

**INT 301 Project**



**L**OVELY  
**P**ROFESSIONAL  
**U**NIVERSITY

NAME: Mudambi Himakiran

REGNO: 11902561

SECTION:KE022

Rollno: 39

Faculty: Dr. Manjot Kaur

Name of the University: Lovely Professional University

Date of submission: 22<sup>nd</sup> March 2023

**You are performing a gray box penetration test. You want to craft a custom packet to test how a server responds and to see what information it responds with. use any open source to do this.**

### **I-INTRODUCTION:**

Grey box penetration testing is a type of penetration testing where the tester has limited knowledge of the target system or application being tested. In grey box testing, the tester has some information about the target system, such as network topology, IP addresses, or system architecture, but does not have full access to the source code or detailed system documentation.

The purpose of grey box penetration testing is to simulate a real-world attack scenario where an attacker has some knowledge of the target system, but not enough to exploit all vulnerabilities. This type of testing can help organizations identify vulnerabilities that can be exploited by attackers with limited knowledge of their systems and applications.

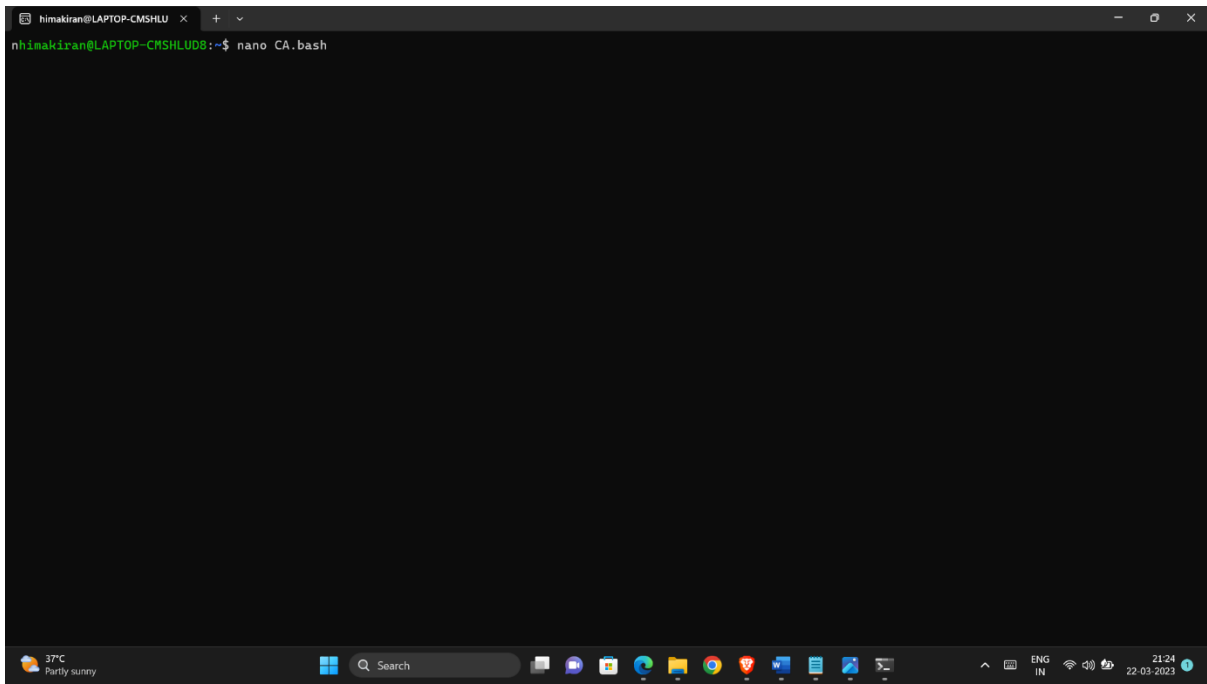
### **DESCRIPTION:**

The question is asking for guidance on how to perform a gray box penetration test by crafting a custom packet to test a server's response and analyze the information it sends back. The question specifies that an open-source tool should be used for this task.

