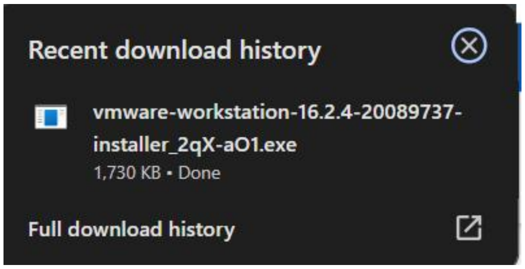
ITS60904

COMPUTER CRIME AND DIGITAL EVIDENCE

PRACTICAL 1 LAB REPORT

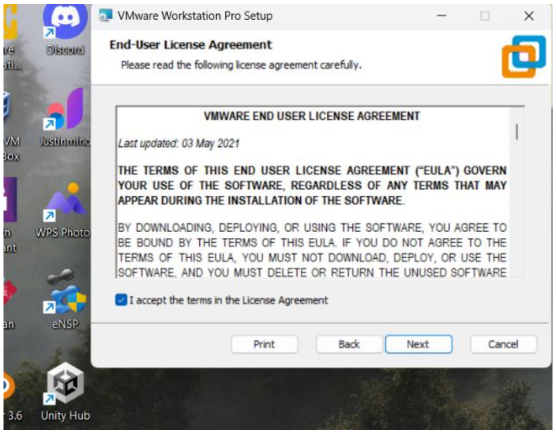
1. Building your forensics Workstation

a. Download and install VMware Workstation Pro on my computer.



Recent download history

vmware-workstation-16.2.4-20089737-installer_2qX-aO1.exe
1,730 KB • Done



VMware Workstation Pro Setup

End-User License Agreement

Please read the following license agreement carefully.

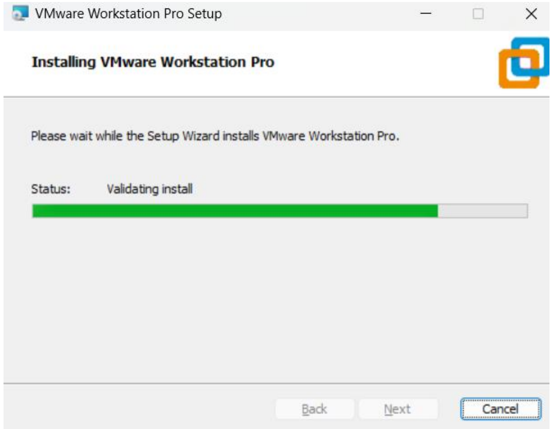
VMWARE END USER LICENSE AGREEMENT

Last updated: 03 May 2021

THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA") GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

BY DOWNLOADING, DEPLOYING, OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, DEPLOY, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE

☑ I accept the terms in the License Agreement

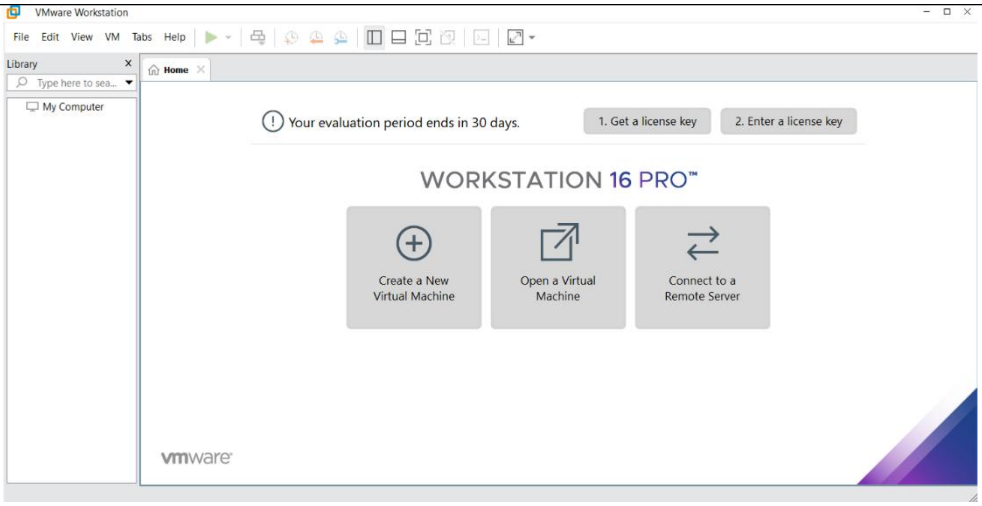


VMware Workstation Pro Setup

Installing VMware Workstation Pro

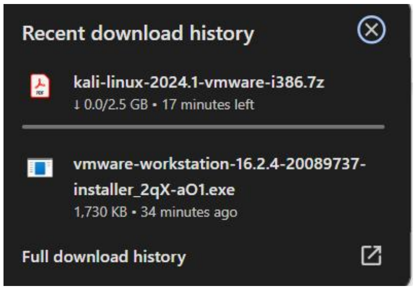
Please wait while the Setup Wizard installs VMware Workstation Pro.

Status: Validating install



- Here's how the VMware Workstation home screen will appear.

b. Download Kali Linux (Kali Linux 64 bit Vmware Preinstalled Image)



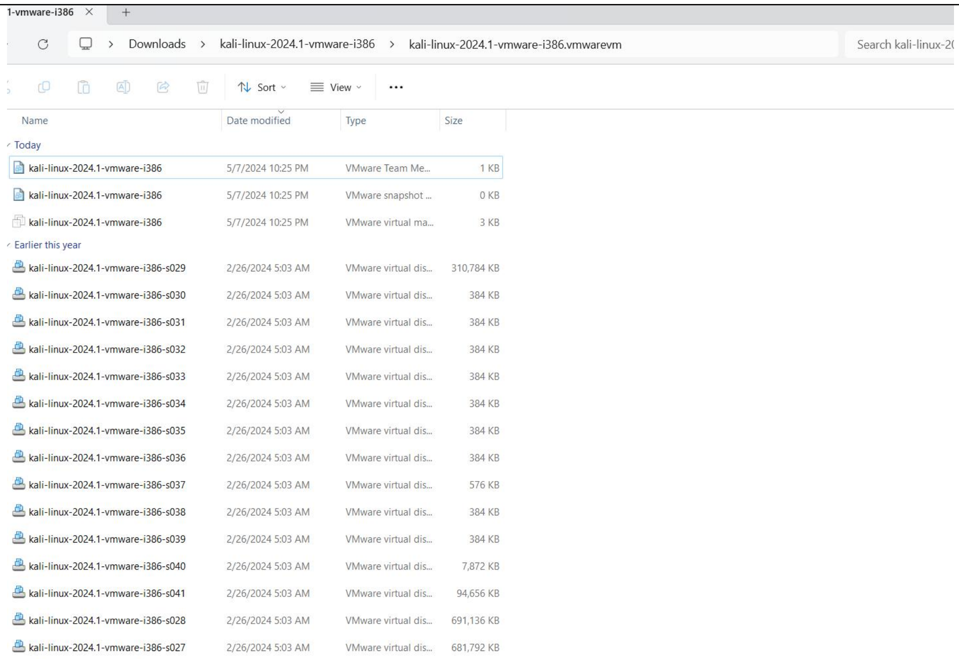
Recent download history

kali-linux-2024.1-vmware-i386.7z
↓ 0.0/2.5 GB • 17 minutes left

vmware-workstation-16.2.4-20089737-installer_2qX-aO1.exe
1,730 KB • 34 minutes ago

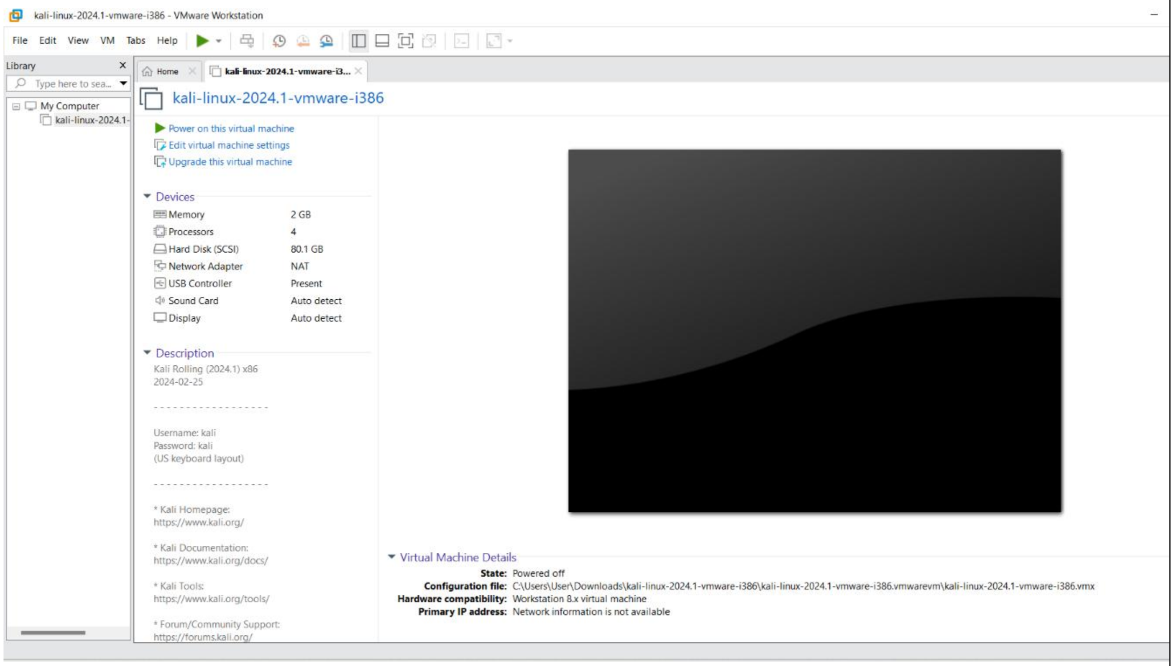
Full download history

- In this case, the downloaded item was a PDF even though I was anticipating a zipped file. As a result, I was able to obtain the picture that is shown below by extracting the text of the PDF file. I then moved the VMware virtual machine 3KB file into the VMware Workstation.


1-vmware-i386
Downloads > kali-linux-2024.1-vmware-i386 > kali-linux-2024.1-vmware-i386.vmwarevm
Search kali-linux-2(
Sort
View

Name	Date modified	Type	Size
Today			
kali-linux-2024.1-vmware-i386	5/7/2024 10:25 PM	VMware Team Me...	1 KB
kali-linux-2024.1-vmware-i386	5/7/2024 10:25 PM	VMware snapshot ...	0 KB
kali-linux-2024.1-vmware-i386	5/7/2024 10:25 PM	VMware virtual ma...	3 KB
Earlier this year			
kali-linux-2024.1-vmware-i386-s029	2/26/2024 5:03 AM	VMware virtual dis...	310,784 KB
kali-linux-2024.1-vmware-i386-s030	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s031	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s032	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s033	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s034	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s035	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s036	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s037	2/26/2024 5:03 AM	VMware virtual dis...	576 KB
kali-linux-2024.1-vmware-i386-s038	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s039	2/26/2024 5:03 AM	VMware virtual dis...	384 KB
kali-linux-2024.1-vmware-i386-s040	2/26/2024 5:03 AM	VMware virtual dis...	7,872 KB
kali-linux-2024.1-vmware-i386-s041	2/26/2024 5:03 AM	VMware virtual dis...	94,656 KB
kali-linux-2024.1-vmware-i386-s028	2/26/2024 5:03 AM	VMware virtual dis...	691,136 KB
kali-linux-2024.1-vmware-i386-s027	2/26/2024 5:03 AM	VMware virtual dis...	681,792 KB

c. Click "Open." After the import process is completed, user will see the newly imported Kali Linux virtual machine listed among the available virtual machines on the left side of VMware Workstation, as shown below.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
kali-linux-2024.1-vmware-i386
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

Kali Rolling (2024.1) x86
2024-02-25

Username: kali
Password: kali
(US keyboard layout)

----

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

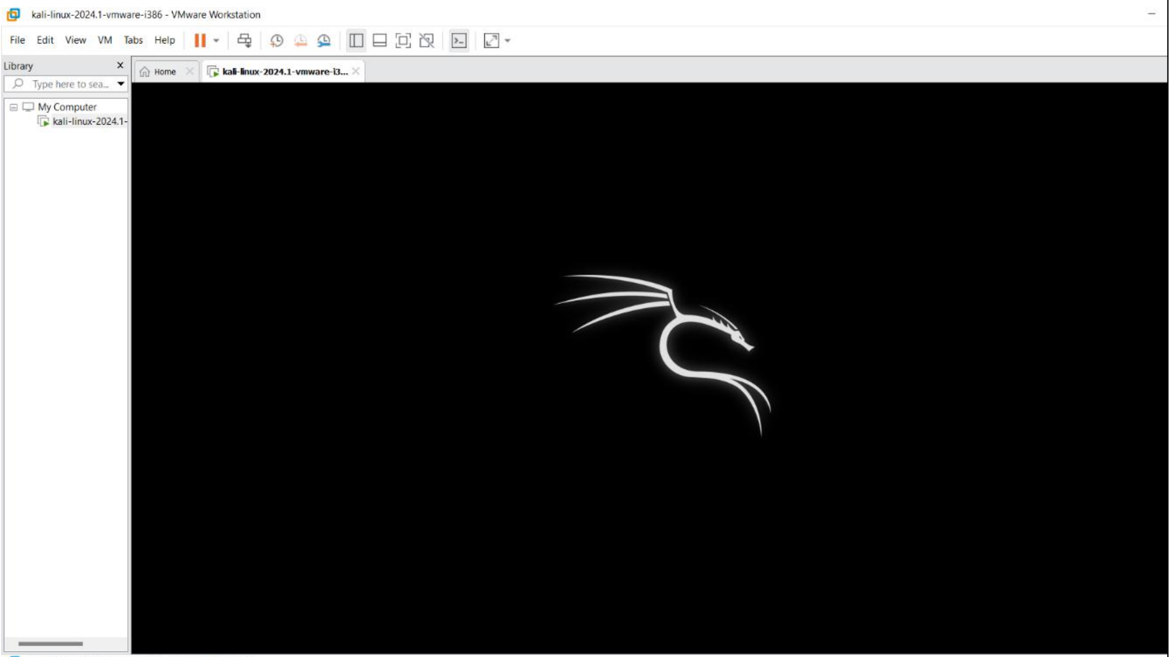
* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

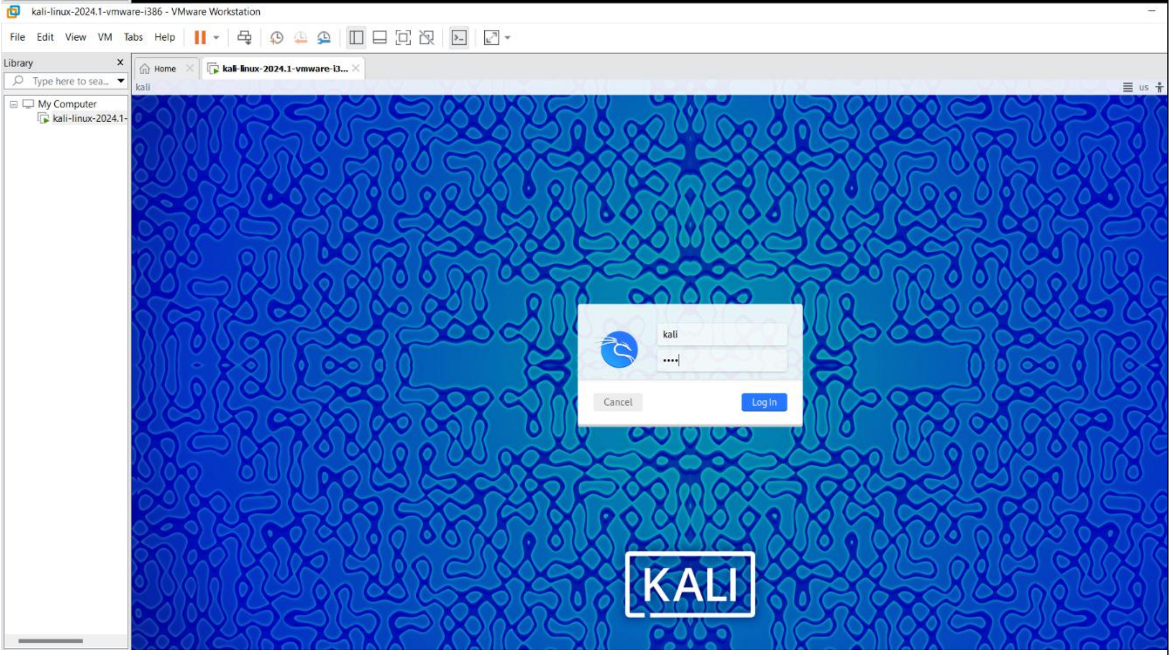
Virtual Machine Details

State: Powered off
Configuration file: C:\Users\User\Downloads\kali-linux-2024.1-vmware-i386\kali-linux-2024.1-vmware-i386.vmwarevm\kali-linux-2024.1-vmware-i386.vmx
Hardware compatibility: Workstation 8.x virtual machine
Primary IP address: Network information is not available

d. **<u>Here is how user can check the version of TSK installed on Kali Linux and Vmware-tools.</u>**

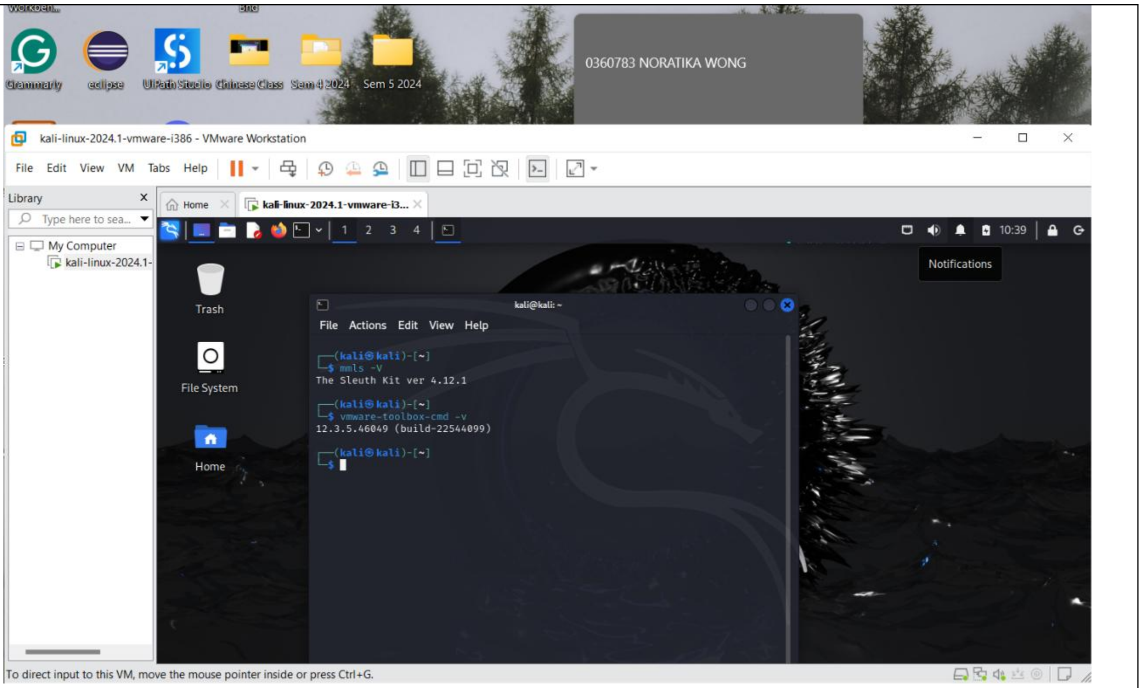


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...



kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
kali
us
kali
Cancel
Log In
KALI

- User will need to power on the Kali-Linux first and the put in the username and password which is 'kali'.


Grammarly
eclipse
UiPath Studio
Chinese Class
Sem 4 2024
Sem 5 2024
0360783 NORATIKA WONG
kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
10:39
Notifications
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(kali㉿kali)-[~]
└─$ mmls -V
The Sleuth Kit ver 4.12.1

┌──(kali㉿kali)-[~]
└─$ vmware-toolbox-cmd -v
12.3.5.46049 (build-22544099)

┌──(kali㉿kali)-[~]
└─$ 
```

- ‘mmls -V’ This command is being used to check the version of TSK (The Sleuth Kit) installed on the system while ‘vmware-toolbox-cmd -v’ This command is used to check the version of VMware Tools installed on the system. Above is shown both the version of TSK that already being installed in system and VMware Tools.

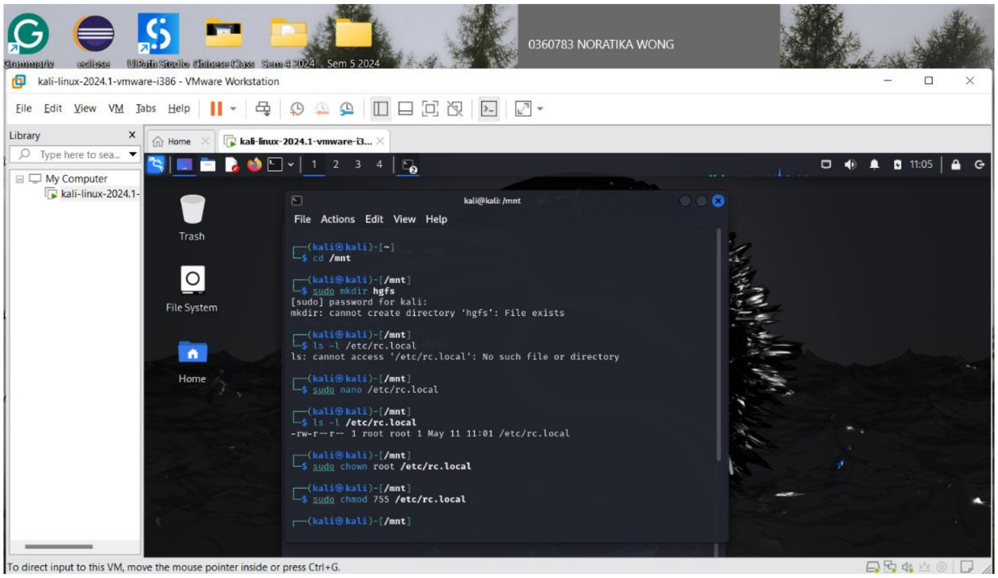
2. Creating a shared folder

a. <u>Create the missing folder in the system</u>

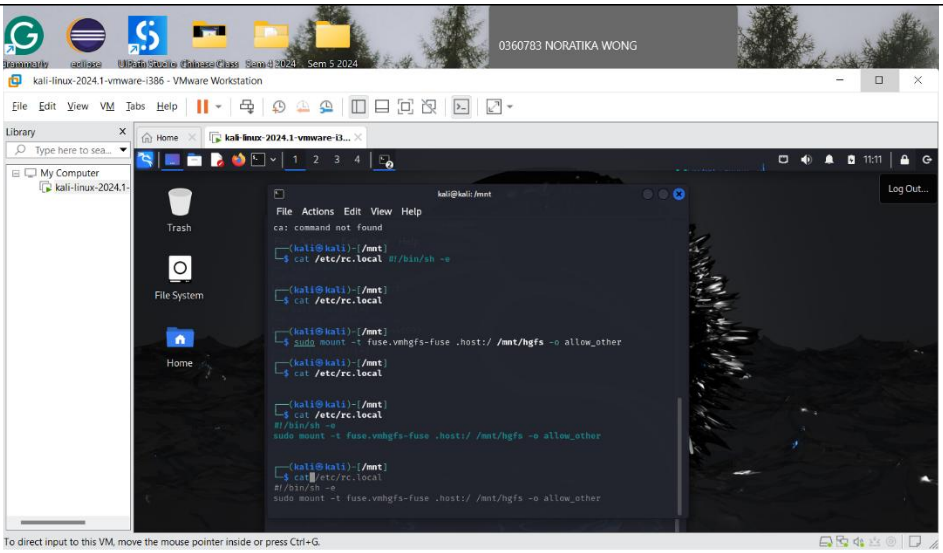
- The command ‘cd /mnt’ modifies the current directory to ‘/mnt’, which is commonly utilised as a mount point for external file systems or devices.
- ‘sudo mkdir hgfs’ In this case, the mkdir command is run with administrator rights using sudo. The command ‘mkdir’ denotes "make directory," and the directory that is being created inside of ‘/mnt’ is called ‘hgfs’.
- Use the following command to create or change the /etc/rc.local file ‘sudo nano /etc/rc.local’. This command opens the /etc/rc.local file and launches the Nano text editor with administrator rights, if it doesn't already exist. In here there will be screen pop which user need to press together ‘Ctrl + X’ and after that ‘Enter’ to exist from the screen and back to the terminal screen.

- ‘ls -l /etc/rc.local’ This command displays comprehensive details on the ownership and permissions of the /etc/rc.local file.
- ‘sudo chown root /etc/rc.local’ This changes the owner of the file to root.
- ‘sudo chmod 755 /etc/rc.local’ This changes the file permissions to 755, which means it becomes executable by the owner (root) and readable and executable by others.
- ‘cat #!/bin/sh -e’ This line specifies the shell to be used for executing the script (/bin/sh) and -e ensures that the script exits immediately if any command fails.

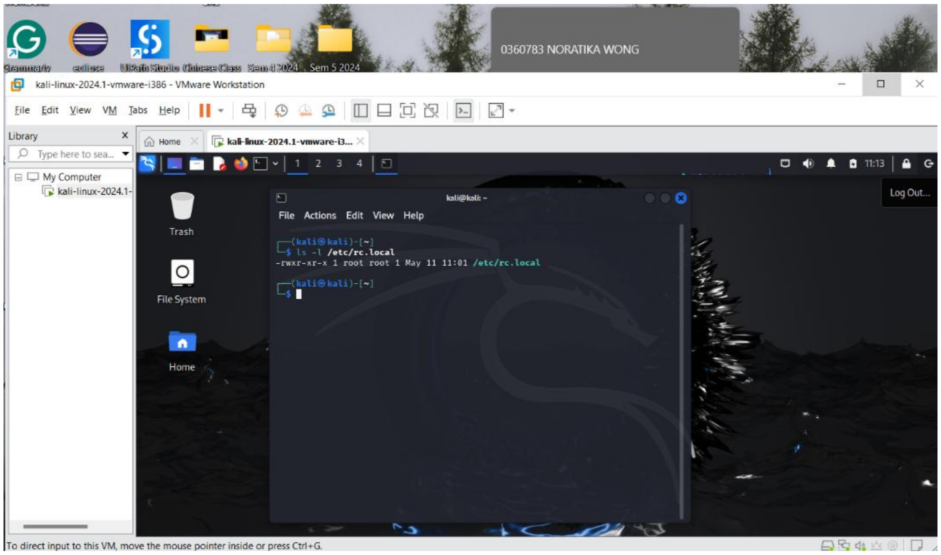
  ‘sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other’ This mounts the VMware shared folder to /mnt/hgfs using the fuse.vmhgfs-fuse file system type, allowing other users to access it. For this command user need to type cat first and press space until the below line to type in the ‘#!/bin/sh -e’ another space to next line and type in ‘sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other’


0360783 NORATIKA WONG
kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
kali@kali: /mnt
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(kali㉿kali)-[~]
└─$ cd /mnt

┌──(kali㉿kali)-[/mnt]
└─$ sudo mkdir hgfs
[sudo] password for kali:
mkdir: cannot create directory ‘hgfs’: File exists

┌──(kali㉿kali)-[/mnt]
└─$ ls -l /etc/rc.local
ls: cannot access '/etc/rc.local': No such file or directory

┌──(kali㉿kali)-[/mnt]
└─$ sudo nano /etc/rc.local

┌──(kali㉿kali)-[/mnt]
└─$ ls -l /etc/rc.local
-rw-r--r-- 1 root root 1 May 11 11:01 /etc/rc.local

┌──(kali㉿kali)-[/mnt]
└─$ sudo chown root /etc/rc.local

┌──(kali㉿kali)-[/mnt]
└─$ sudo chmod 755 /etc/rc.local

┌──(kali㉿kali)-[/mnt]
```


0360783 NORATIKA WONG
kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
Log Out...
kali@kali: /mnt
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

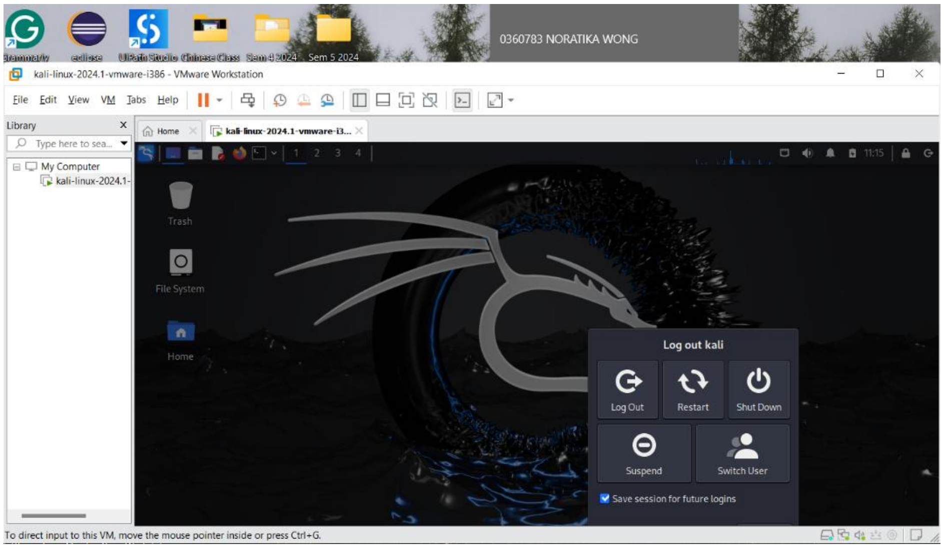
```
ca: command not found

┌──(kali㉿kali)-[/mnt]
└─$ cat /etc/rc.local #!/bin/sh -e


┌──(kali㉿kali)-[/mnt]
└─$ cat /etc/rc.local


┌──(kali㉿kali)-[/mnt]
└─$ sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other

┌──(kali㉿kali)-[/mnt]
└─$ cat /etc/rc.local


┌──(kali㉿kali)-[/mnt]
└─$ cat /etc/rc.local
#!/bin/sh -e
sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other


┌──(kali㉿kali)-[/mnt]
└─$ cat /etc/rc.local
#!/bin/sh -e
sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other
```


0360783 NORATIKA WONG
kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
Log Out...
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(kali㉿kali)-[~]
└─$ ls -l /etc/rc.local
-rwxr-xr-x 1 root root 1 May 11 11:01 /etc/rc.local

┌──(kali㉿kali)-[~]
└─$ 
```

- Now to check user can key in the command `ls -l /etc/rc.local` which provides information about the `/etc/rc.local` file. The output will be `-rwxr-xr-x.` indicates the file's permissions. Each letter or symbol represents permissions for different user groups. In this case, the first `-` indicates it's a regular file. The next set of characters (`rwx`) indicates that the owner has read, write, and execute permissions, while the next group (`r-x`) indicates that the group and others have read and execute permissions, but not write permissions.

  The final `.` indicates that there are no additional permissions or special modes set. Overall, this means that now the file is readable and executable by all users, and writable only by the owner.



kali-linux-2024.1-vmware-i386 - VMware Workstation

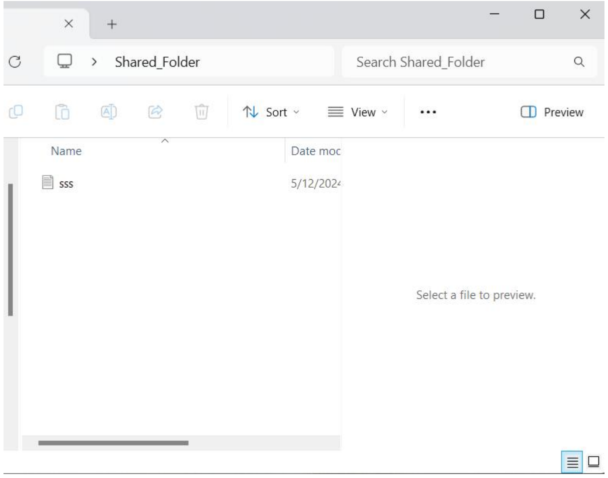
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

☑ Save session for future logins

- The machine must be powered off before continue with the next step which is to enable shared file.

b. <u>Shared file between the laptop and Kali Linux through VMware Workstation</u>

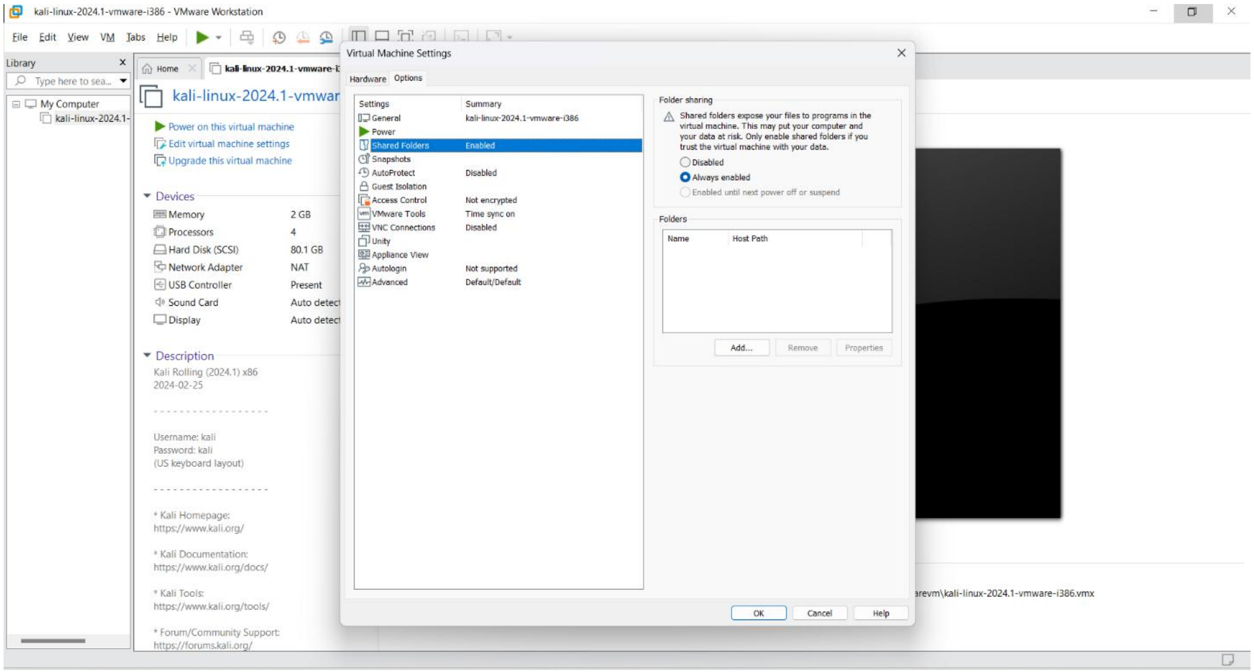
- In the initial step of file sharing, users must first create a directory on their laptop and place a text file inside.



Name	Date moc
sss	5/12/2024

Select a file to preview.

- After successfully creating the file, users should open VMware Workstation and navigate to the Kali Linux virtual machine. From there, they can click on 'Edit virtual machine settings,' then access 'Options' to enable folder sharing and add the previously created file. Users must ensure to enable the attribute part.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i386
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Description
Virtual Machine Settings
Hardware Options
Add... Remove Properties
OK Cancel Help

Devices	
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Kali Rolling (2024.1) x86
2024-02-25

Username: kali
Password: kali
(US keyboard layout)

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

Settings	Summary
General	kali-linux-2024.1-vmware-i386
Power	
Shared Folders	Enabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync on
VNC Connections	Disabled
Unity	
Appliance View	
Autologin	Not supported
Advanced	Default/Default

Folder sharing

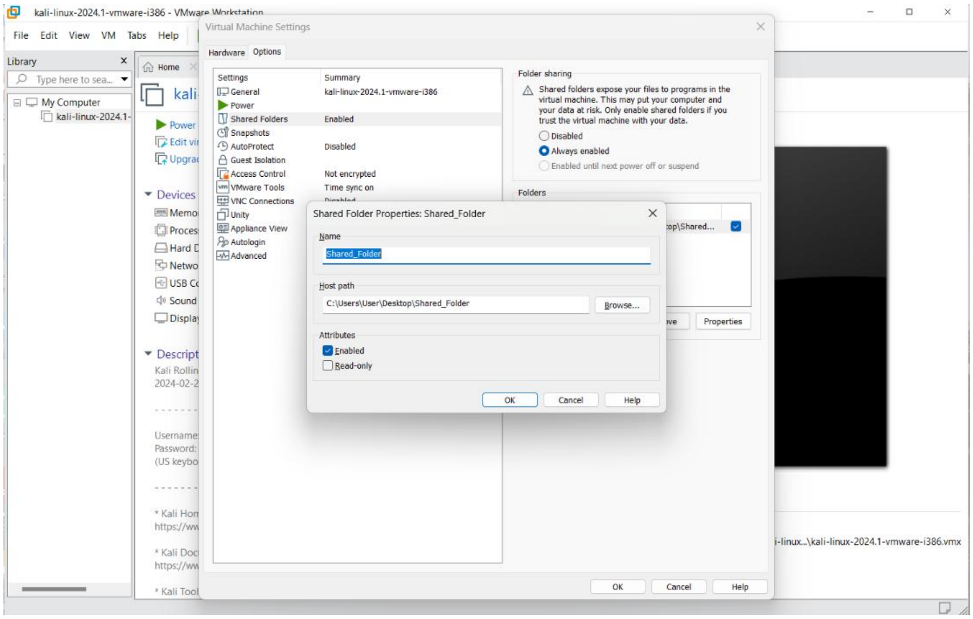
Shared folders expose your files to programs in the virtual machine. This may put your computer and your data at risk. Only enable shared folders if you trust the virtual machine with your data.

○ Disabled
● Always enabled
○ Enabled until next power off or suspend

Folders

Name	Host Path

...arevm\kali-linux-2024.1-vmware-i386.vmx



Shared Folder Properties: Shared_Folder

Name: Shared_Folder

Host path: C:\Users\User\Desktop\Shared_Folder

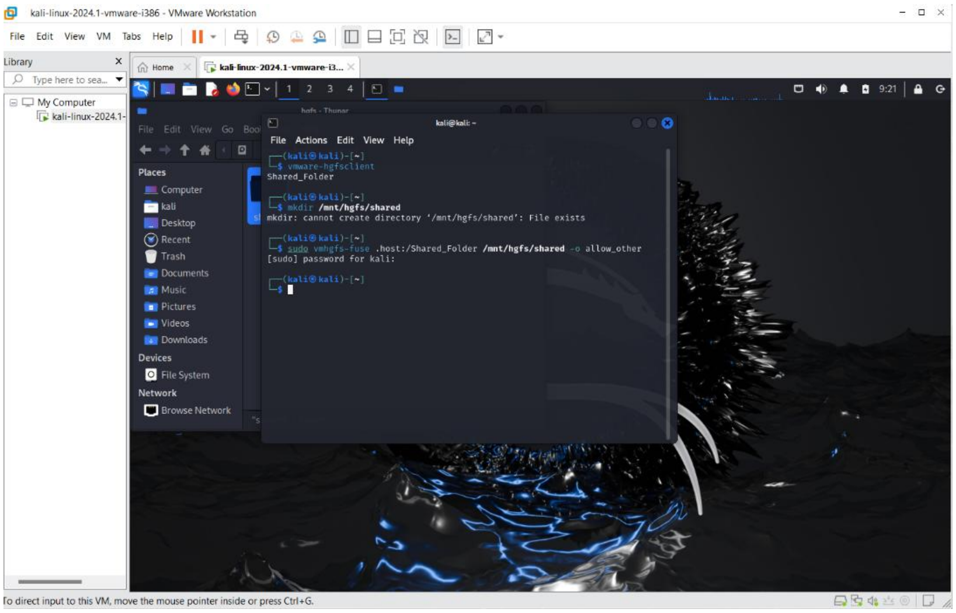
Attributes
☑ Enabled
☐ Read-only

Folder sharing
○ Disabled
● Always enabled
○ Enabled until next power off or suspend

...op\Shared... ☑

...i-linux...\kali-linux-2024.1-vmware-i386.vmx

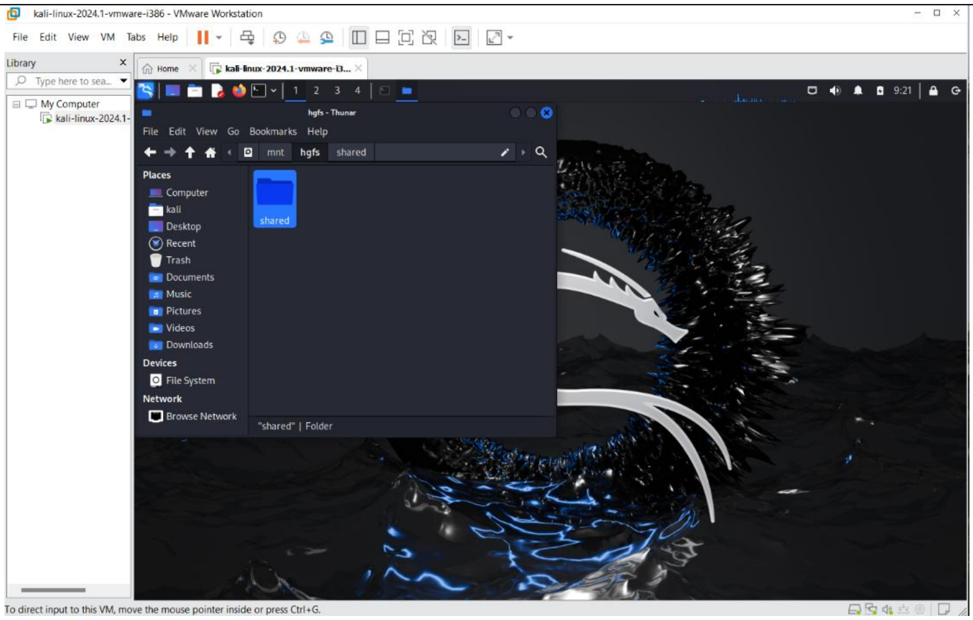
- After successfully adding the file path, the user should power on the virtual machine and log back into Kali Linux. Then, they can access the terminal, located at the top of the home screen.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
hgfs - Thunar
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@kali: ~
File Actions Edit View Help
9:21
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

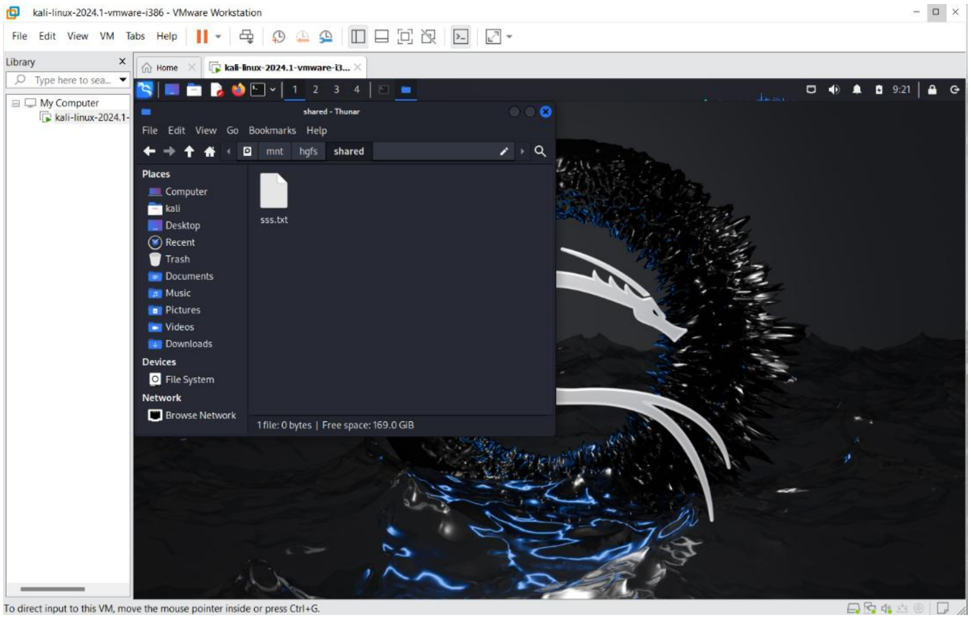
```
┌──(kali㉿kali)-[~]
└─$ vmware-hgfsclient
Shared_Folder

┌──(kali㉿kali)-[~]
└─$ mkdir /mnt/hgfs/shared
mkdir: cannot create directory '/mnt/hgfs/shared': File exists

┌──(kali㉿kali)-[~]
└─$ sudo vmhgfs-fuse .host:/Shared_Folder /mnt/hgfs/shared -o allow_other
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ 
```

- The first command is used to find out the available shared folders from the VMware host. The second creates a directory named "shared" in the /mnt/hgfs directory. This directory will be used as a mount point for accessing the shared folders from the VMware host. The command `sudo vmhgs-fuse .host:/ file name /mnt/hgfs/shared -o allow_other` does the following: It mounts a shared folder from a VMware host onto your local file system.

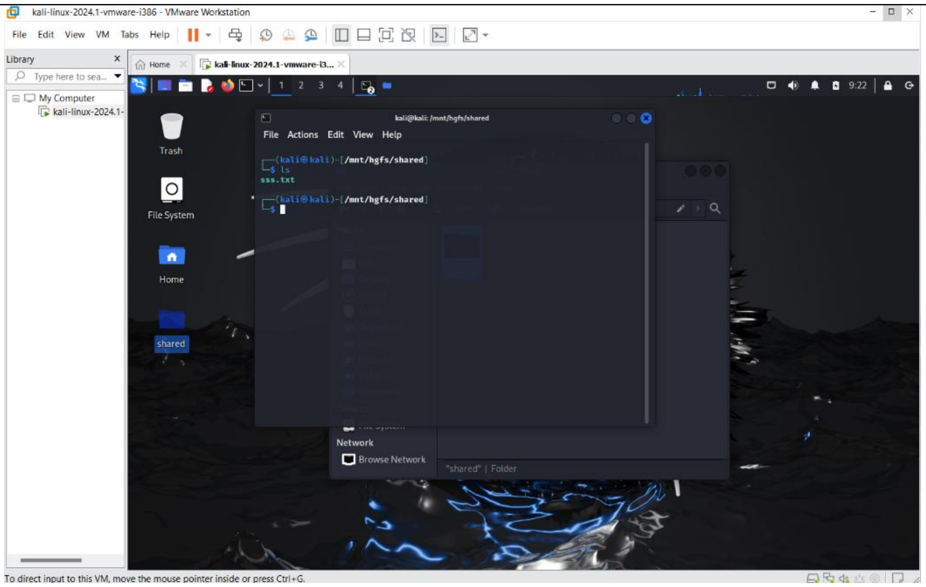
  The `sudo` command ensures the execution with administrative privileges. `vmhgs-fuse` is the command used for mounting VMware shared folders. `.host:/` specifies the VMware host and the root directory of shared folders. `file name` is where you specify the name of the shared folder you want to mount. `/mnt/hgfs/shared` is the directory created earlier, serving as the mount point for accessing the shared folder. Finally, `-o allow_other` allows other users to access the mounted shared folder, enabling broader accessibility beyond the user who mounted it.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
hgfs - Thunar
File Edit View Go Bookmarks Help
mnt hgfs shared
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
shared
"shared" | Folder
9:21
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- The file that was created can be find by navigating to "Devices" > "File System," then opening the "mnt" directory and selecting "hgfs." Within this directory, it can be discover the file mentioned in the previous explanation.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
shared - Thunar
File Edit View Go Bookmarks Help
mnt hgfs shared
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
sss.txt
1 file: 0 bytes | Free space: 169.0 GiB
9:21
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- The shared file between this system and the computer has been successfully shared. The text file that was created within the Kali Linux file system can be located.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
1 2 3 4
9:22
Trash
File System
Home
shared
kali@kali: /mnt/hgfs/shared
File Actions Edit View Help
Network
Browse Network
"shared" | Folder
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(kali㉿kali)-[/mnt/hgfs/shared]
└─$ ls
sss.txt

┌──(kali㉿kali)-[/mnt/hgfs/shared]
└─$ 
```

- To confirm the existence of the file, you can open the terminal in the file directory by right-clicking and then input the `ls` command. This command will list all files and directories present in the current directory, ensuring the file's presence.