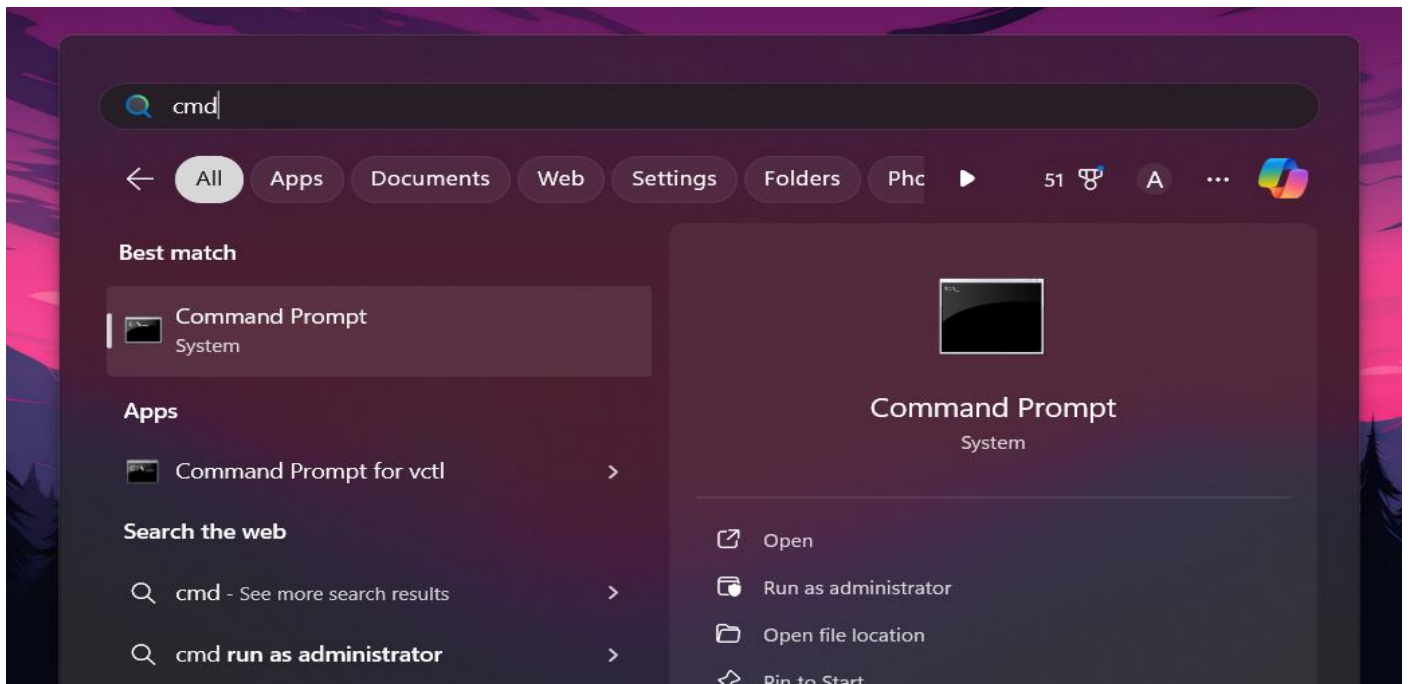# LAP1..bart1

Name: Abdullah Abdulaziz Rabah Alshammari
ID: 202100569

Exercise 1: Open Source Information Gathering Using Windows Command Line Utilities Scenario

1. To launch command prompt, type **cmd** in **Search** field as shown in screenshot, and then click **Command Prompt** from the search result. If a **User Account Control** pop-up appears click **Yes**.

2. Type ping **www.moviescope.com** in the command prompt window, and press **Enter** to find its IP address.

3. In the command prompt window, type **ping www.moviescope.com –f –l 1500** and press **Enter**. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented.

-f switch sets the **Do Not Fragment** bit on the ping packet. By default, the ping packet allows fragmentation.

Since we used the **-f** switch with the ping command, the packet was not sent, and the ping command returned this error.

```
Command Prompt        ×    +   ⌄                                 —   □   ×

C:\Users\aborb>ping www.moviescope.com

Pinging www.moviescope.com [13.56.33.8] with 32 bytes of data:
Reply from 13.56.33.8: bytes=32 time=204ms TTL=51
Reply from 13.56.33.8: bytes=32 time=205ms TTL=51
Reply from 13.56.33.8: bytes=32 time=205ms TTL=51
Reply from 13.56.33.8: bytes=32 time=204ms TTL=51

Ping statistics for 13.56.33.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 204ms, Maximum = 205ms, Average = 204ms

C:\Users\aborb>ping www.moviescope.com -f -l 1500

Pinging www.moviescope.com [13.56.33.8] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 13.56.33.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\aborb>
```

