**Linux Network Configuration**

**Project Overview**

The aim of this project is to demonstrate my proficiency as an entry-level cybersecurity analyst, showcasing my skills in Linux commands, network configurations, SSH key generation, SCP and RSYNC file transfer protocols, and secure device connections. This project involves configuring a virtual machine with a static IP address, generating SSH keys, securely connecting two devices using SSH, and transferring files using SCP and RSYNC.

Key Accomplishments:

* Configured a virtual machine with a static IP address using Ubuntu Linux and Netplan.
* Generated SSH keys and securely connected two devices using SSH.
* Implemented best practices for SSH security, including key pair management, disabling root login, and limiting user access.

Technical Details:

* Assigned a static IP address to a virtual machine using Netplan configuration.
* Generated SSH keys using the **ssh-keygen** command and securely transferred the public key to another device.
* Implemented SSH best practices, such as disabling password authentication and changing the default listening port.

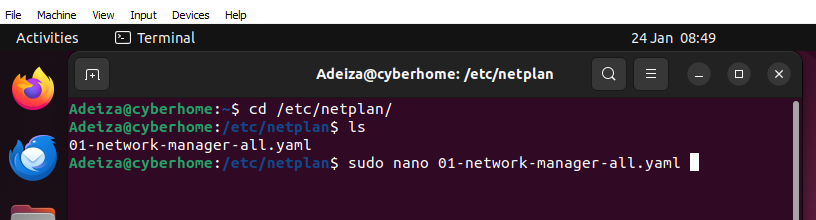
Potential Challenges:

* Ensuring proper permissions and syntax when configuring Netplan and SSH.
* Troubleshooting SSH connection issues, such as firewall settings or incorrect credentials.
* Understanding the differences between SCP and RSYNC and choosing the appropriate method for specific use cases.

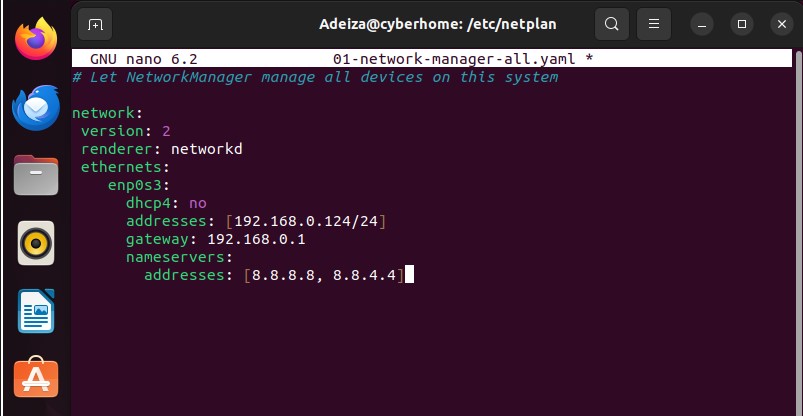
By completing this project, I have showcased my ability to manage Linux systems, configure network settings, and implement secure file transfer protocols. This project serves as a foundation for further exploration of cybersecurity concepts and techniques.

**Assign IP address to a virtual machine**

* **Identify the Network Interface**: Begin by identifying the network interface that you want to configure. You can use the **ifconfig** command to list all the available network interfaces on your system.
* **Locate the Netplan Configuration File**: Next, locate the Netplan configuration file, which is typically found in the **/etc/netplan/** directory. Netplan is a network configuration tool used in Ubuntu and other Linux distributions.
* **Edit the Netplan Configuration File**: Open the Netplan configuration file using a text editor with root privileges. For example, you can use the **nano** editor to open the file: **$ sudo nano /etc/netplan/“config\_file”**

****

**Configure the Network Interface**: In the Netplan configuration file, configure the network interface by specifying the desired IP address, netmask, gateway, and DNS servers. Here is an example configuration:



After configuring the network interface in the Netplan configuration file, make sure to replace "Interface", "[Ip\_address/netmask]", gateway, and server address with the appropriate values for your specific network environment. Since we want to assign a static IP address, set **dhcp4** to **no**.

Once you have made the necessary changes, save and exit the file using the keyboard shortcut **Ctrl+O** followed by **Enter**, then **Ctrl+X**.

Next, apply the changes to the IP address using the command, **$** **sudo netplan apply**. This command updates the network interface configuration and applies the new IP address.

To verify the new IP address, run the command **$** **ip addr show "interface\_name"**. In this example, the interface name is **enp0s3**. Replace **enp0s3** with the actual name of your network interface. This command displays the network interface configuration, including the new IP address.

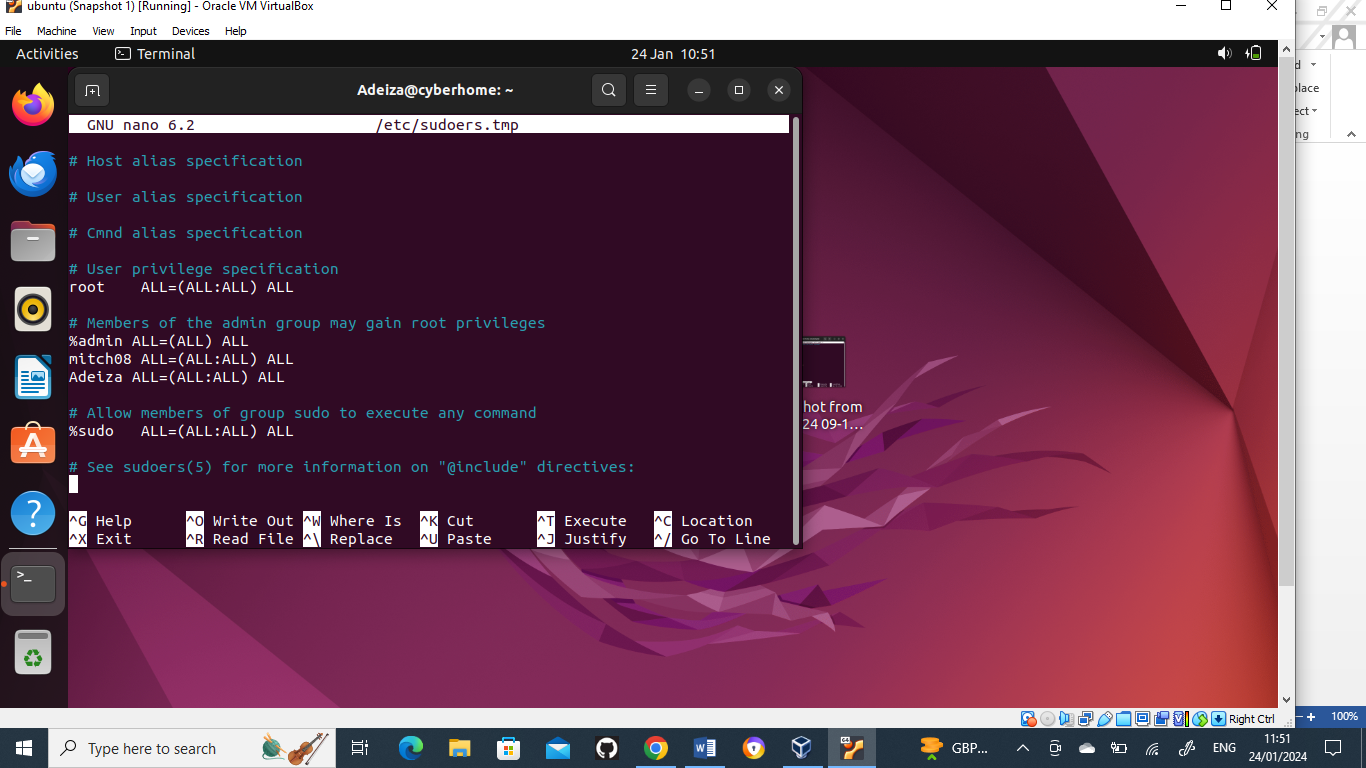
By following these steps, you can successfully assign a static IP address to a network interface and verify the new IP address using the **$** **ip addr show** command. This skill is essential for any cybersecurity professional, as it allows you to configure and manage network interfaces, ensuring secure and stable network connectivity.

**Challenges Faced:**

* Permission issue while trying to configure the network interface due to lack of **sudo** privileges.

**Resolution:**

1. Log in as the root user and open the Sudoer configuration file using the command **sudo visudo**.
2. Add the user "me" to the sudoer file with the following configuration
3. Add user to sudoer file. In my case I am the user Adeiza and this is the configuration. “user” ALL= (ALL:ALL) ALL.



