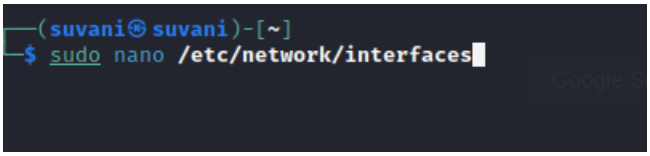
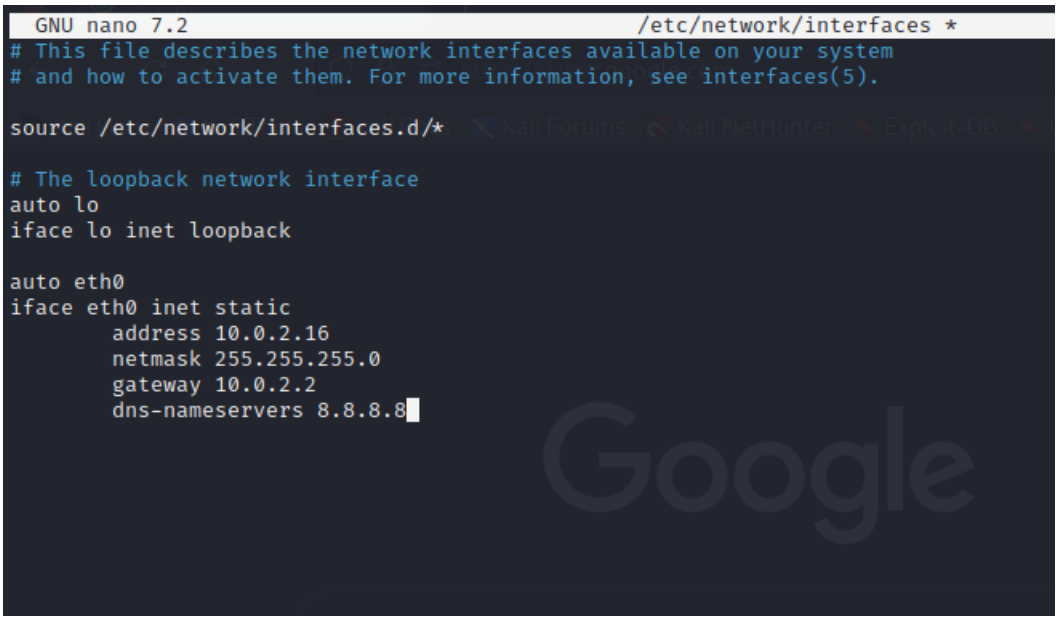
1)Configure the network settings of your Linux VM using a static IP address and verify the connection using ping protocol (Do not ping your IP). [10]

ans: I used to configure ip via static method using the network interface. The command along with sudo privilege was used inorder for configuration.

Step1



Step 2 doing nano into /network/interfaces



Step 3 concatinating using the cat command inorder to view if the ip has been set or not .

```
┌──(suvani㉿suvani)-[~]
└─$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 10.0.2.16
        netmask 255.255.255.0
        gateway 10.0.2.2
        dns-nameservers 8.8.8.8
```

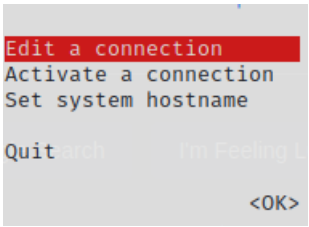
Hence, in this case it's clear that the ip has been set.

Method 2

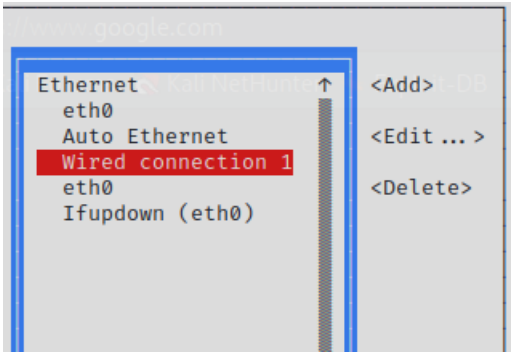
Using the command nmtui I went to this interface

```
┌──(suvani㉿suvani)-[~]
└─$ sudo nmtui
```