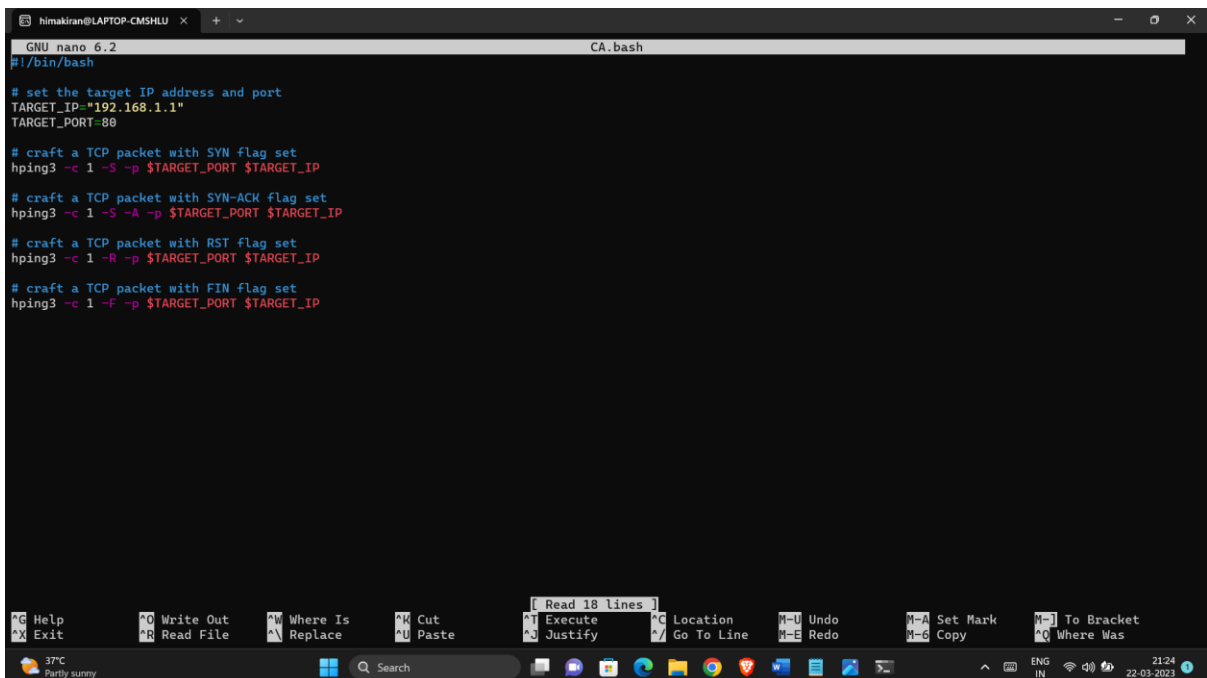
### **SCOPE:**

The Scope of the project is how to perform a gray box penetration test by crafting a custom packet to test a server's response and analyze the information it sends back. The question specifies that an open-source tool should be used for this task.