4. Type **ping www.moviescope.com –f –l 1300** and press **Enter.**

In the ping command, the **–l** option means to send the buffer size.

```
C:\Users\aborb>ping www.moviescope.com -f -l 1300

Pinging www.moviescope.com [13.56.33.8] with 1300 bytes of data:
Reply from 13.56.33.8: bytes=1300 time=211ms TTL=51
Reply from 13.56.33.8: bytes=1300 time=205ms TTL=51
Reply from 13.56.33.8: bytes=1300 time=208ms TTL=51
Reply from 13.56.33.8: bytes=1300 time=206ms TTL=51

Ping statistics for 13.56.33.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 205ms, Maximum = 211ms, Average = 207ms

C:\Users\aborb>
```

5. Type **ping www.moviescope.com –f –l 1473** and press **Enter.**
   The command replies with **Packet needs to be fragmented but DF set.**

```
C:\Users\aborb>ping www.moviescope.com -f -l 1473

Pinging www.moviescope.com [13.56.33.8] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 13.56.33.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\aborb>
```
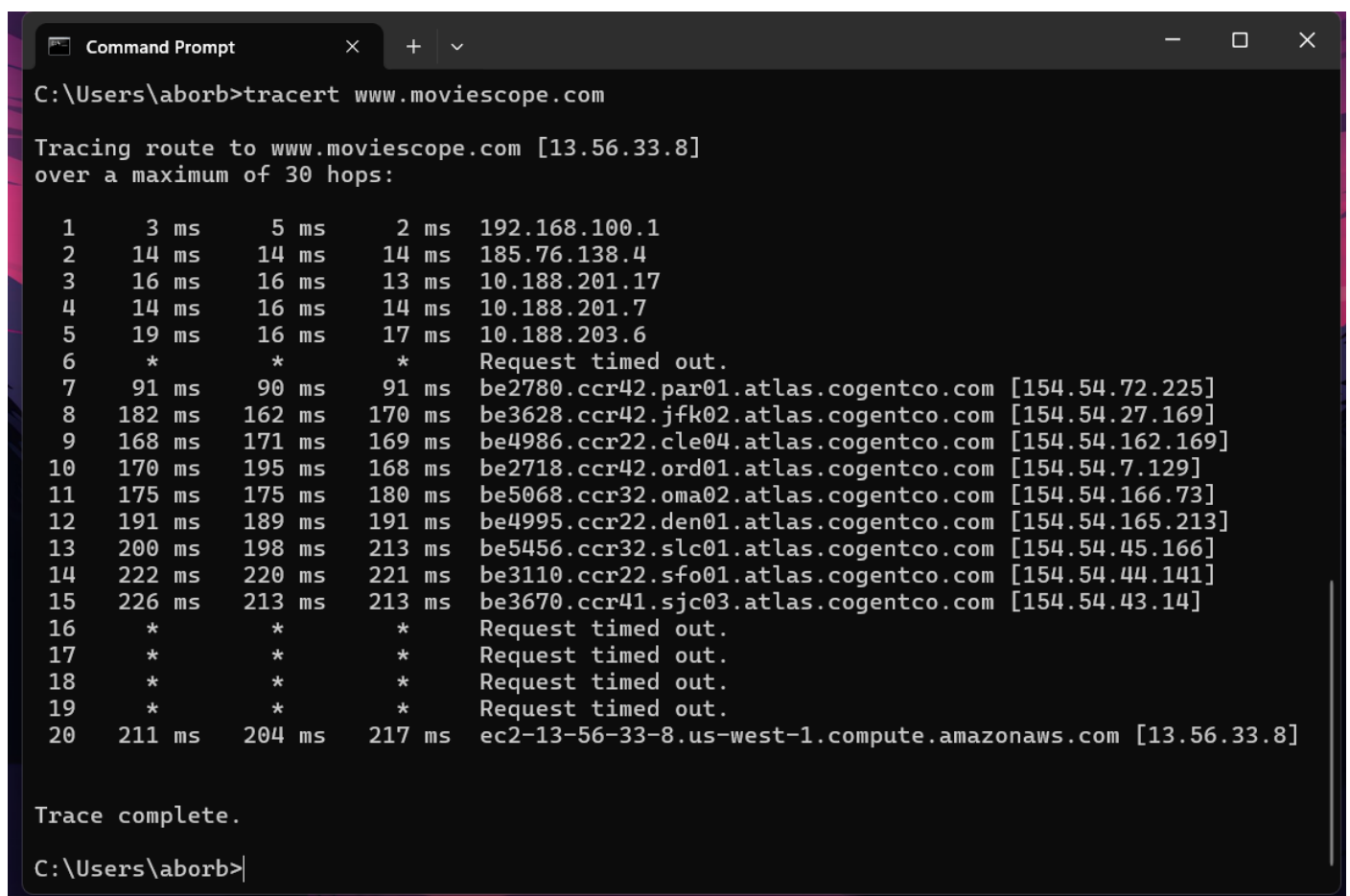
6. In the command prompt type **tracert www.moviescope.com** and press **Enter.**

This command traceroutes the network configuration information of the target domain.

In this lab the command finds the target website in a single hop because it is locally hosted in the Windows Server 2016 machine.

```
Command Prompt          ×    +  ∨                                    —    □    ×

C:\Users\aborb>tracert www.moviescope.com

Tracing route to www.moviescope.com [13.56.33.8]
over a maximum of 30 hops:

  1      3 ms      5 ms      2 ms   192.168.100.1
  2     14 ms     14 ms     14 ms   185.76.138.4
  3     16 ms     16 ms     13 ms   10.188.201.17
  4     14 ms     16 ms     14 ms   10.188.201.7
  5     19 ms     16 ms     17 ms   10.188.203.6
  6      *         *         *      Request timed out.
  7     91 ms     90 ms     91 ms   be2780.ccr42.par01.atlas.cogentco.com [154.54.72.225]
  8    182 ms    162 ms    170 ms   be3628.ccr42.jfk02.atlas.cogentco.com [154.54.27.169]
  9    168 ms    171 ms    169 ms   be4986.ccr22.cle04.atlas.cogentco.com [154.54.162.169]
 10    170 ms    195 ms    168 ms   be2718.ccr42.ord01.atlas.cogentco.com [154.54.7.129]
 11    175 ms    175 ms    180 ms   be5068.ccr32.oma02.atlas.cogentco.com [154.54.166.73]
 12    191 ms    189 ms    191 ms   be4995.ccr22.den01.atlas.cogentco.com [154.54.165.213]
 13    200 ms    198 ms    213 ms   be5456.ccr32.slc01.atlas.cogentco.com [154.54.45.166]
 14    222 ms    220 ms    221 ms   be3110.ccr22.sfo01.atlas.cogentco.com [154.54.44.141]
 15    226 ms    213 ms    213 ms   be3670.ccr41.sjc03.atlas.cogentco.com [154.54.43.14]
 16      *         *         *      Request timed out.
 17      *         *         *      Request timed out.
 18      *         *         *      Request timed out.
 19      *         *         *      Request timed out.
 20    211 ms    204 ms    217 ms   ec2-13-56-33-8.us-west-1.compute.amazonaws.com [13.56.33.8]

Trace complete.

C:\Users\aborb>
```
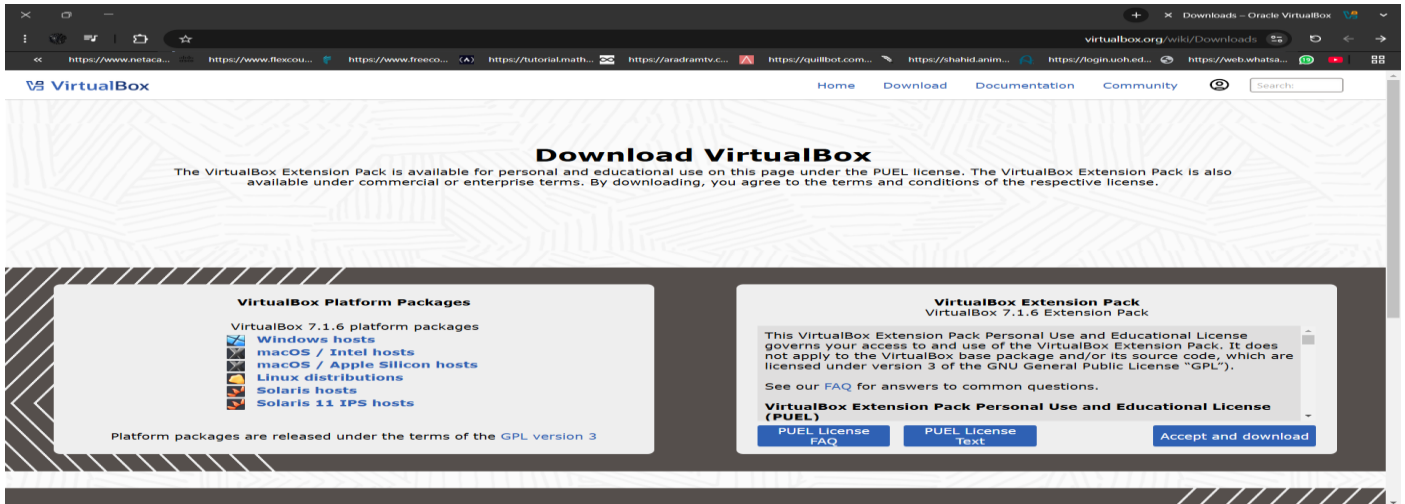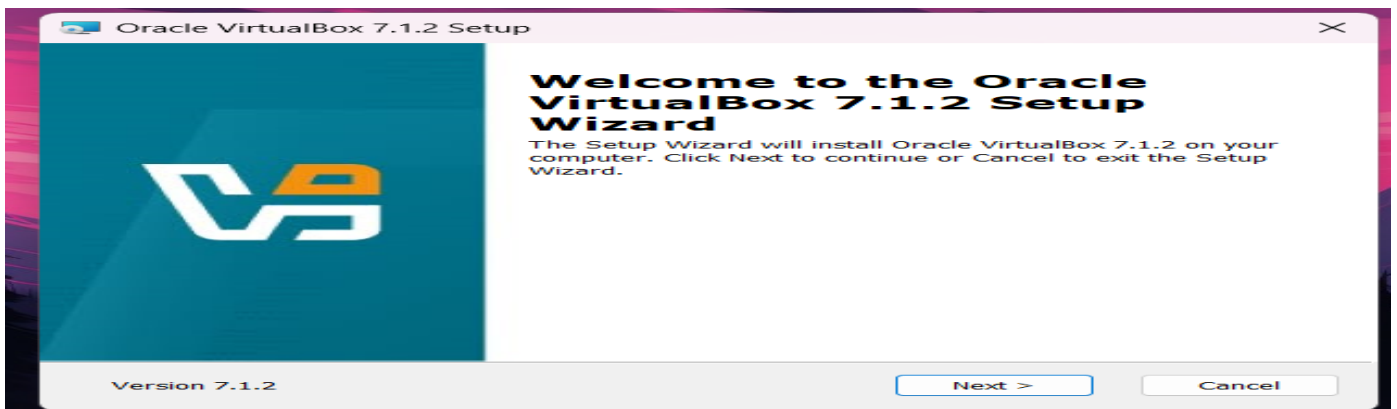
Installing and Setting Up Kali Linux On VirtualBox

Step 1: Install VirtualBox

1. Download **VirtualBox** from **here** and install it. Just follow the on-screen instructions.
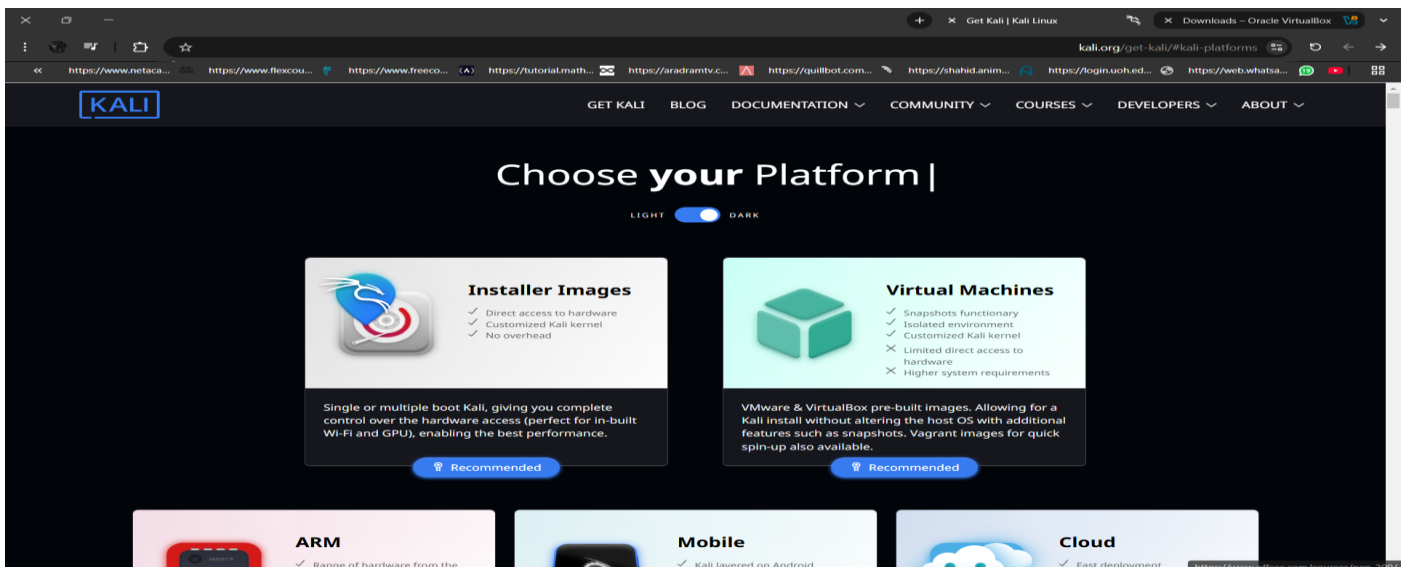

2. Once installed, open VirtualBox.

Step 2: Download Kali Linux ISO

1. Go to the Kali Linux installer images page under downloads.
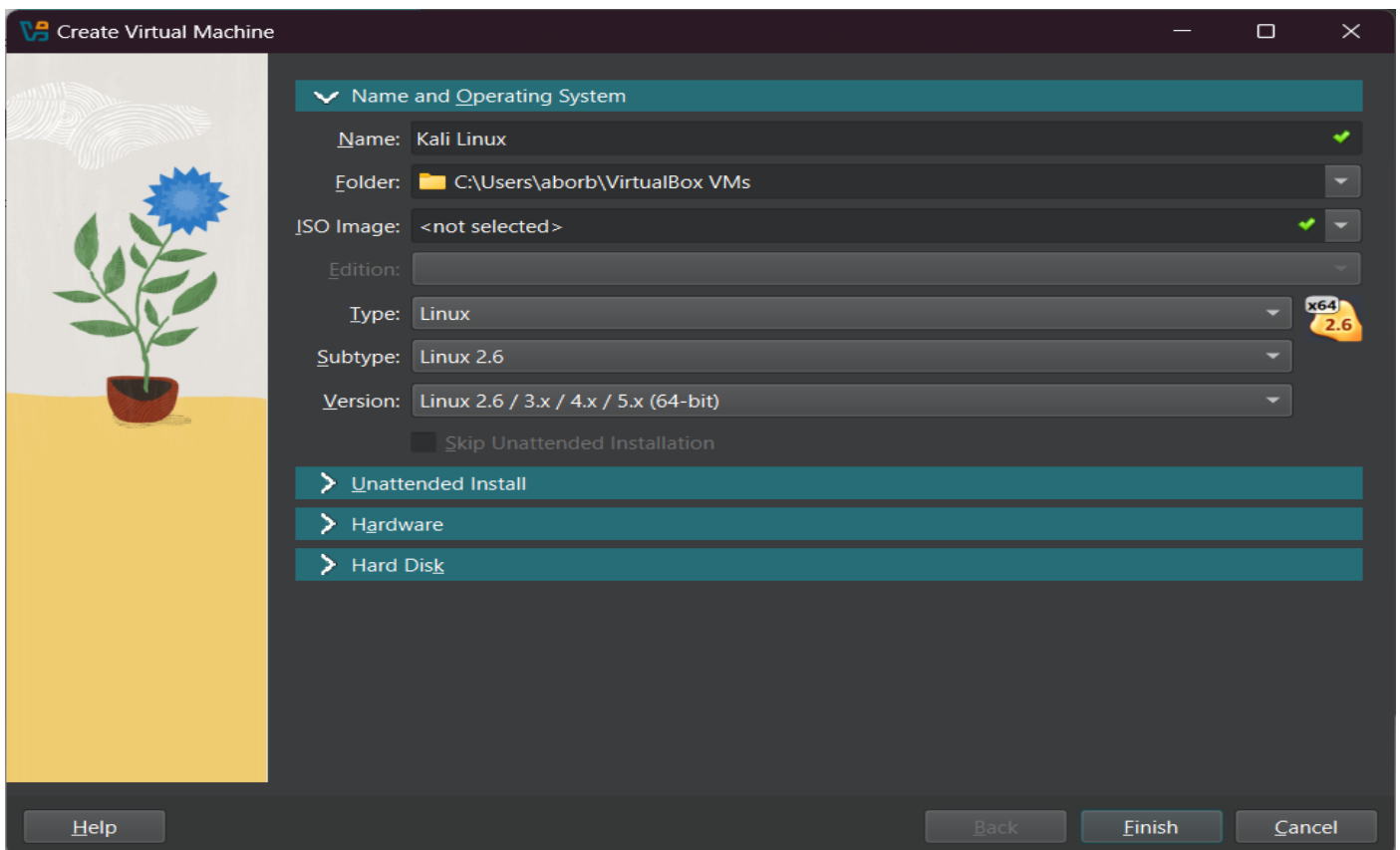
2. Download the **64-bit ISO file** from here.

Step 3: Create a Virtual Machine for Kali Linux

1. Open **VirtualBox** and click the **New** button.

2. Name it **Kali Linux**.

-
  - **Type**: Linux
  - **Version**: Debian (64-bit)

**Step 4: Attach Kali Linux ISO to the Virtual Machine**

1.In VirtualBox, click on the **Kali Linux** virtual machine you just created and go to **Settings**.

2.Click **Storage** and then click on **Empty** under **Controller: IDE**

3. Click the disk icon on the right and select Choose a disk file.

4. Find and select the Kali Linux ISO file you downloaded earlier.

5. Click OK.
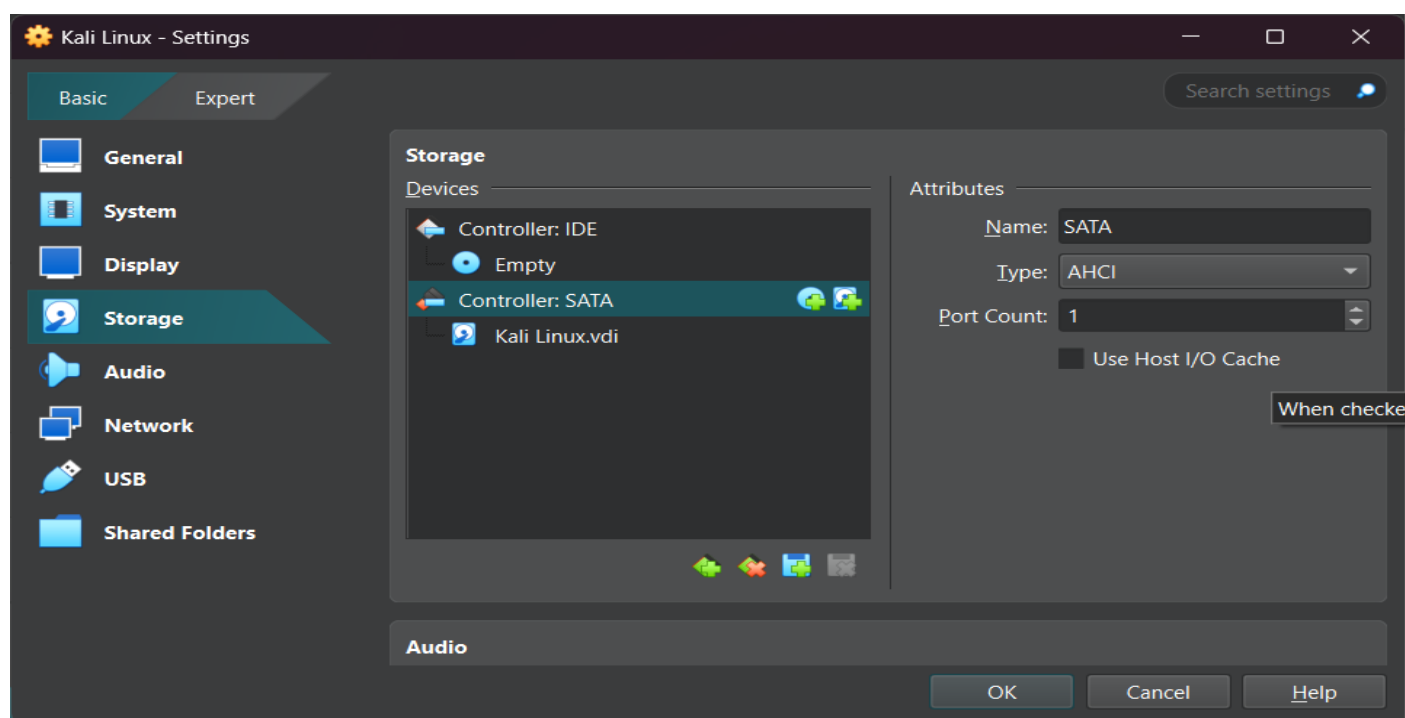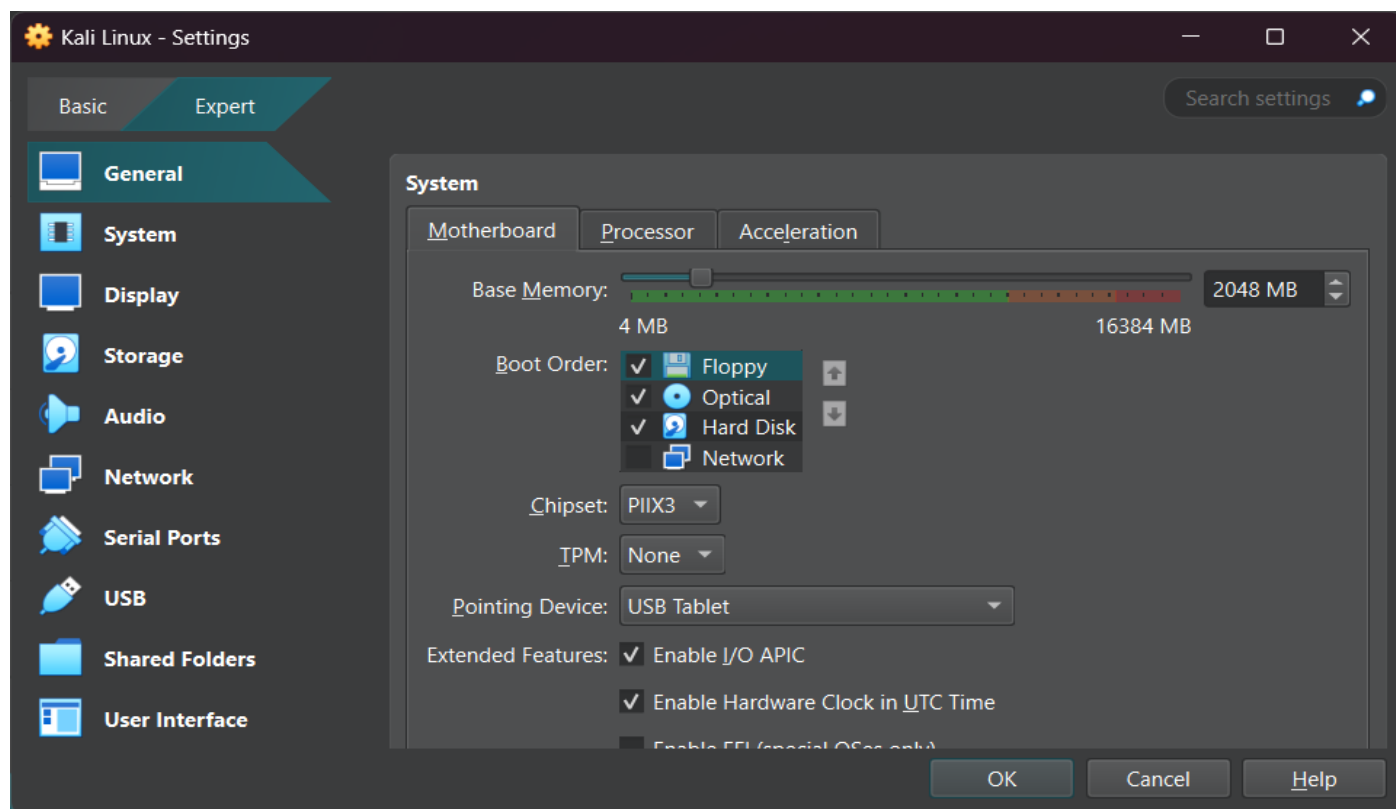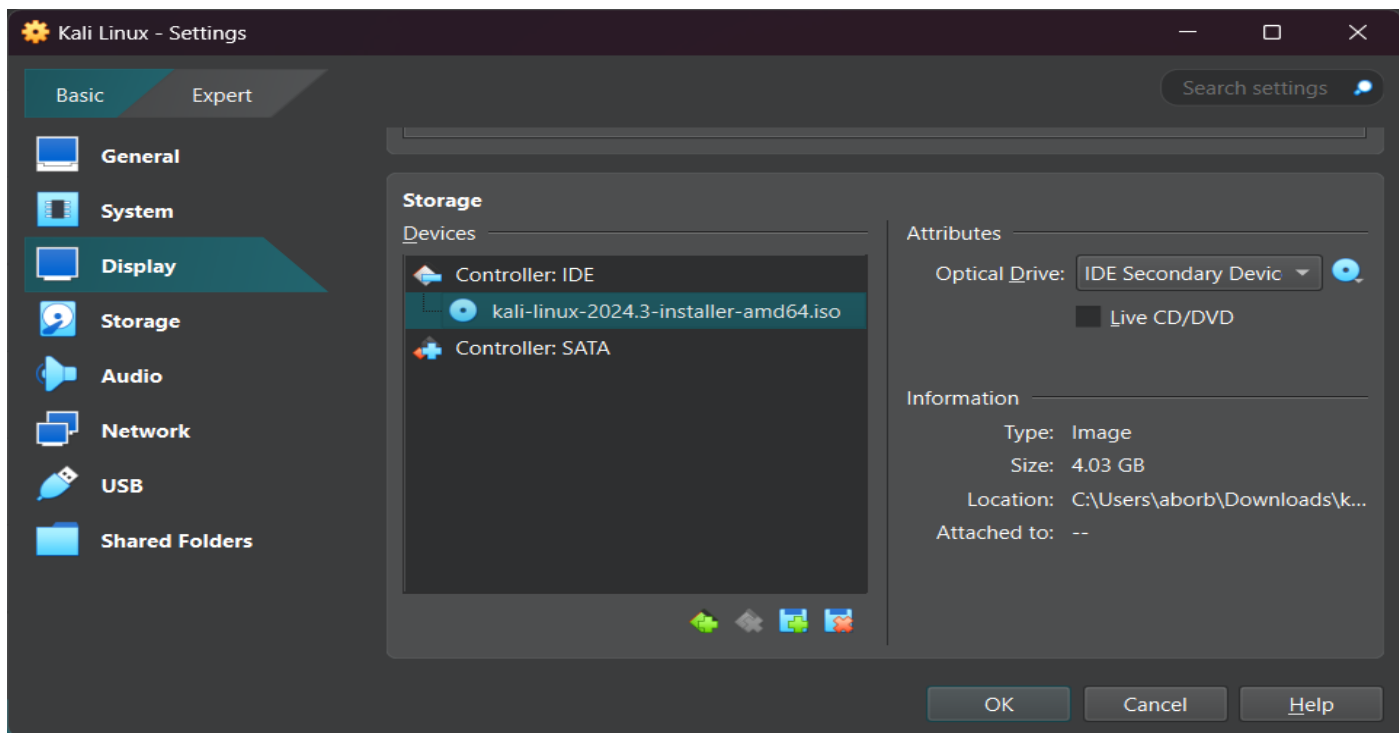
Step 5: Install Kali Linux

