William Fan

Aug 10th 2025

Prof. Lemma

Lab Objective:

This lab aims to set up and configure TightVNC on an Kali Linux to enable secure remote desktop access via an SSH tunnel. I installed VNC Server on Kali Linux, and was able to establish a connection via an app called VNC Viewer on my MacOS machine. I also connect to a different machine in a different network.

Lab Questions[Extra Point]:

1. Are you able to access your teammate’s machine or VM setup?

Yes.

2. What concerns should you bring to your organization’s IT manager regarding remote

Connection?

1) Weak authentication risks, as TightVNC only requires a static password, which could be compromised.

2) Unencrypted data transmission, as the setup showed warnings about an unencrypted connection.

3) Unsecured devices potentially introducing malware, since there are no restrictions on connecting devices.

4) Lack of monitoring for suspicious activity on the VNC connection.

3. How do you protect your network and devices when you have a remote access policy?  
 1) Use strong passwords and enable MFA to enhance authentication.

2) Encrypt all data in transit using an SSH tunnel for secure communication.

3) Deploy a VPN to create a secure connection channel.

4. What would you consider implementing for endpoint protection when you have remote

connection policy?

1) Use a firewall to block unauthorized access.

2) Implement Endpoint Detection and Response (EDR) tools for real-time monitoring.

3) Install antivirus software to detect and remove malware.

5. Consider the following and associate the benefits they provide with remote connection security.

a. MFA: Adds extra authentication layer, reducing unauthorized access.

b. Encryption: Protects data from interception during transmission.

c. VPN: Creates secure tunnel for remote access, hiding traffic.

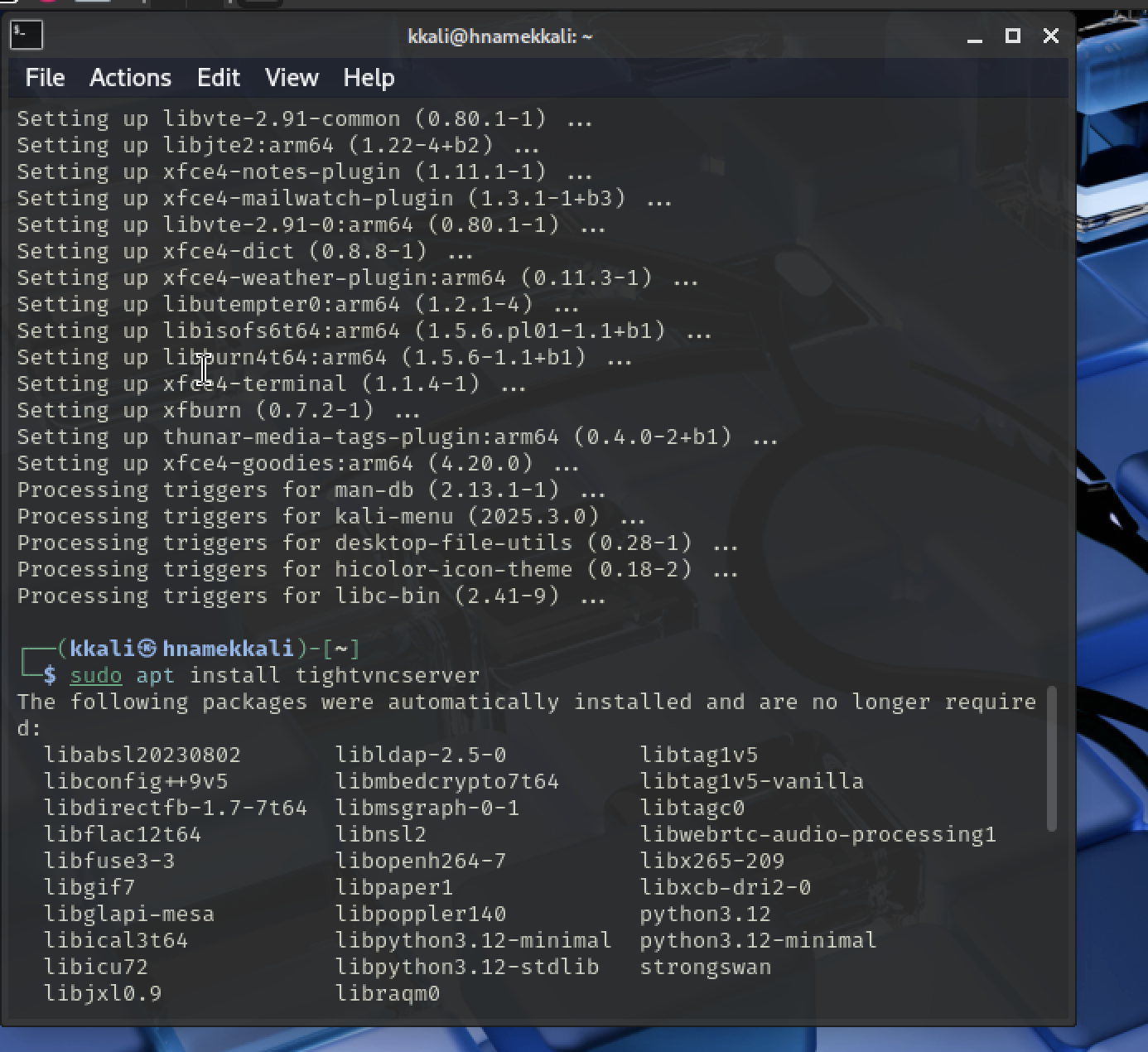
d. IDS/IPS: Detects and blocks suspicious network activity.

