METASPLOIT

EXP.NO: 14   **DATE:15-04-2025**

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:

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 |

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 | ♀ Hint |

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 |

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

NANDITHA N   220701182