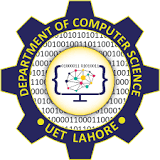
**LAB REPORTS**



**Session 2023-2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza

**Course:**

Information Security

**Department of Computer Science**

**University of Engineering and Technology,**

**Lahore Pakistan**

Contents

[**TASK 3 EXPLORING THREAT AGENTS** 3](#_Toc188787422)

[**1.** **Metasploit Framework:** 3](#_Toc188787423)

[**2.** **Process Followed:** 3](#_Toc188787424)

[ **msfconsole:** 3](#_Toc188787425)

[ **Exploit:** 3](#_Toc188787426)

[**3.** **CONCLUSION:** 6](#_Toc188787427)

# **TASK 4 EXPLORING THREAT AGENTS**

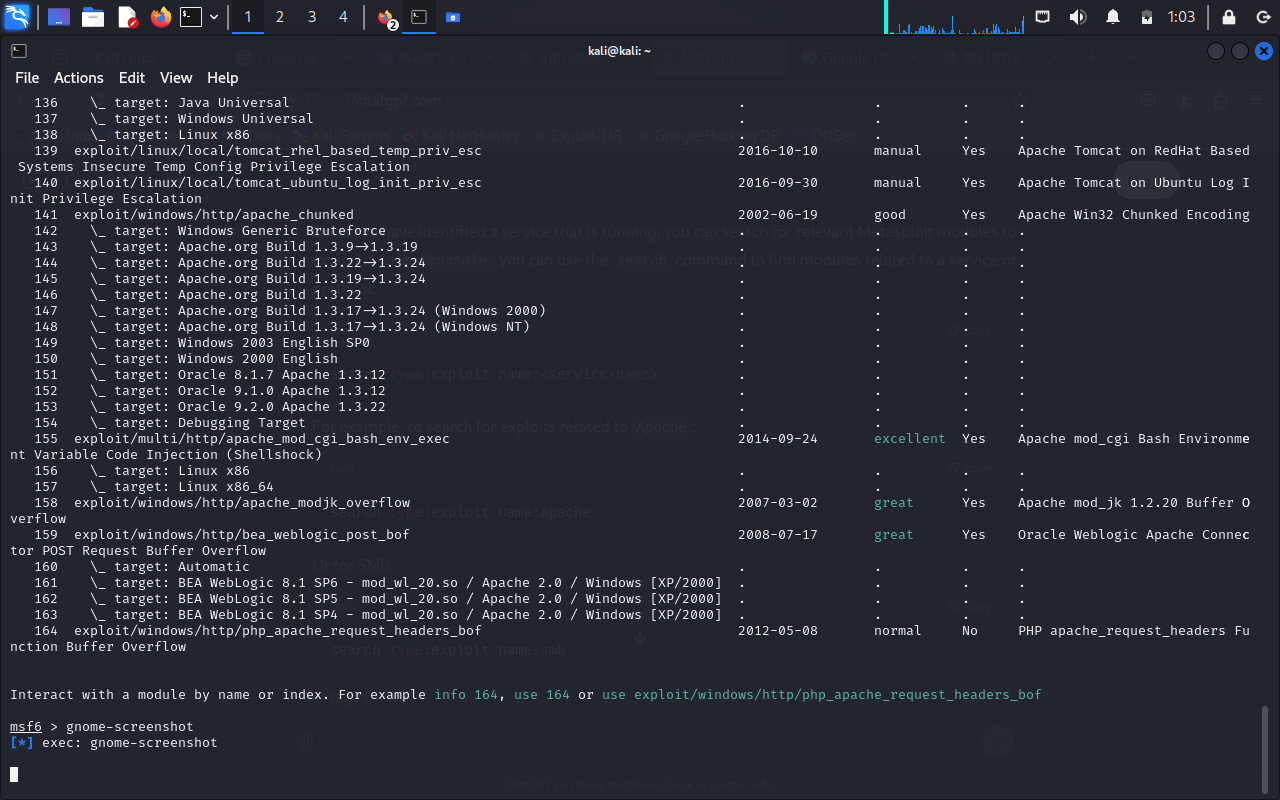
## **Metasploit Framework:**

This report presents an analysis of threat agents to exploit the vulnerabilities in a system using Metasploit Framework.

