METASPLOIT

EXP.NO: 14

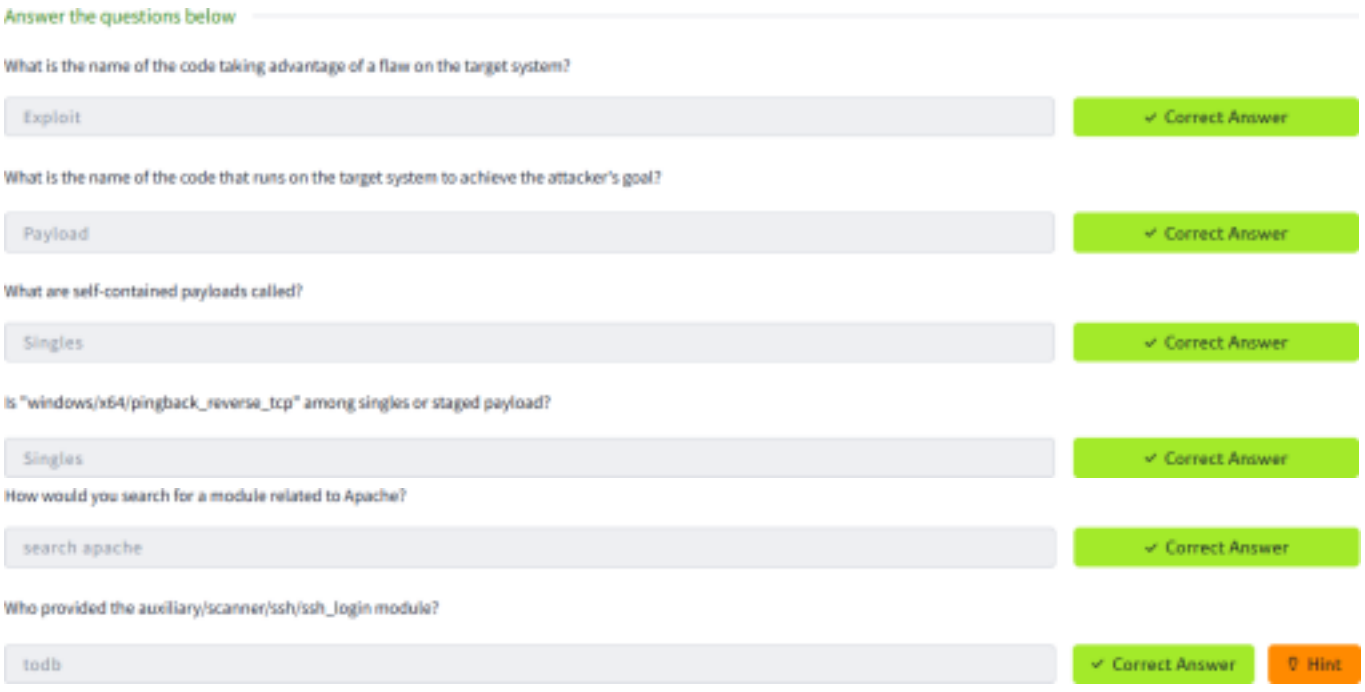
AIM:

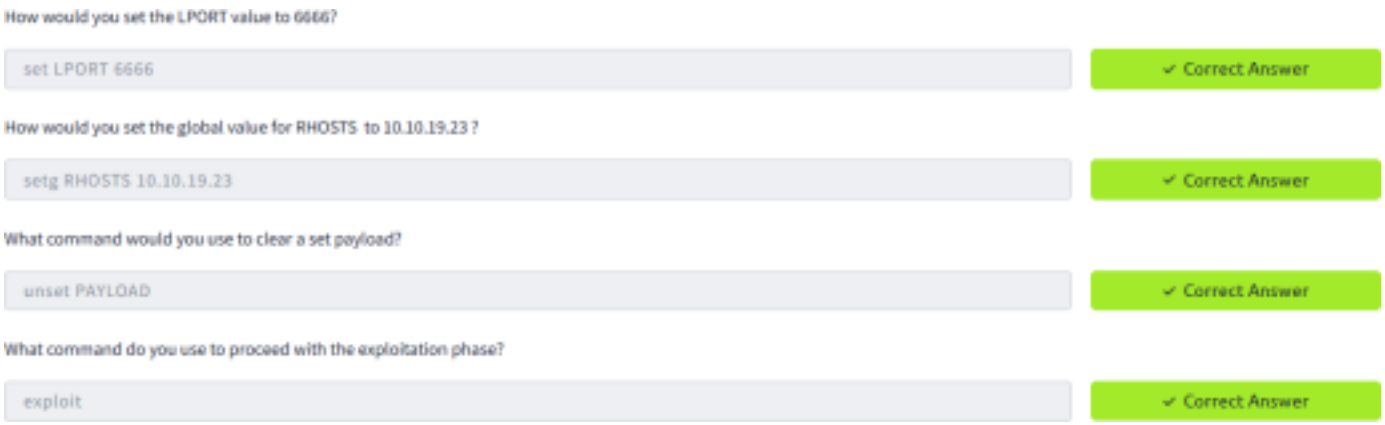
The aim of this experiment is to explore and understand the basic usage of the Metasploit Framework, focusing on exploiting vulnerabilities in a target system using various Metasploit modules, setting appropriate parameters, and successfully executing the exploit to gain access to the system.

ALGORITHM:

1. Identify Vulnerability: Use the search function to find exploits related to the target system.
2. Select Exploit: Choose an appropriate exploit based on the identified vulnerability (e.g., MS17-010 EternalBlue).
3. Configure Exploit: Set the necessary parameters such as target IP (RHOSTS), payload, and local port (LPORT).
4. Choose Payload: Select the payload that will run on the target system to achieve the desired result (e.g., reverse TCP shell).
5. Execute Exploit: Launch the exploit to attempt to compromise the target system.
6. Post-Exploitation: After successful exploitation, interact with the compromised system through the Meterpreter session or other post-exploitation tools.

OUTPUT:





RESULT:

As far we have seen, Metasploit is a powerful tool that facilitates the exploitation process. It would be best if you had used the ms 17-010-eternal blue exploit to gain access to the targetVM