CHRIST
UNIVERSITY
BENGALURU, INDIA

Declared as Deemed to be University under Section 3 of UGC Act 1956

School of Engineering and Technology

Department of AIML & DS

ETHICAL HACKING (CSHO331CSP)

Topic: Ncat Chat Terminal

Name: Abel Alexander

Registration Number: 2462004

Academic Year: 2025-2026

Name: Abel Alexander
Register Number: 2462004
Class: 3BTCSAIML A

Index

Name: Abel Alexander
Register Number: 2462004
Class: 3BTCSAIML A

Objective: Create a simple chat system between two computers using network tools.

This assignment required building a basic, real-time text chat between a MacBook (Host) and a Kali Linux Virtual Machine (Guest) using the `ncat` and `nc` utilities. This report details the network setup, the scripts used, and the cybersecurity principles demonstrated by the project.

1. Network Setup & IP Addresses

To enable direct communication, the Kali VM was configured with a **Bridged Adapter** in VirtualBox, allowing it to function as a separate device on the same network as the MacBook. Due to initial DHCP failures, a static IP address was manually assigned to Kali Linux.

- **MacBook (Host) IP:** `172.16.213.190`
- **Kali Linux (Guest) IP:** `172.16.213.191`

The static IP configuration successfully placed both machines on the same subnet, establishing the necessary foundation for the chat.

2. Ncat Chat Terminal Scripts

The chat system was implemented using the `nc` command on the Kali listener and the `ncat` command on the Mac connector.

Terminal A: Listener Script (Kali Linux)

This script sets up a listener on Kali, waiting for connections on port `12345`.

```
# Purpose: Listen for incoming Netcat
connections on port 12345.
nc -lvp 12345
```

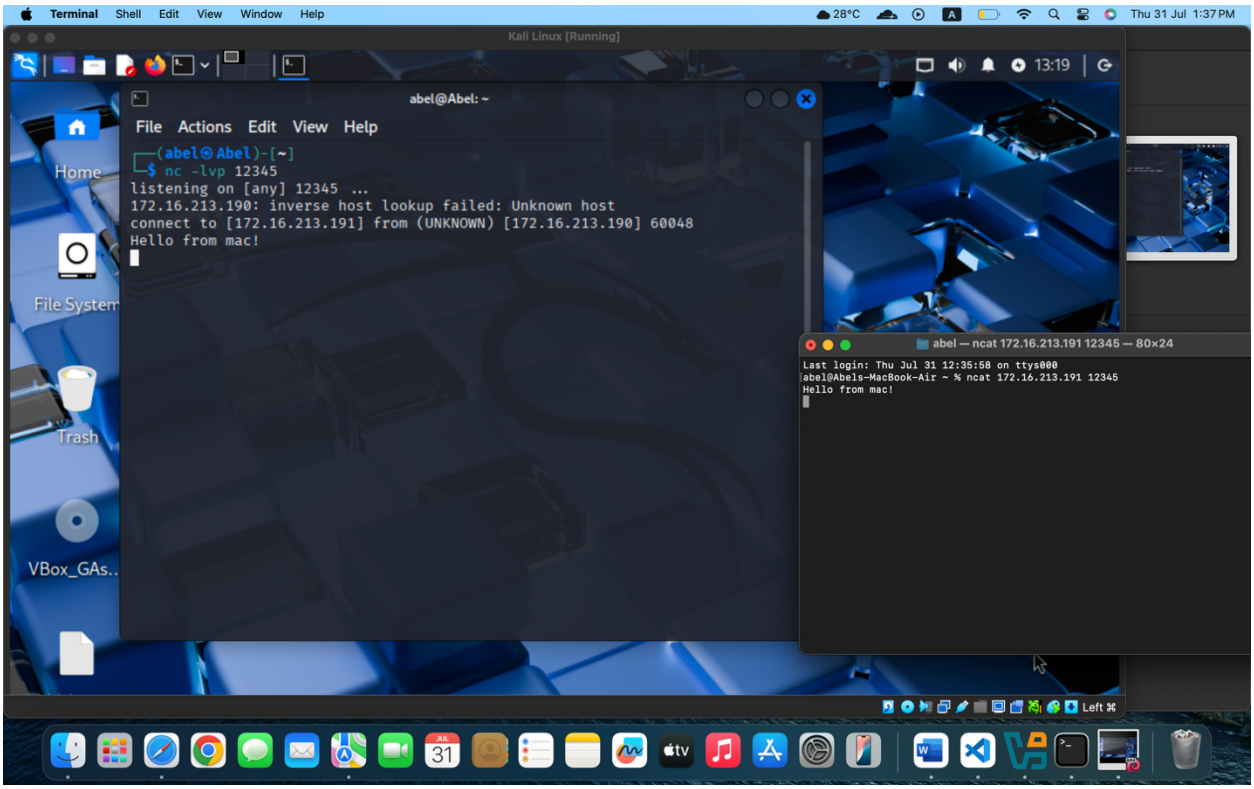
Terminal B: Connector Script (MacBook)

This script initiates a connection from the MacBook to the Kali listener.

```
# Purpose: Connect to the Netcat listener and
send/receive messages.
ncat 172.16.213.191 12345
```

3. Demonstration of Chat Functionality

With the scripts executed on their respective terminals, a successful connection was established. Messages typed in one terminal were instantly visible in the other, demonstrating a functional bidirectional chat.



4. Cybersecurity Relevance

This project provides practical experience with foundational cybersecurity concepts:

- **Network Primitives:** It reinforces understanding of IP addresses (device identity) and ports (application identity), which are fundamental to all network communication and security.
- **Client-Server Model:** The setup illustrates this fundamental model, which is essential for analyzing network traffic and services.

- **Vulnerability Scanning:** The listener on Kali demonstrates how services expose themselves on ports. In a real-world scenario, attackers scan for open ports to find exploitable services.
- **Unencrypted Data:** The plain-text chat highlights the vulnerability of unencrypted data. It shows how easily this information could be intercepted, emphasizing the need for encryption in all secure communications.
- **Command & Control (C2) Simulation:** The chat system directly simulates how malicious tools like Netcat can be used to establish a C2 channel, providing an attacker with remote access to a compromised machine.

Through this hands-on assignment, the theoretical concepts of network communication are made tangible, providing a solid foundation for further study in network security.