## **Process Followed:**

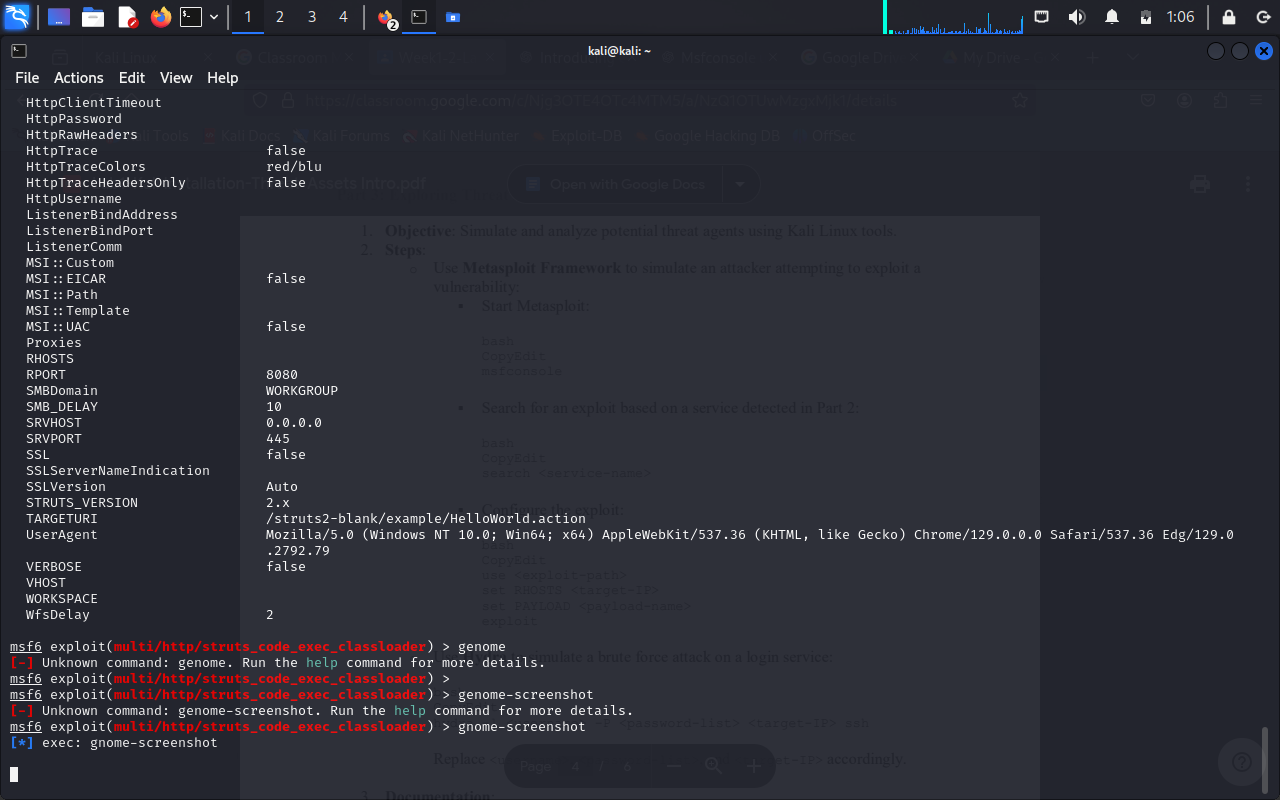
### **msfconsole:**

It opens interface for Metasploit Framework. After that search command is used to search for exploiting vulnerabilities.



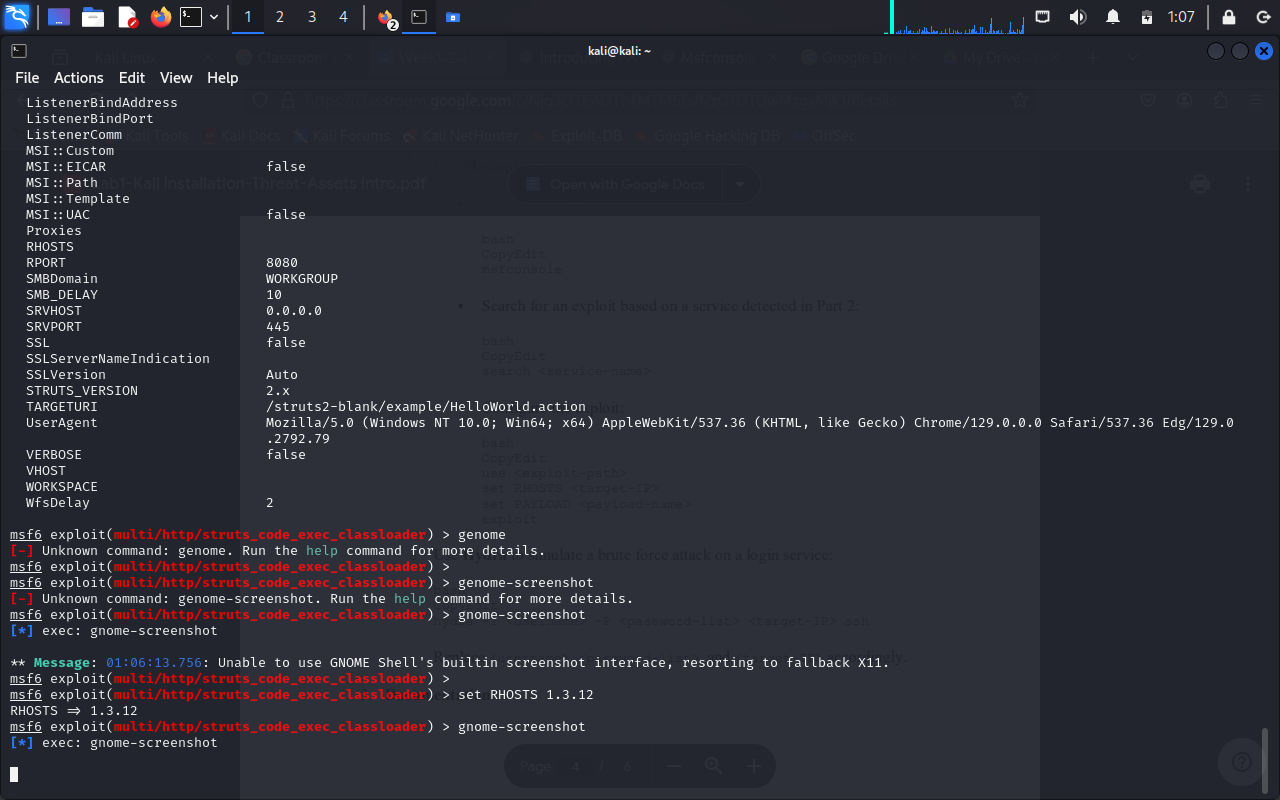
### **Exploit:**

After exploiting the specific path it provides all the data related to that path where you can exploit its vulnerabilities.

****

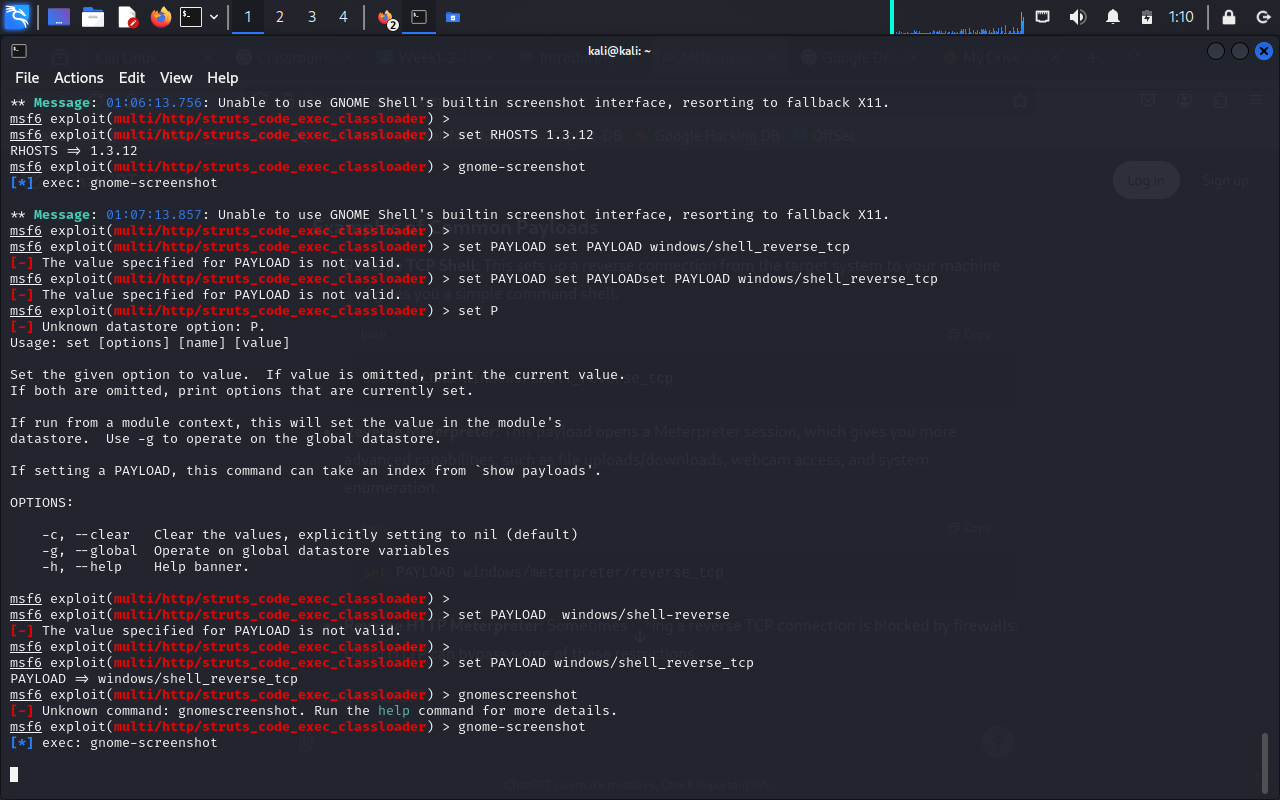
* **RHOSTS:**

It is used to specify target host or network range for an exploit It defines the systems you want to attack or test against.

****

* **PAYLOAD:**

The payload command in Metasploit is used to specify the type of payload that will be delivered to the target system during an exploit.

****

# **CONCLUSION:**

The vulnerability research identified critical security risks in the software infrastructure. Immediate remediation actions are recommended to address high-risk vulnerabilities. Implementing long-term security best practices will further strengthen the system’s resilience against cyber threats.