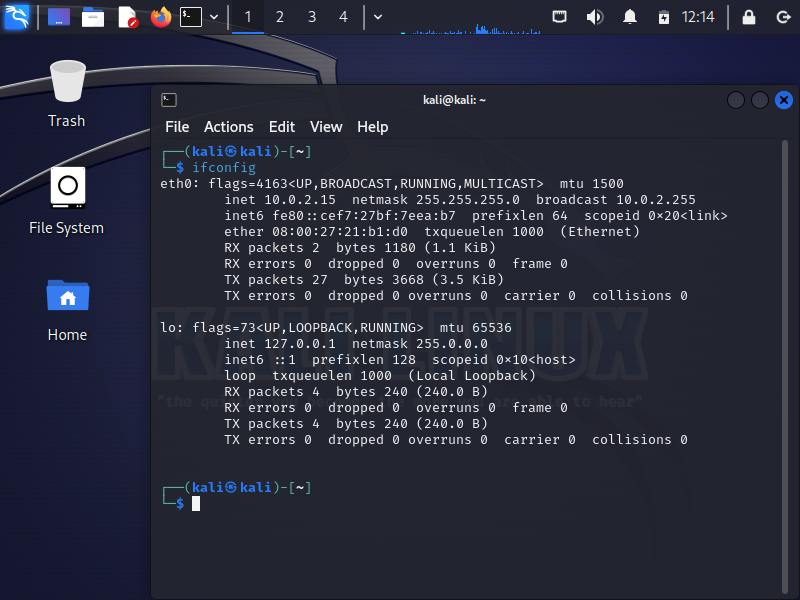
**NITHIN THOMAS NINAN ERUTHICKAL**

**8866468**

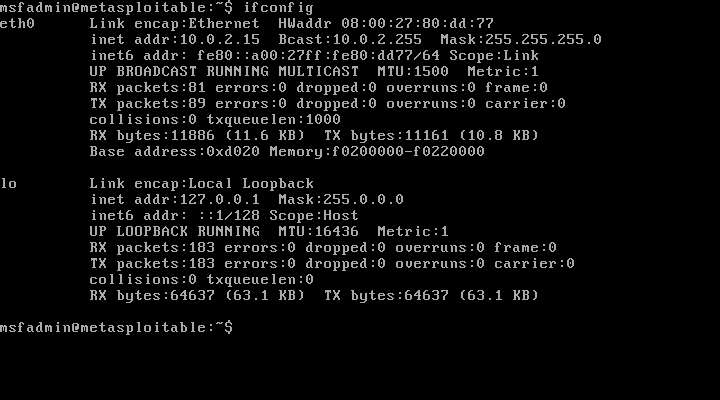
**Assignment #1**

**22-Jan-2024**

**Task1**

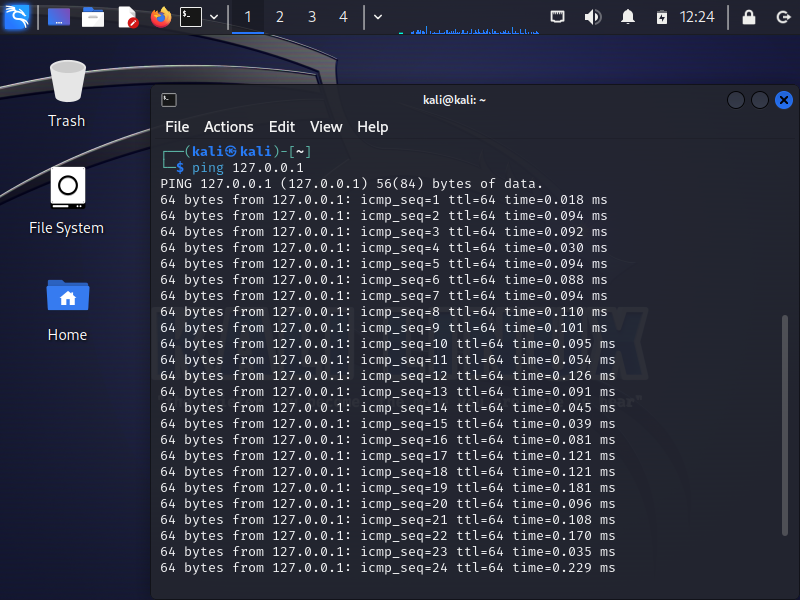
IP address of Kali (127.0.0.1)

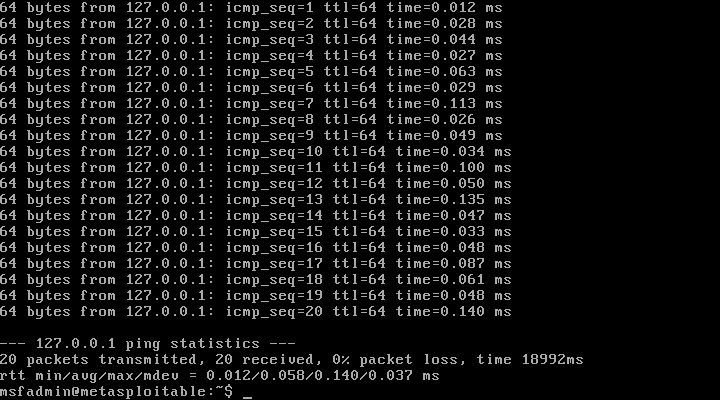
IP address of Metasploitable (127.0.0.1)



IP address of Kali and Metasploitable were found using the command “ifconfig” in both the machines

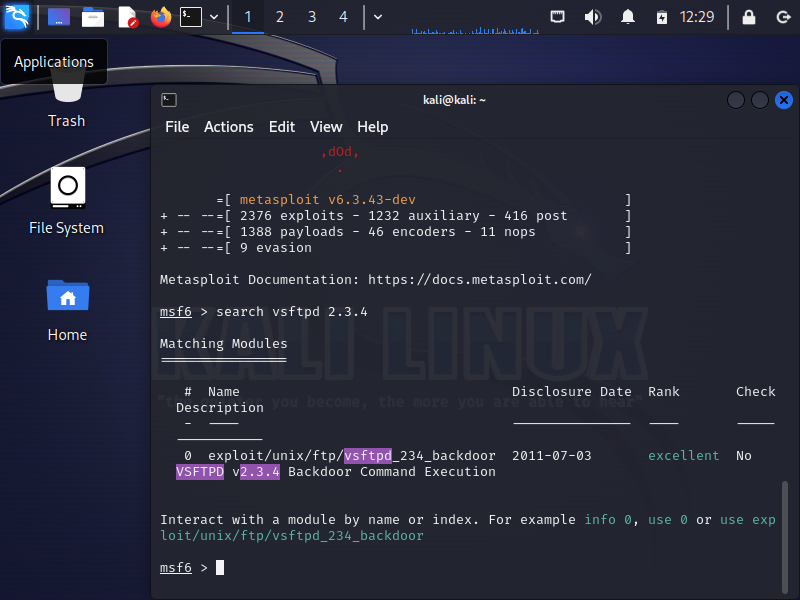
**Task2**





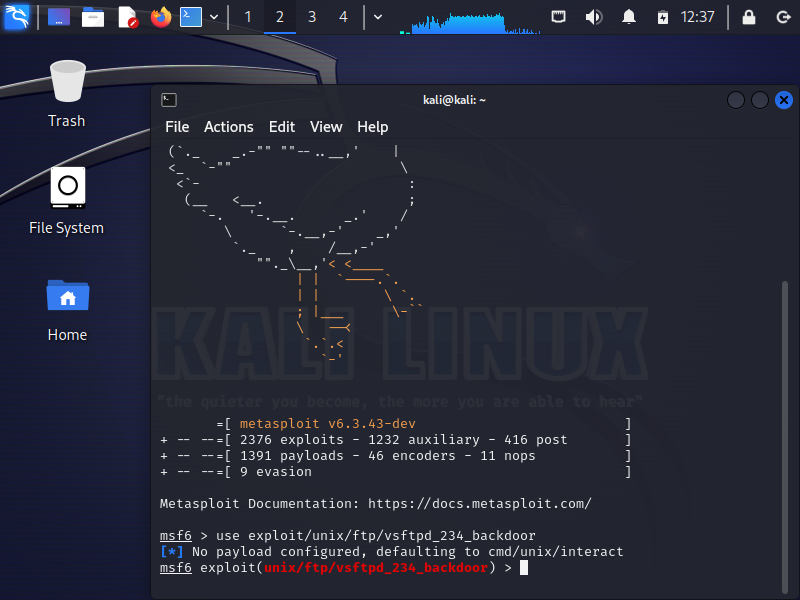
Command used: ping 127.0.0.1(IP address) in both kali and Metasploitable to check and view the success responses.

**Task3**



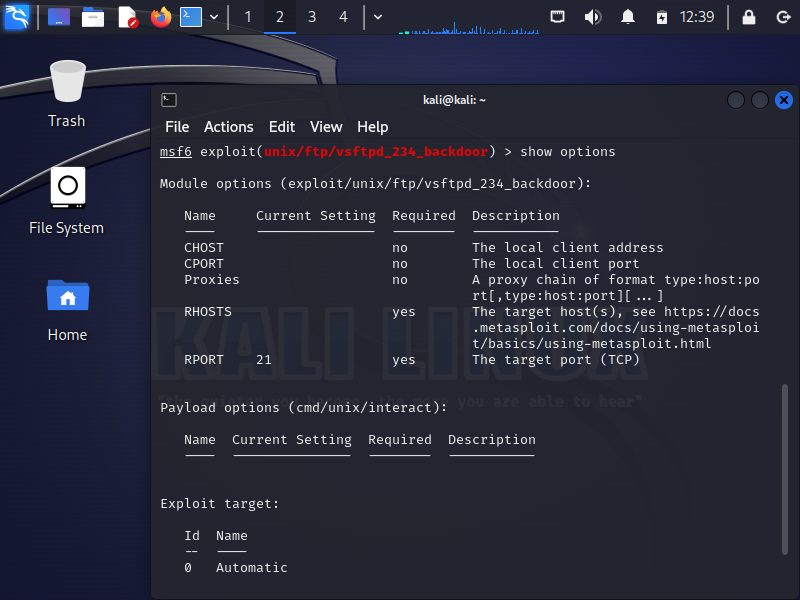
Command used: msfconsole to start the Metasploit and search vsftpd 2.3.4 to view the modules related to vsftpd 2.3.4

**Task4**



Command used: use exploit/unix/ftp/vsftpd\_234\_backdoor

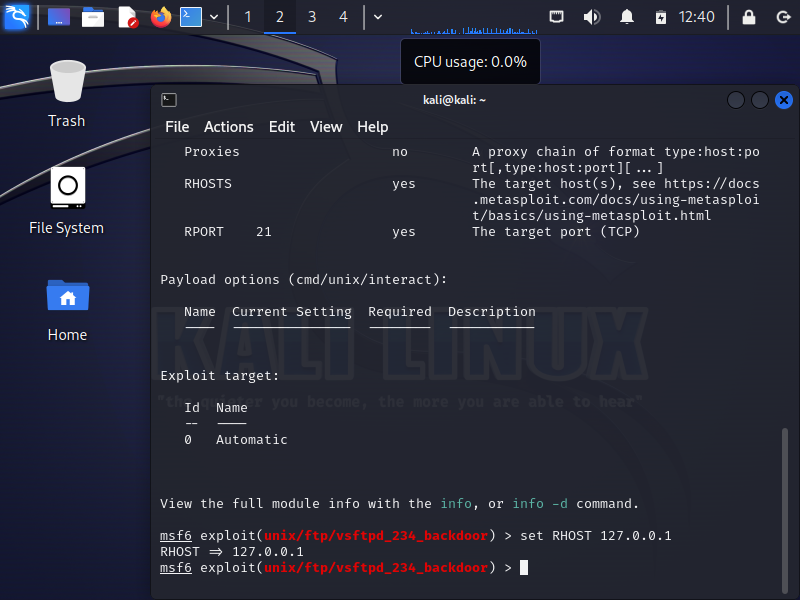
**Task5**



Command used: show options

Displays the payload options

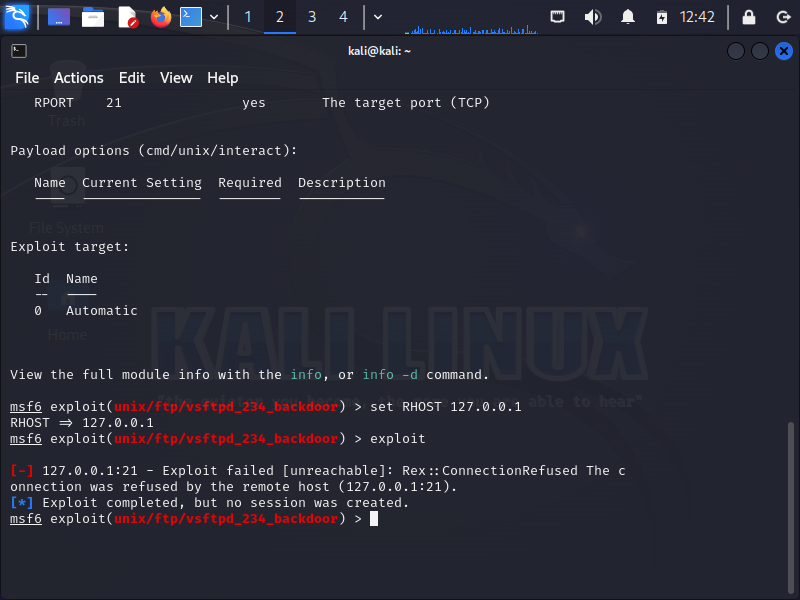
**Task6**



Command used set RHOST 127.0.0.1

Changes the RHOST to 127.0.0.1

**Task7**



Command used: exploit

Result: Exploit completed, but no session was created

**Task 8**

What worked well:

* I was able to locate and record the IP addresses of the Metasploitable 2 and Kali virtual machines.

* The ping command confirmed that the two virtual machines could communicate as anticipated.

* Metasploit was launched successfully on the Kali virtual machine, and the search for vsftpd 2.3.4 proceeded without any problems.

What didn’t work well:

I was having trouble with the payload when attempting to exploit the vsftpd 2.3.4 backdoor. Before using the exploit, I had to set a payload using the set PAYLOAD command.

Thing I learned

I gained hands-on experience using Metasploit to exploit vulnerabilities in a controlled environment. This assignment helped reinforce my understanding of penetration testing techniques and the importance of proper configuration when using exploit frameworks.