What is the name of the code that runs on the target system to achieve the attacker's goal?	Payload	This is the "payload" or "cargo" delivered.
What are self-contained payloads called?	Singles	They do not require a second stage to function.
Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?	singles	Found in the above info
How would you search for a module related to Apache?	Search apache	By using search command we can find modules
Who provided the auxiliary/scanner/ssh/ssh_login module?	todb	By running command auxiliary/scanner/ssh/ssh_login in the terminal of Attackbox.
How would you set the LPORT value to 6666?	set LPORT 6666	We use set command to set the local port
How would you set the global value for RHOSTS to 10.10.19.23 ?	setg RHOSTS 10.10.19.23	We use setg command to set global value .

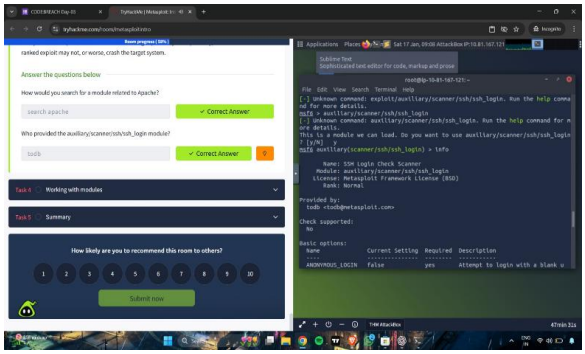
Question	Answer	Reason
What command would you use to clear a set payload?	unset PAYLOAD	We use unset command to clear set values
What command do you use to proceed with the exploitation phase?	exploit	Exploit command is use to proceed exploitation phase

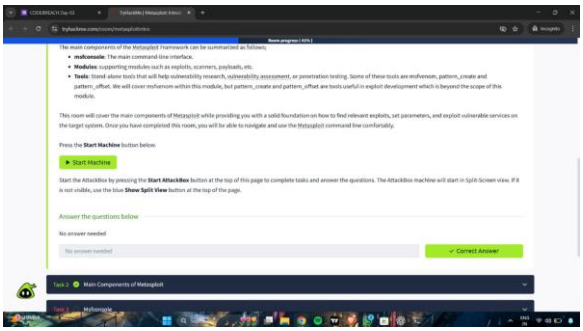
5. Technical Skill:

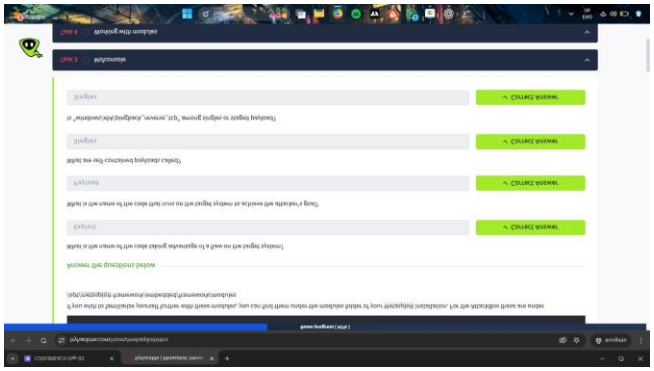
- **Tab Completion:** Utilizing the Tab key to auto-fill long module paths.
- **Persistence:** Using back to exit a module context without closing the console.
- **Cleanup:** Using unset all to clear parameters when switching targets.
- **Filesystem Navigation:** Identifying that modules are stored at /opt/metasploit-framework/embedded/framework/modules on the AttackBox.

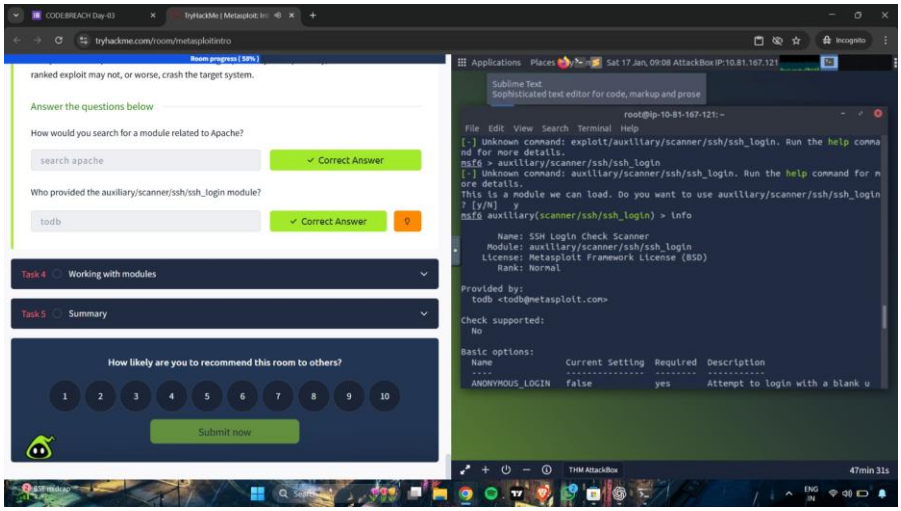
6. conclusion:

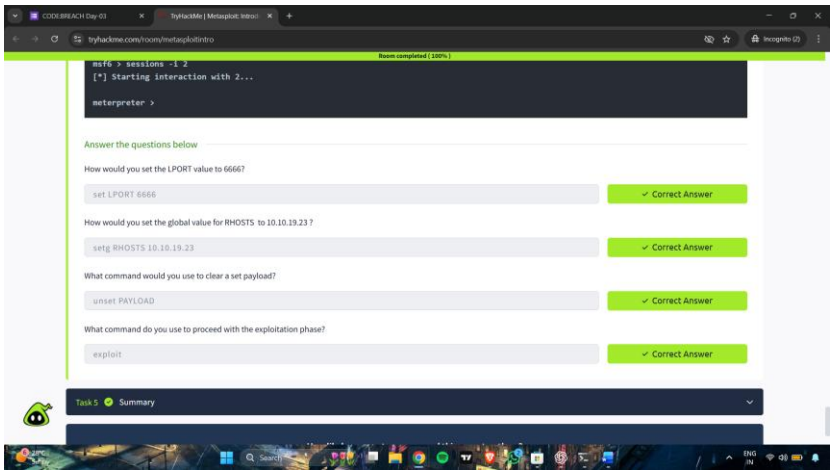
Below are the screenshots as a proof that I solved the above lab by my own and find the answers.

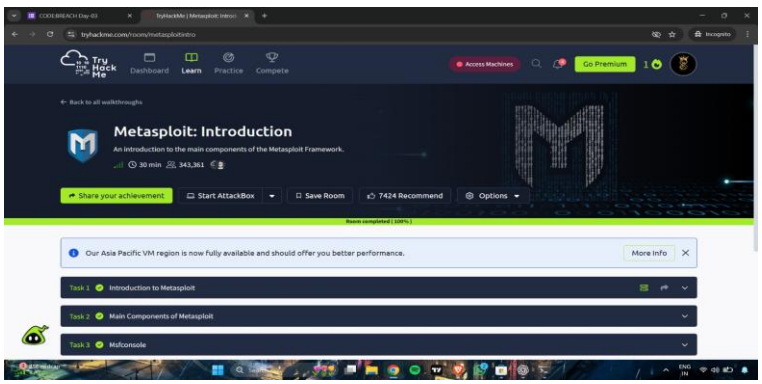







tryhackme.com/room/metasploitintro
Room progress (50%)
ranked exploit may not, or worse, crash the target system.
Answer the questions below
How would you search for a module related to Apache?
search apache
Correct Answer
Who provided the auxiliary/scanner/ssh/ssh_login module?
todb
Correct Answer
Task 4 Working with modules
Task 5 Summary
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
Sublime Text
Sophisticated text editor for code, markup and prose
root@ip-10-81-167-121: ~
File Edit View Search Terminal Help
[-] Unknown command: exploit/auxiliary/scanner/ssh/ssh_login. Run the help comma
nd for more details.
msf6 > auxiliary/scanner/ssh/ssh_login
[-] Unknown command: auxiliary/scanner/ssh/ssh_login. Run the help command for m
ore details.
This is a module we can load. Do you want to use auxiliary/scanner/ssh/ssh_login
? [y/N] y
msf6 auxiliary(scanner/ssh/ssh_login) > info
Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal
Provided by:
todb <todb@metasploit.com>
Check supported:
No
Basic options:
Name Current Setting Required Description
ANONYMOUS_LOGIN false yes Attempt to login with a blank u
THM AttackBox
47min 31s


tryhackme.com/room/metasploitintro
Room completed (100%)
msf6 > sessions -i 2
[*] Starting interaction with 2...
meterpreter >
Answer the questions below
How would you set the LPORT value to 6666?
set LPORT 6666
Correct Answer
How would you set the global value for RHOSTS to 10.10.19.23?
setg RHOSTS 10.10.19.23
Correct Answer
What command would you use to clear a set payload?
unset PAYLOAD
Correct Answer
What command do you use to proceed with the exploitation phase?
exploit
Correct Answer
Task 5 Summary


Try Hack Me
Dashboard
Learn
Practice
Compete
Access Machines
Go Premium
Metasploit: Introduction
An introduction to the main components of the Metasploit Framework.
30 min 343,361
Share your achievement
Start AttackBox
Save Room
7424 Recommend
Options
Our Asia Pacific VM region is now fully available and should offer you better performance.
More Info
Task 1 Introduction to Metasploit
Task 2 Main Components of Metasploit
Task 3 Msfconsole