## II- Analysis Report:



Shell script creating with nano with the file name as CA.bash

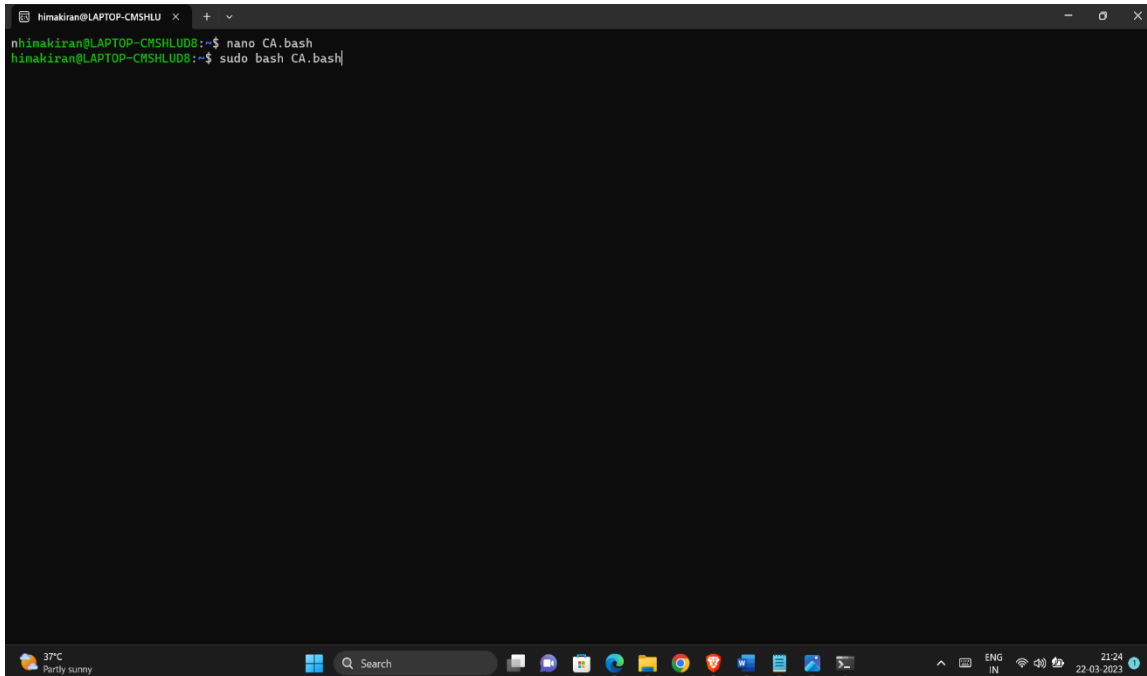


This script uses the hping3 tool to craft different TCP packets with various flags set and sends them to a target IP address and port. The script can be used for testing and network troubleshooting.

- The first line crafts a TCP packet with the SYN flag set, which is used to initiate a connection.
- The second line crafts a TCP packet with the SYN-ACK flags set, which is used to acknowledge

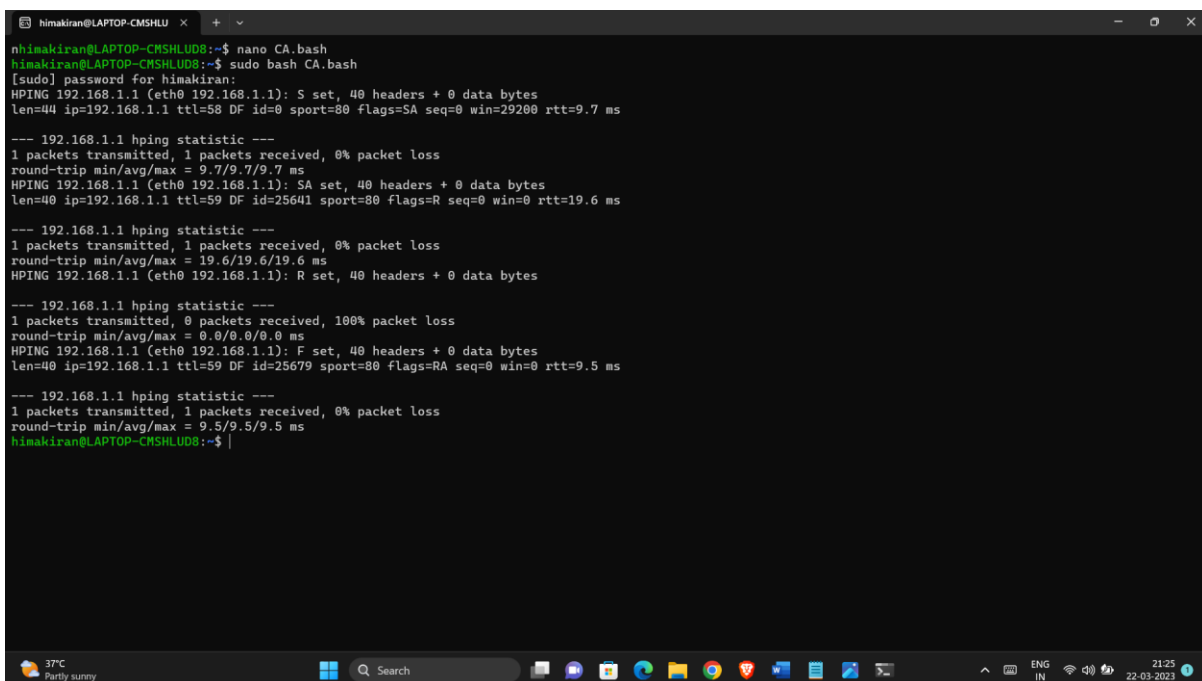
the initiation of a connection.

- The third line crafts a TCP packet with the RST flag set, which is used to reset a connection.
- The fourth line crafts a TCP packet with the FIN flag set, which is used to terminate a connection.



```
himakiran@LAPTOP-CMSHLU x + v
nhimakiran@LAPTOP-CMSHLUD8:~$ nano CA.bash
himakiran@LAPTOP-CMSHLUD8:~$ sudo bash CA.bash
```

Now we type the command `sudo bash CA.bash` for getting the outputs



```
himakiran@LAPTOP-CMSHLU x + v
nhimakiran@LAPTOP-CMSHLUD8:~$ nano CA.bash
himakiran@LAPTOP-CMSHLUD8:~$ sudo bash CA.bash
[sudo] password for himakiran:
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
len=44 ip=192.168.1.1 ttl=58 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=9.7 ms

--- 192.168.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 9.7/9.7/9.7 ms
HPING 192.168.1.1 (eth0 192.168.1.1): SA set, 40 headers + 0 data bytes
len=40 ip=192.168.1.1 ttl=59 DF id=25641 sport=80 flags=R seq=0 win=0 rtt=19.6 ms

--- 192.168.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 19.6/19.6/19.6 ms
HPING 192.168.1.1 (eth0 192.168.1.1): R set, 40 headers + 0 data bytes

--- 192.168.1.1 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.1.1 (eth0 192.168.1.1): F set, 40 headers + 0 data bytes
len=40 ip=192.168.1.1 ttl=59 DF id=25679 sport=80 flags=RA seq=0 win=0 rtt=9.5 ms

--- 192.168.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 9.5/9.5/9.5 ms
himakiran@LAPTOP-CMSHLUD8:~$
```

The output of an HPING tool running on a device with IP address 192.168.1.1. HPING is a command-line oriented TCP/IP packet assembler/analyzer tool for Linux and other operating systems.

The first line indicates that a packet was sent with the "S" flag set (SYN). This is part of the TCP three-way handshake, which is used to establish a connection between two devices. The packet was sent to port 80 (HTTP), and the response shows that a packet was received with the "SA" flag set, indicating that the destination device is willing to establish a connection. The round-trip time (RTT) is 19.5 ms.

The second line indicates that another packet was sent with the "SA" flag set (SYN-ACK). This is the second part of the TCP three-way handshake, which acknowledges the receipt of the first packet and establishes the connection. The response shows that a packet was received with the "R" flag set (RESET), indicating that the destination device has reset the connection.

The third line indicates that a packet was sent with the "R" flag set (RESET). This indicates that the sender has reset the connection.

The fourth line indicates that a packet was sent with the "F" flag set (FIN). This is part of the TCP connection termination process. The response shows that a packet was received with the "RA" flag set (FIN-ACK), indicating that the destination device is acknowledging the termination of the connection.