e. Antivirus: Scans and removes malware from devices.

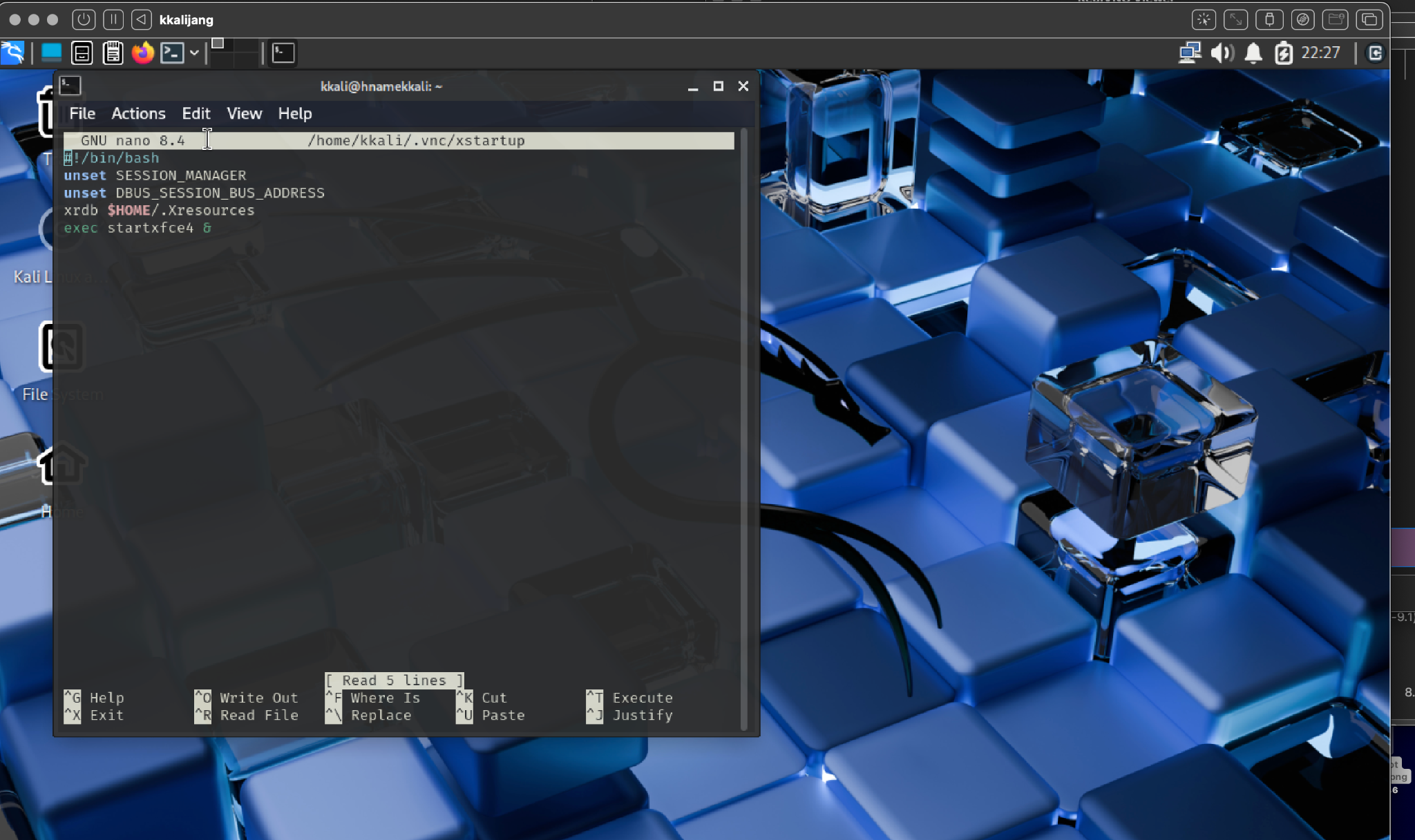
f. IT Department Members: Monitor systems, enforce policies, and respond to incidents.