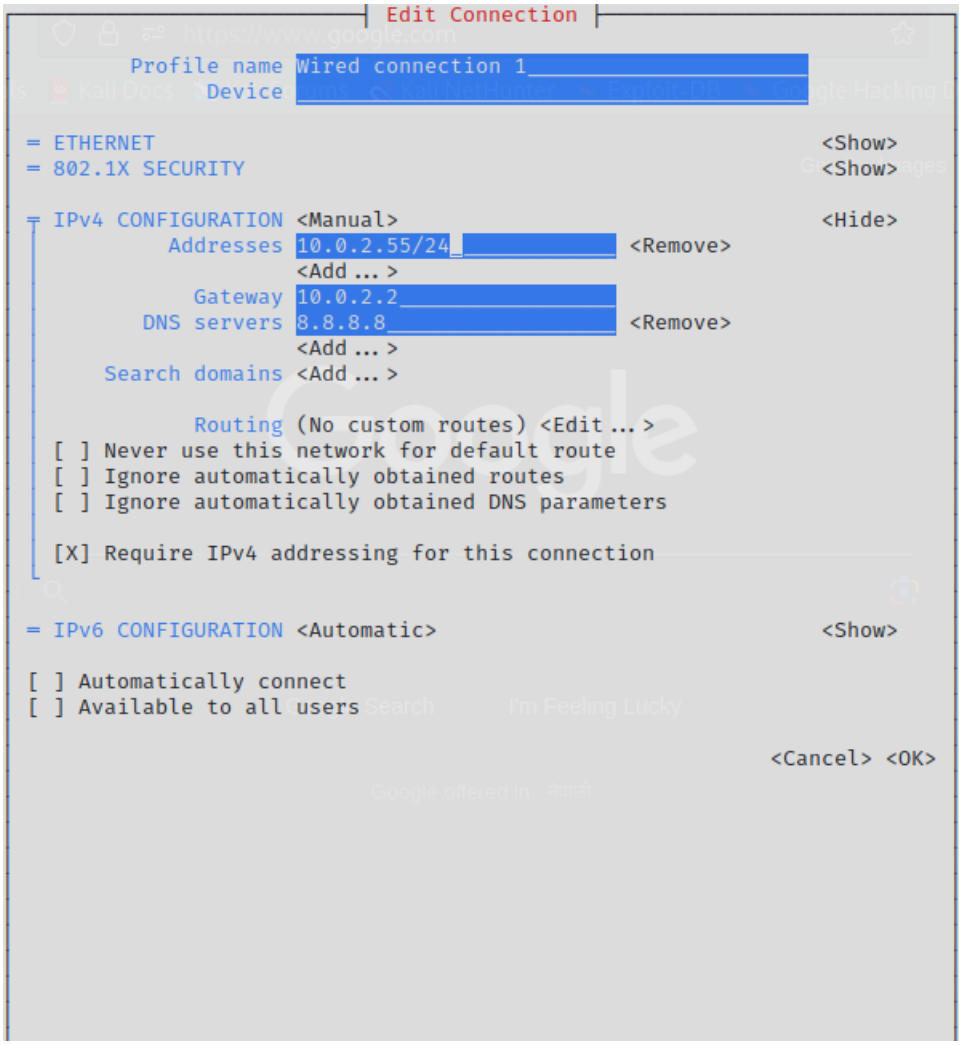
To edit a connection I clicked edit a connection



We were meant to edit wired connection so I clicked onto that



Then I proceeded to enter the suitable ips along with their subnet mask

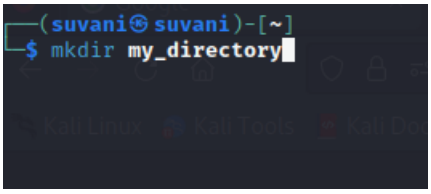


2. Create a script called "backup.sh" that compresses and encrypts a directory named

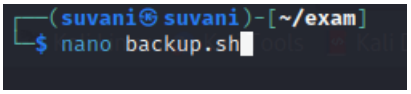
"my_directory" in the home directory, and saves the output in another directory named "backup" also located in the home directory. [15]

Compression – compression is the process of squeezing or smothering the files or directory ina way can have passwords too. These are specifically design inorder to help a secure transmission of files and folders. 'Zip bomb' are also zip files (compressed files that does harm to our system , so installation of antivirus is suggested inorder to prevent from these.on the otherhand the compressed file is decompressed using certain commands.

I made a directory called my_directory



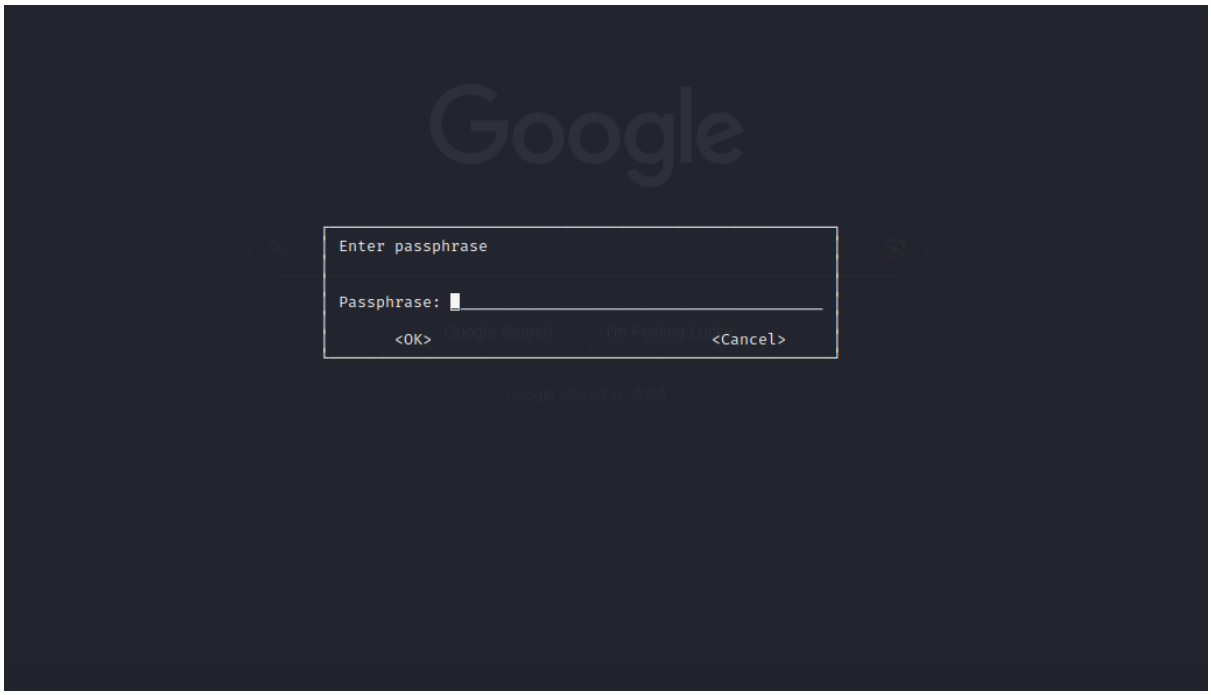
I made the .sh called backup.sh



```
 GNU nano 7.2                                  backup.sh *
#2023-08-07
#!/bin/bash
dir="my_directory"

if [ ! -d /home/suvani/"$dir" ]; then
 echo "the directory doesnt exists"
 exit 1
else
 tar -cvzf "$dir".tar.gz "$dir"
 gpg -output  "$dir".gz.gpg --encrypt "$dir".tar.gz

fi
```




```
drwxr-xr-x 2 root root 4096 Aug  7 10:26 my_directory
-rw-r--r-- 1 root root  119 Aug  7 10:28 my_directory.tar.gz
```

3. Find and delete all files in the /var/log directory that are more than 30 days old. [10]

find is a very powerful command which is used to search for certain directory and files.

Find – command name that helps to search

-type = used inorder to dictate the type fo file of folder

F = because in this case we are searching for files

-mtime = helps to specify time in term of days

30 means we are searching files more than 30 days old

-exec = to execute the command that we are writing afterwards

rm -rf = deletion process

```
┌──(root㉿suvani)-[/home/suvani]
└─# sudo find /var/log/ -type f -mtime 30 -exec rm -rf {} \;

┌──(root㉿suvani)-[/home/suvani]
└─# date
Mon  7 Aug 10:22:22 BST 2023
```

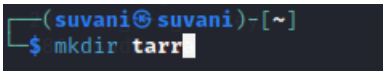
Hemce, all the files which were more than 30 days old was deleted successfully using the following command.

4. Use the tar command to create a compressed archive of a directory named "my_data"

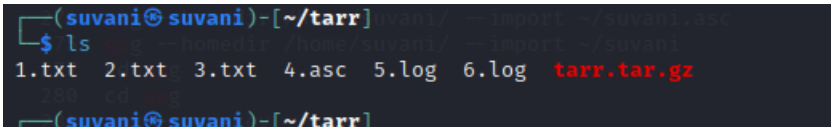
located in the home directory and exclude all files with the ".log" extension. [15]

: tar command is used for compression. The full form of tar command is tape archieve. Tar command helps to bind or smother all the files into a single file which could help us save space of our device or even protect our files.

Here I have made a directory called tar



Then I added some files using various extensions so log extension so each of them are unique,



Then I procceded to use this command which would search all the files in th etarr directory using find and once they search it would look at the extension and skip the log extension as we have done there -not -name “*log” using this wildcard mask.

Now we can see a particular tar file has been created over there using this command

```
┌──(suvani㉿suvani)-[~]
└─$ find /home/suvani/tarr -type f -not -name "*log" -exec tar -cvzf EXAM.tar.gz {} \;
tar: Removing leading `/' from member names
/home/suvani/tarr/3.txt
tar: Removing leading `/' from member names
/home/suvani/tarr/4.asc
tar: Removing leading `/' from member names
/home/suvani/tarr/1.txt
tar: Removing leading `/' from member names
/home/suvani/tarr/2.txt
tar: Removing leading `/' from member names
/home/suvani/tarr/tarr.tar.gz
tar: Removing leading `/' from hard link targets
┌──(suvani㉿suvani)-[~]
└─$ tar -xvzf EXAM.tar.gz
home/suvani/tarr/tarr.tar.gz
┌──(suvani㉿suvani)-[~]
└─$ date
Mon  7 Aug 10:48:38 BST 2023
┌──(suvani㉿suvani)-[~]
```

```
┌──(suvani㉿suvani)-[~/tarr]
└─$ find /home/suvani/tarr -type f -not -name "*log"
/home/suvani/tarr/3.txt
/home/suvani/tarr/4.asc
/home/suvani/tarr/1.txt
/home/suvani/tarr/2.txt
/home/suvani/tarr/tarr.tar.gz
```

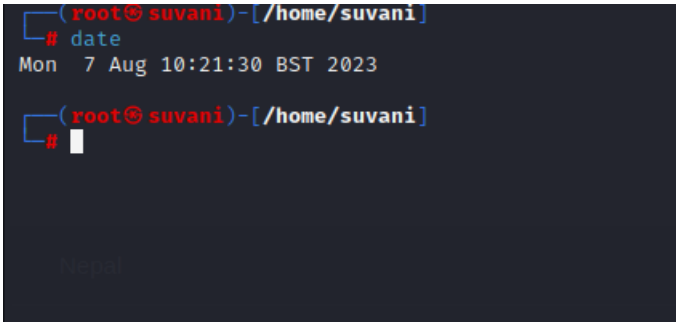
```
-rw-r--r-- 1 suvani suvani      149 Aug  7 10:48  EXAM.tar.gz
```

Hence, the zip file was created.

5. Configure a firewall to allow incoming SSH connections only from a specific IP address

range (e.g., 192.168.1.0/24) and block all other incoming traffic. [10]

Iptables are inbuilt adminstrative tool in linux that not only helps by working as a firewall but it can also be used for NAT purposes . This will help to set up firewall rules on basis of ACCEPT, REJECT, DROP for incoming and outgoing traffic. The main purpose of this firewall is to become a barrier between outside the network and inside of the network in order to verify the traffic. This serves as a essential security purpose .

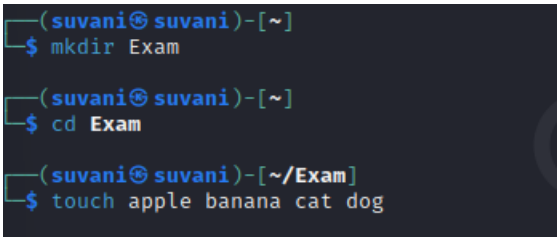


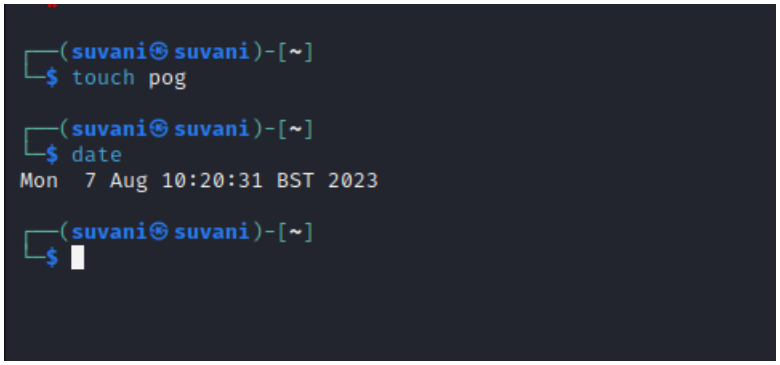
This command shows that the ssh traffic is being accepted from a particular ip range 192.168.1.0/24.

6. Use the "grep" command to search for a specific pattern across multiple files in a directory and output the results to a new file. [10]

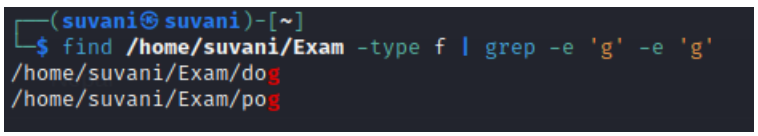
grep is a command line utility that searches for PATTERNS in each file and those patterns could be anything ranging from patterns like the patterns separated by newline characters grep prints each line that matches a pattern. Typically the patterns should be quoted when grep is used.It is a very essential command to search for a particular pattern among a number of patterns

Here we made directory named exam, then we created multiple files over there





Then we procceded to search for similar pattern but under multiple files which are under the same directory. -type f hints we are searching for a file where as -e option is used inorder to search for multiple patterns in grep.



7. Create a cron job that runs a script named "cleanup.sh" every day at 2 AM. The script

should delete all files in the /tmp directory that are more than 24 hours old. [10]

```
 GNU nano 7.2                                  cleanup.sh
#!/bin/bash

cd /tmp
find . -type f -mtime +1 -not -ntime +7 -exec rm {} \;
```

Checking the reliability of command

```
┌──(suvani㉿suvani)-[~]
└─$ nano Cleanup.sh

┌──(suvani㉿suvani)-[~]
└─$ chmod +777 Cleanup.sh

┌──(suvani㉿suvani)-[~]
└─$ ./Cleanup.sh
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-apache2.service-VBrKh3': Permission denied
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-colord.service-TJimyK': Permission denied
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-haveged.service-wvh0Sl': Permission denied
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-upower.service-Imx7ci': Permission denied
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-systemd-logind.service-TCWjiV': Permission denied
find: '/tmp/systemd-private-8bf81ebb52094a40a247114bdf89fd62-ModemManager.service-7VWXxR': Permission denied
```

```
# m h  dom mon dow   command
54 07 12 03 * echo "hello iam the file" > /home/suvani/cronmade
15 03 20 03 * echo " This is a file" > /home/suvani/cronmade.txt
03 20  *  * 1-5 echo "helloww" > /home/suvani/suv.txt
12 20 * * 0-5 echo "helloww" > /home/suvani/surafi.txt
00 2  * * * > /home/suvani/cleanup.sh
 #date 2023-08-07
```

Cronjob is a command utility in linux to automate tasks. The main purpose of this command is to automate task so we don't have to be prepared at the very second we need the file or the task to be done !

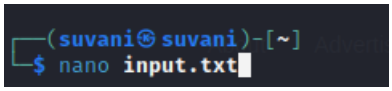
8. Take standard input from a file named "input.txt" and output the result to a file named

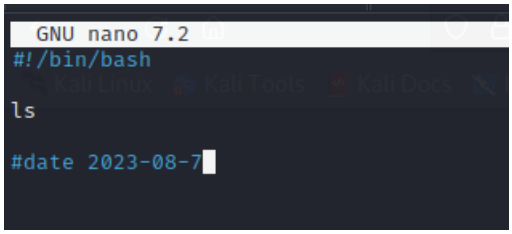
"output.txt" using the command line. [10]

Stdin :

Standard input command is used to communicate with the users. Think of it like we are interacting with computer by the help of keyboard. It helps to take the responses and make decisions. The file descriptor of stdin is 0, where as standard output helps to display messages or response after an interaction. The file descriptor of stdout is 0 and stderr is 2. Stderr is used to display error especially.

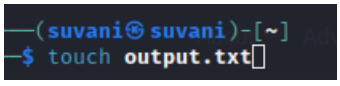
I made a file named input.txt

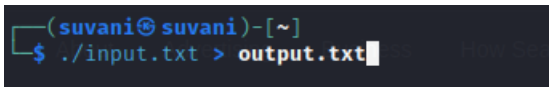




I wrote a command that would display the files using ls and it will be taken as an inout and whil ethe answers are displayed we will display it into a certain file called output.txt

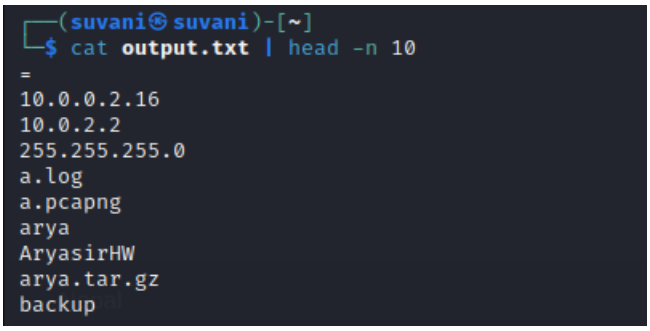
.





'>Is used for redirection purpose'

And as we can see th eoutput is redirected.



9. Use the find command to find the flags within your system and redirect the standard output to a specific file and error to another and verify it. [10]

find – command inorder to serahc for a particular file.

F = as we are searching for a file

-name = inorder to find the file via it's particular name

Here in this case we are asked to search for file that has flags, so we used a wildcard for flags that is "*flags*" this would list all the files with flags words on them .

In this case I directed the std error on err.txt . standard output has a file descriptor of 0.

Here I used the same command with root privilages as in the error we saw that the permission was denied so I procceded with the root privilege and then sucefully I gathered the output in find.txt file

```
┌──(root㉿suvani)-[/home/suvani]
└─#   find / -type f -name "*flag*"\n > find.txt


┌──(root㉿suvani)-[/home/suvani]
└─# cat find.txt
/usr/lib/x86_64-linux-gnu/perl5/5.36/Tk/demos/images/flagdown
/usr/share/rubygems-integration/all/gems/mime-types-data-3.2022.0105/data/mime.flags.column
/usr/share/ruby-mime-types-data/data/mime.flags.column
/usr/include/X11/bitmaps/flagdown

┌──(root㉿suvani)-[/home/suvani]
└─#
```

```
┌──(root㉿suvani)-[/home/suvani]
└─# date
Mon  7 Aug 10:19:35 BST 2023

┌──(root㉿suvani)-[/home/suvani]
```