EXPT NO: 16 ROLL NO: 220701245

METASPLOIT-INTRODUCTION

AIM:

To understand the basics of the Metasploit Framework and learn how to use it for identifying, exploiting, and gaining access to vulnerable systems.

PROCEDURE:

1. Start the TryHackMe machine and connect to the VPN.
2. Launch Metasploit Framework using the msfconsole command in the terminal.
3. Use search to find an exploit module for the target service (e.g., search vsftpd).
4. Select an appropriate module using use [module_path].
5. View and configure required parameters using show options and set them using set RHOSTS [target IP], set LHOST [your IP], etc.
6. Execute the exploit using the run or exploit command.
7. Upon successful exploitation, interact with the session using sessions and explore post-exploitation options.

TASK-1 INTRODUCTION TO METASPLOIT

Metasploit is the most widely used exploitation framework for penetration testing and vulnerability research. It supports all phases of a pentest — from information gathering to post-exploitation.

Versions:

- Metasploit Pro: Commercial version with a graphical interface.
- Metasploit Framework: Free, open-source, command-line version (focus of this room).

Main Components:

- msfconsole: The primary command-line interface.

- Modules: Includes exploits, payloads, scanners, etc.
- Tools: Standalone utilities like msfvenom, pattern_create, and pattern_offset.

Learning Objectives:

- Learn how to search, configure, and run exploits.
- Gain a solid foundation for using Metasploit effectively.
- Comfortably navigate and use the Metasploit command-line environment.

TASK-2 MAJOR COMPONENTS OF METASPLOIT

1. **Start Console**

bash

CopyEdit

msfconsole

2. **Search Module**

bash

CopyEdit

search <keyword>

3. **Use Module**

bash

CopyEdit

use <module_path>

4. **Show Options**

bash

CopyEdit

show options

5. **Set Values**

bash

CopyEdit

set RHOSTS <target_ip>

set RPORT <port> # if needed

set PAYLOAD <payload> # if needed

6. **Run Exploit**

bash

CopyEdit

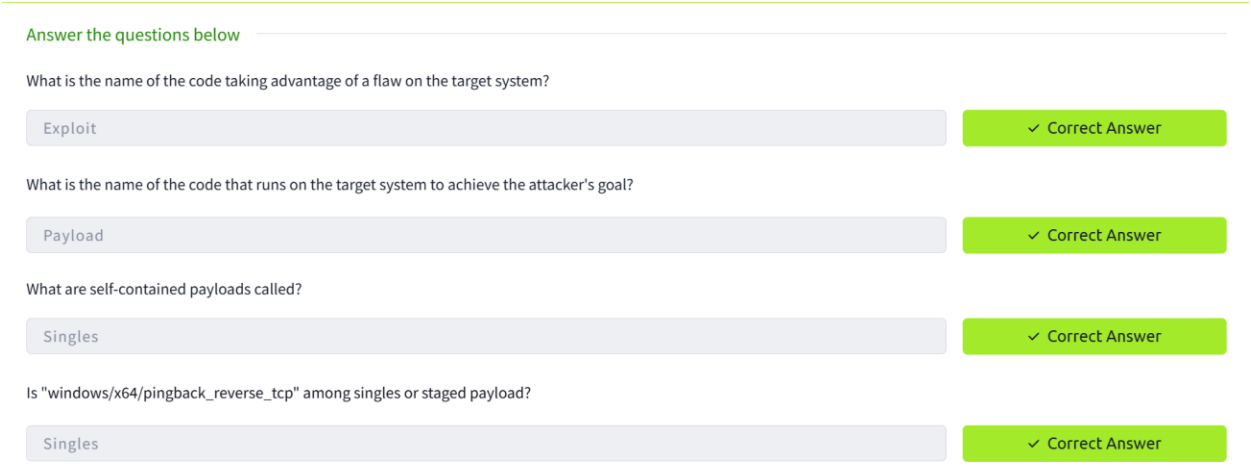
run

7. **Exit Console**

bash

CopyEdit

Exit



TASK-3 MSFCONSOLE

1. Search for a Module (e.g., Apache)

Command:

bash

CopyEdit

search apache

2. Find Module Info (e.g., ssh_login)

Command:

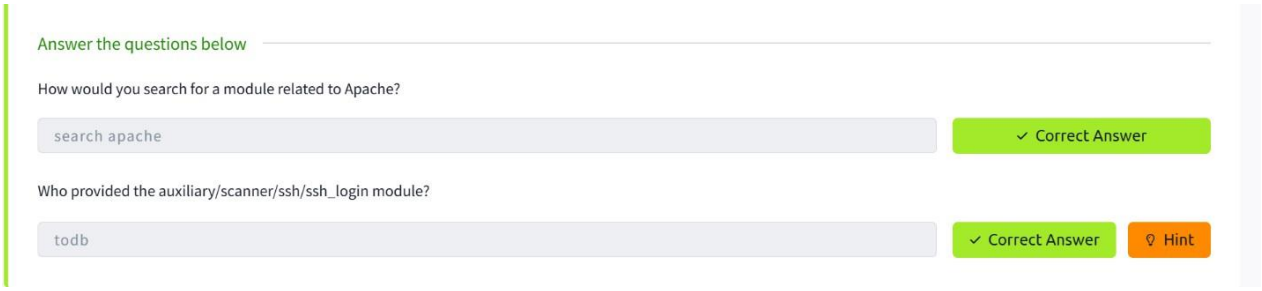
bash

CopyEdit

info auxiliary/scanner/ssh/ssh_login

Look for:

- Name
- Description
- Author → This answers “Who provided the module?”



TASK-4 WORKING WITH MODULES

1. Select Module
Use the use command to choose the module:

bash

CopyEdit

use exploit/windows/smb/ms17_010_eternalblue

2. Set Parameters
Set parameters with set:

bash

CopyEdit

set RHOSTS 10.10.165.39

3. Check Options
View available parameters with show options:

bash

CopyEdit

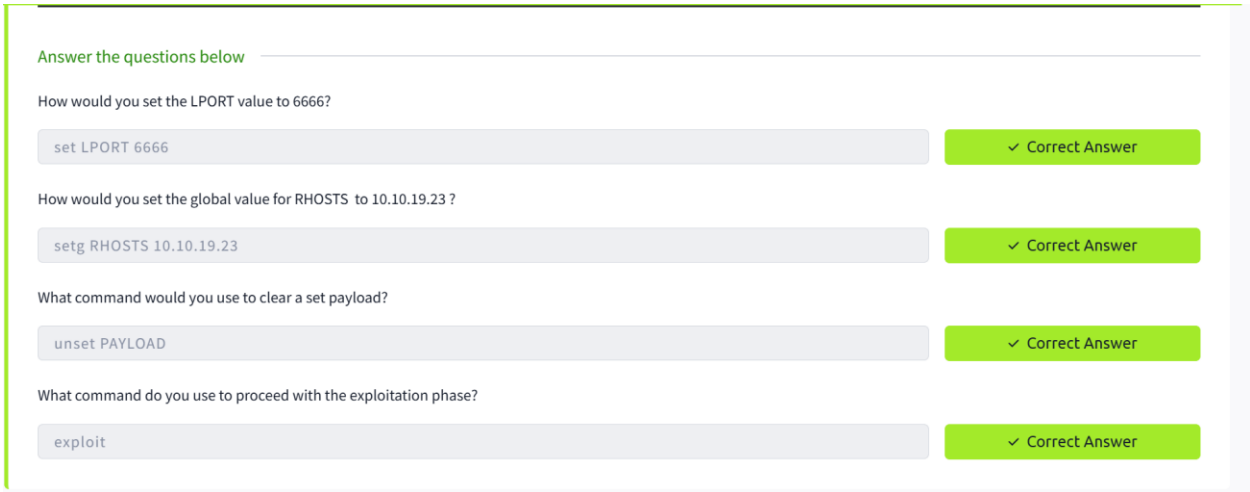
show options

4. Global Parameters
Use setg to apply settings globally across modules:

bash

CopyEdit

setg RHOSTS 10.10.165.39



TASK-5 SUMMARY

1. Finding the Exploit:
Identify a vulnerable service or application on the target system. This could be discovered through scanning or research.

2. Customizing the Exploit:
Once the vulnerability is found, select the corresponding Metasploit module (e.g., ms17_010_eternalblue) and configure its parameters (e.g., RHOSTS, RPORT, LHOST, etc.) using the set command.

RESULT:

Successfully exploited a vulnerable service using Metasploit and gained a Meterpreter session on the target system, demonstrating the power of automated exploitation tools for penetration testing.