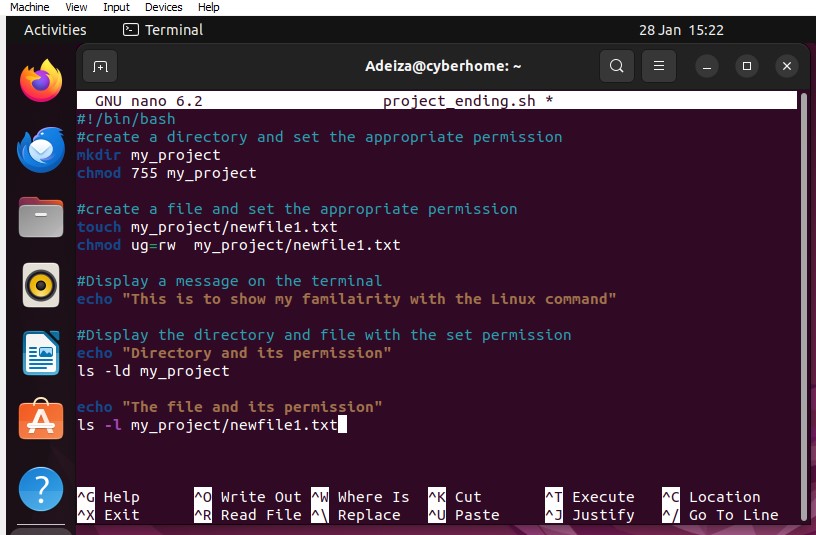
Note: Replace "user" with your actual username.

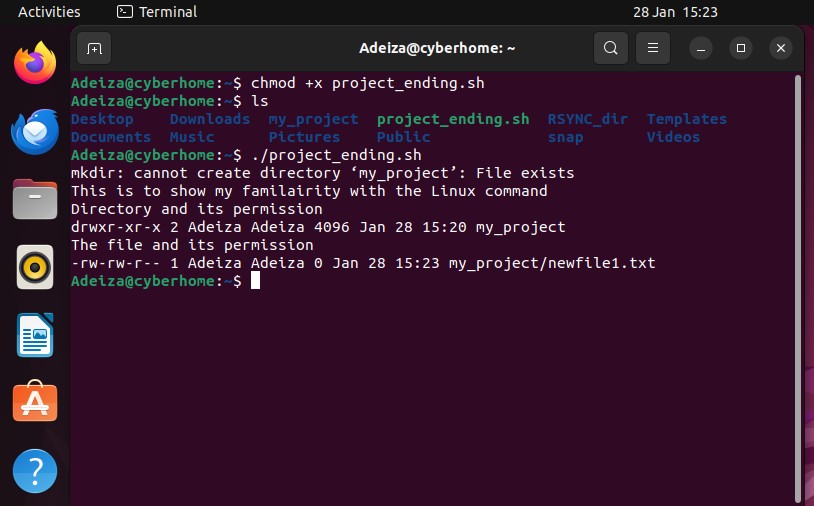
By following these steps, you can grant **sudo** privileges to a user, allowing them to execute commands with root privileges.

Be mindful of your syntax and grammatical errors in the configuration.

**Linux Command Exploration**

To highlight my familiarity with the Linux environment, I will write a script that create a directory and create a file inside the directory then set appropriate permission for both the file and the directory. It will also display a message and the permission of the file and directory created.





In conclusion, the Linux, Network Configuration and SSH project has provided a solid foundation for understanding and implementing essential cybersecurity skills. By completing this project, I have demonstrated my ability to configure a virtual machine with a static IP address, generate SSH keys, securely connect two devices, and also my basic understanding of Linux syntax. I have also showcased my understanding of SSH best practices, such as key pair management, disabling root login, and limiting user access.

This project has been an invaluable learning experience, allowing me to explore various aspects of Linux and network configurations. It has not only solidified my understanding of these concepts but also provided a strong starting point for further exploration in the field of cybersecurity. I am eager to continue building upon these skills and expanding my knowledge in areas such as intrusion detection, vulnerability management, and network security.

As an entry-level cybersecurity analyst, I am committed to continuous learning and growth, and I am confident that this project has prepared me well for the challenges and opportunities that lie ahead. I am excited to apply these skills in a professional setting and contribute to the protection and defence of digital assets and systems.

Thank you for considering my Linux and Network Configuration project as part of my resume. I am eager to bring my enthusiasm, dedication, and growing skillset to a dynamic and innovative cybersecurity team.