Lab Screenshots

Sc1:



Sc2:



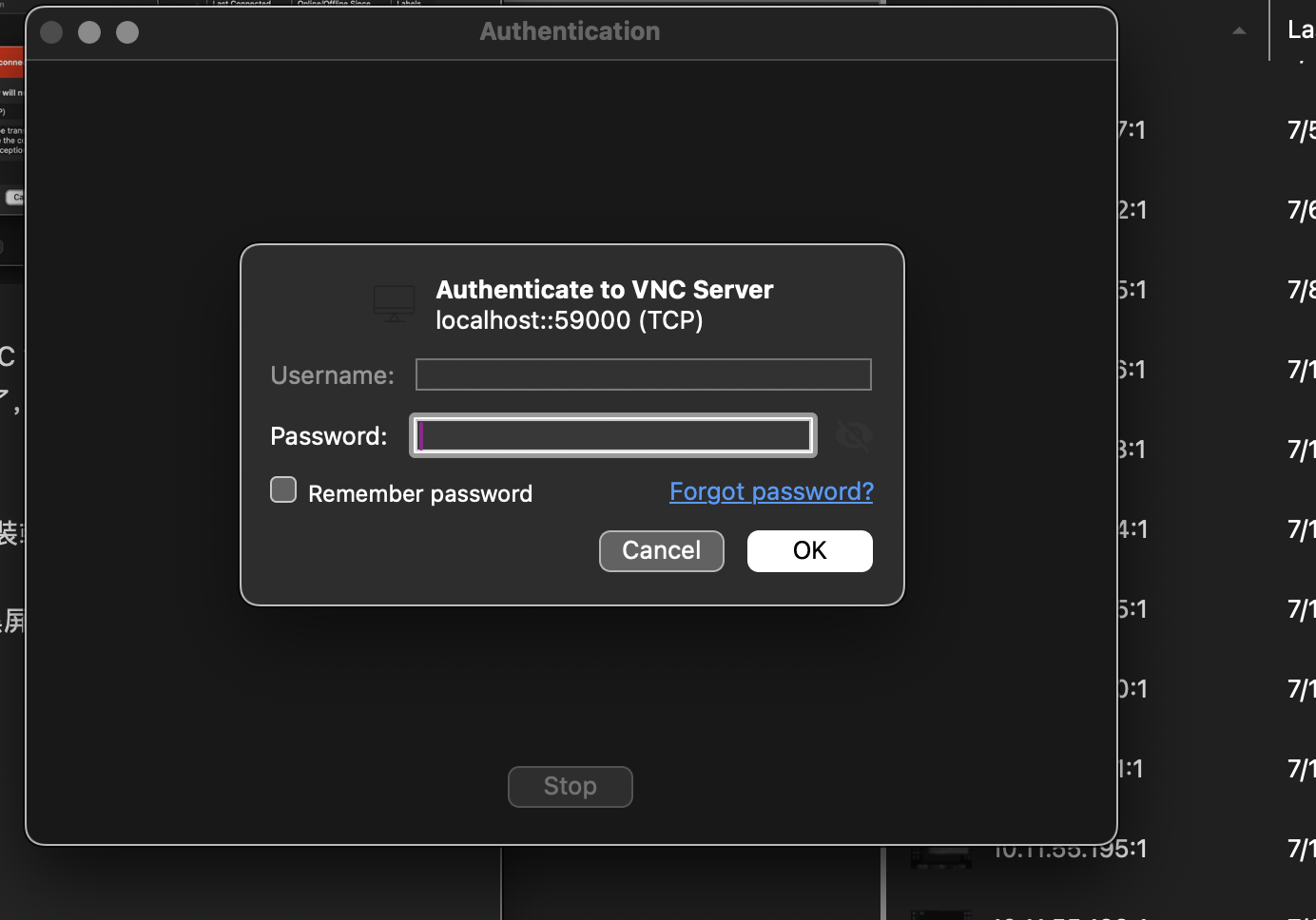
Sc3:



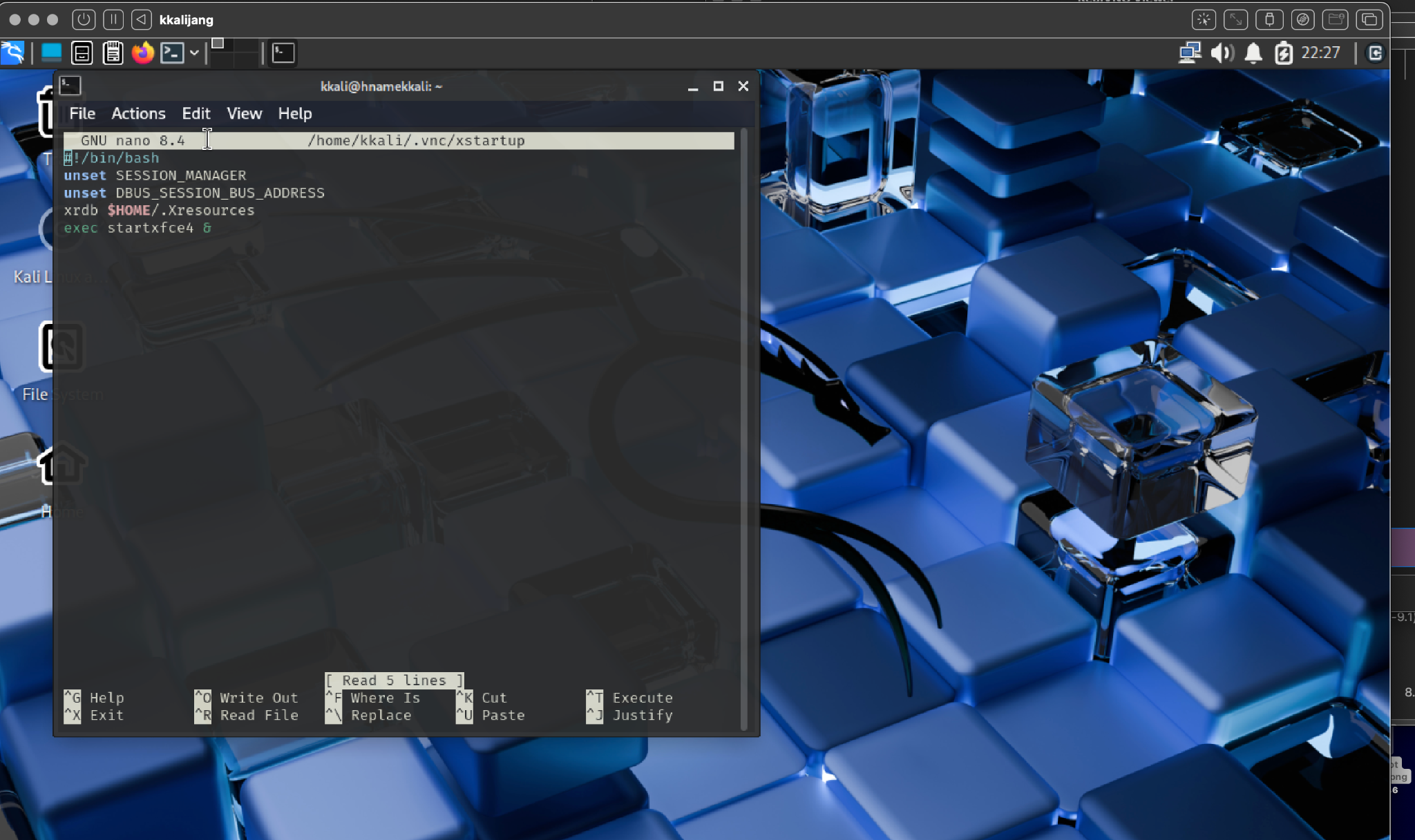
Sc4:



Sc5:



Sc6:



Extra Point: