Enhancing Digital Government and Economy
Cyber Security Course
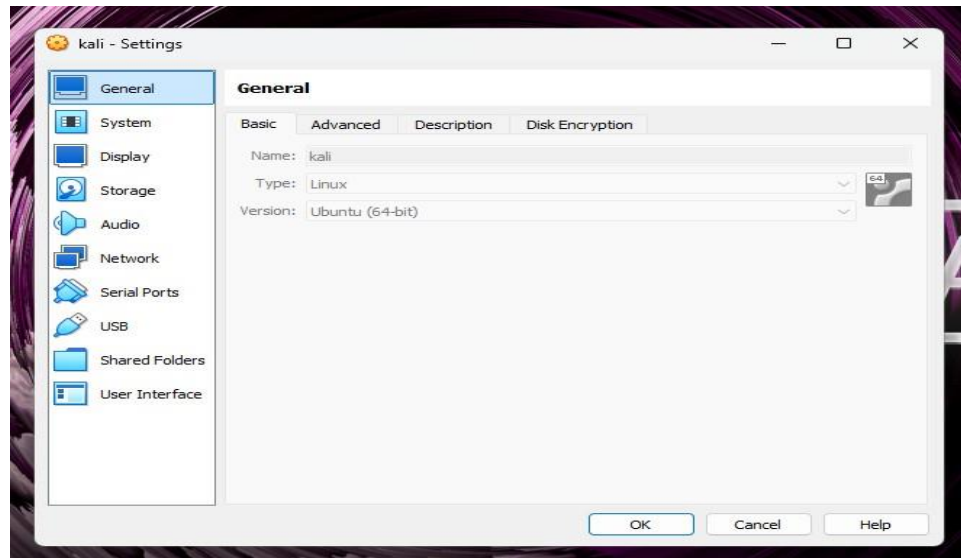## Classwork-05

Submitted by,
Name: Koushiki Devi Agarwalla
Batch: JUR2B11
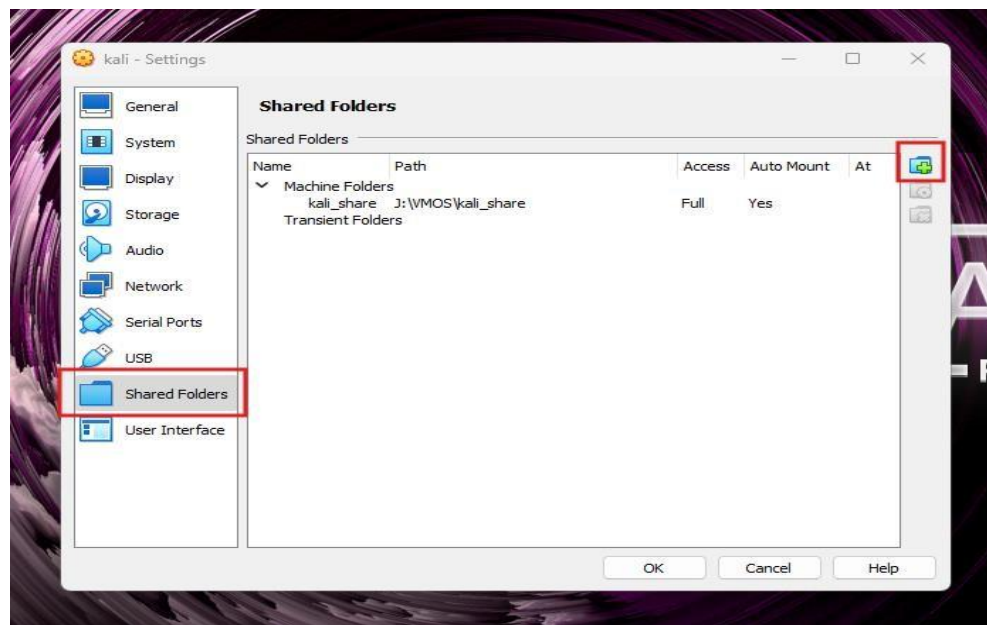ID: 2111271

Create a folder in any drive to your windows machine.
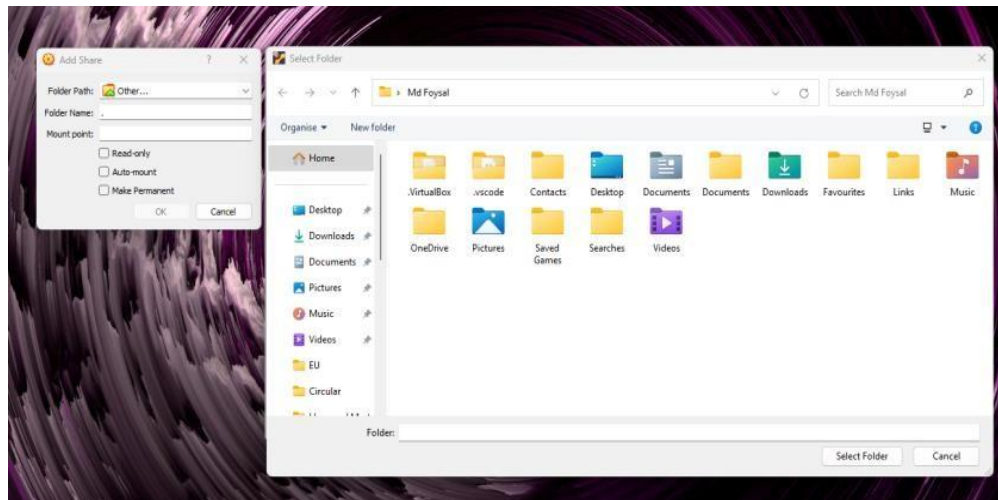Step 01: Start Kali machine.
Step 02: Machine→Settings

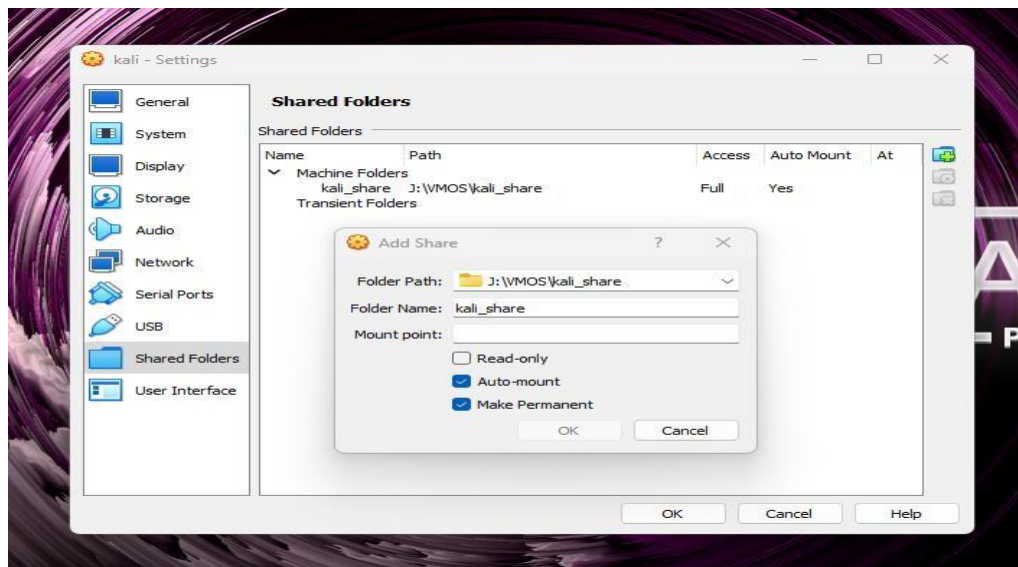Step 03: Go to Network. Change attached to 'NAT'. Then go toShared Folders and click the add icon.

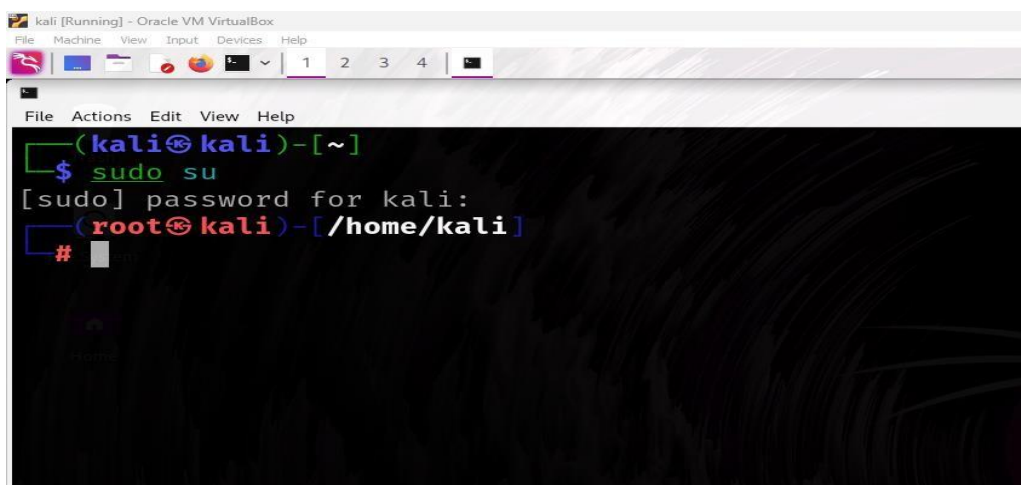Step 04: Choose Folder path to Other and choose windows machine folder that created for share.
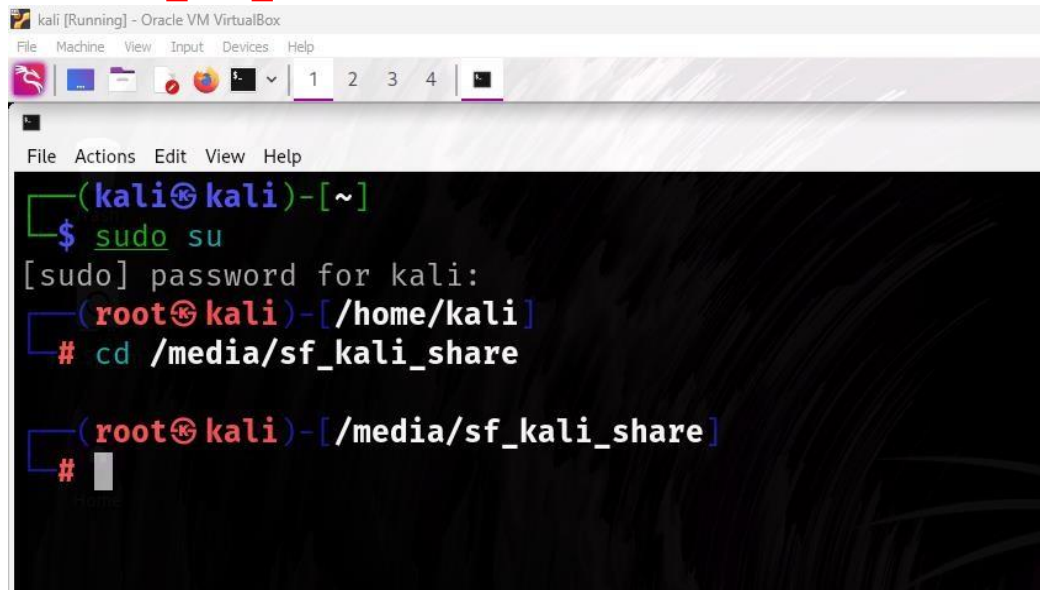

→Check Auto-mount
→Check Make Permanent and click ok.

Step 04: To check folder shared or not, Open terminal
Write sudo su or sudo -i command to get super user access.

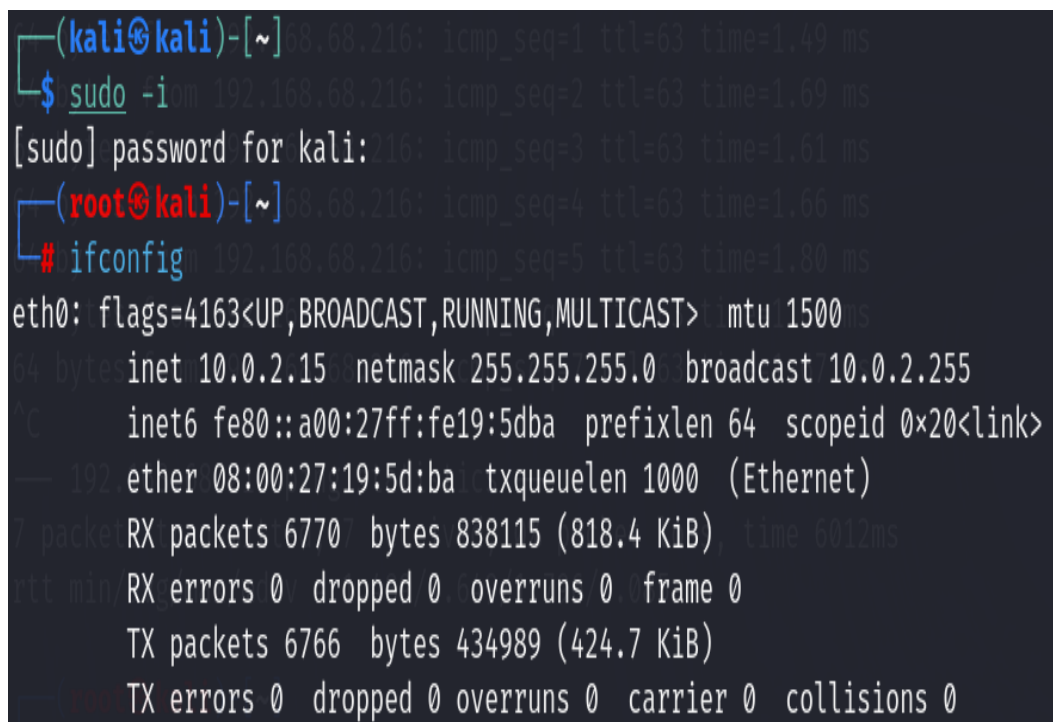Write the following command to get folder# cd /media/sf_kali_share

To find machines own IP address ,the command used is : ifconfig

Commands to find open ports on a target IP:
nmap <target ip>

```
  ┌──(root💀kali)-[~]
  └─# nmap 192.168.68.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:36 EDT
Nmap scan report for 192.168.68.216
Host is up (0.0044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  commplex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

To find service version, command used: nmap -sV <target ip> -p 80

Service Version : STATE SERVICE VERSION

```
  ┌──(root💀kali)-[~]
  └─# nmap -sV 192.168.68.216 -p 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:37 EDT
Nmap scan report for 192.168.68.216
Host is up (0.00050s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod
_ssl/2.2.14 OpenSSL...)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds
```

To find operating system running on the machine, command used: nmap -sV <target ip> -O
Operating System : Linux

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.68.216 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:38 EDT
Nmap scan report for 192.168.68.216
Host is up (0.00091s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6
.5 mod_ssl/2.2.14 OpenSSL ... )
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6
.5 mod_ssl/2.2.14 OpenSSL ... )
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port5001-TCP:V=7.94SVN%I=7%D=10/5%Time=6700ED0F%P=x86_64-pc-linux-gnu%r
SF:(NULL,4,"\xac\xed\0\x05");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.11 seconds
```