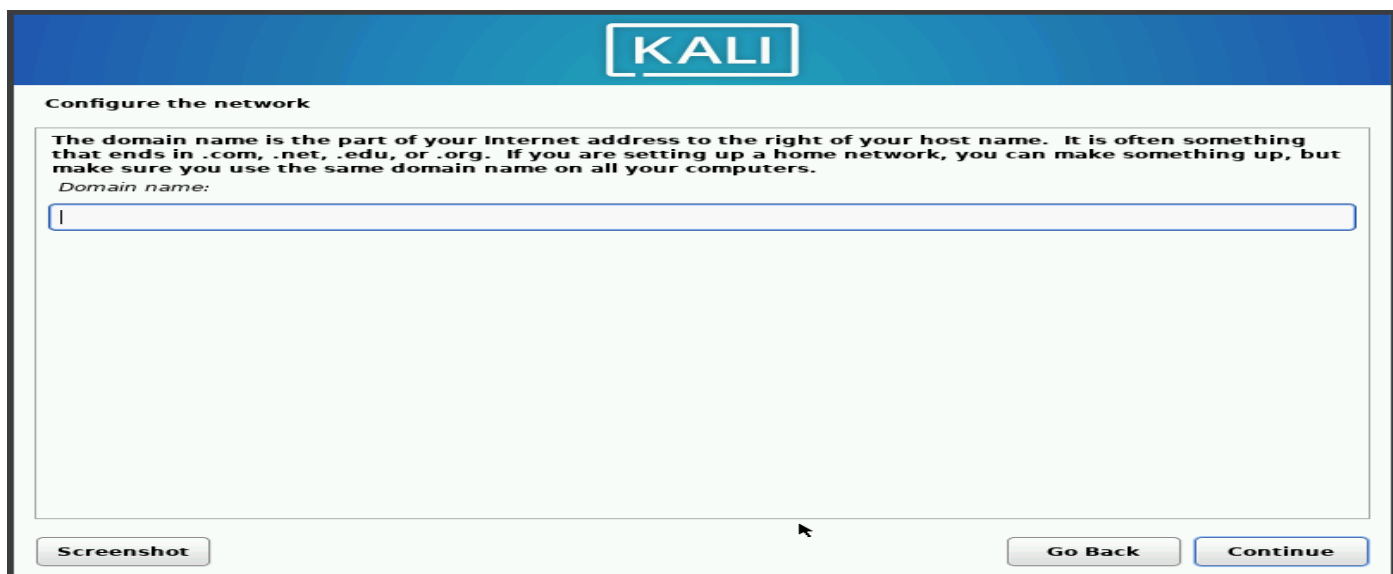1. Now, click **Start** to boot up the **Kali Linux** virtual machine.
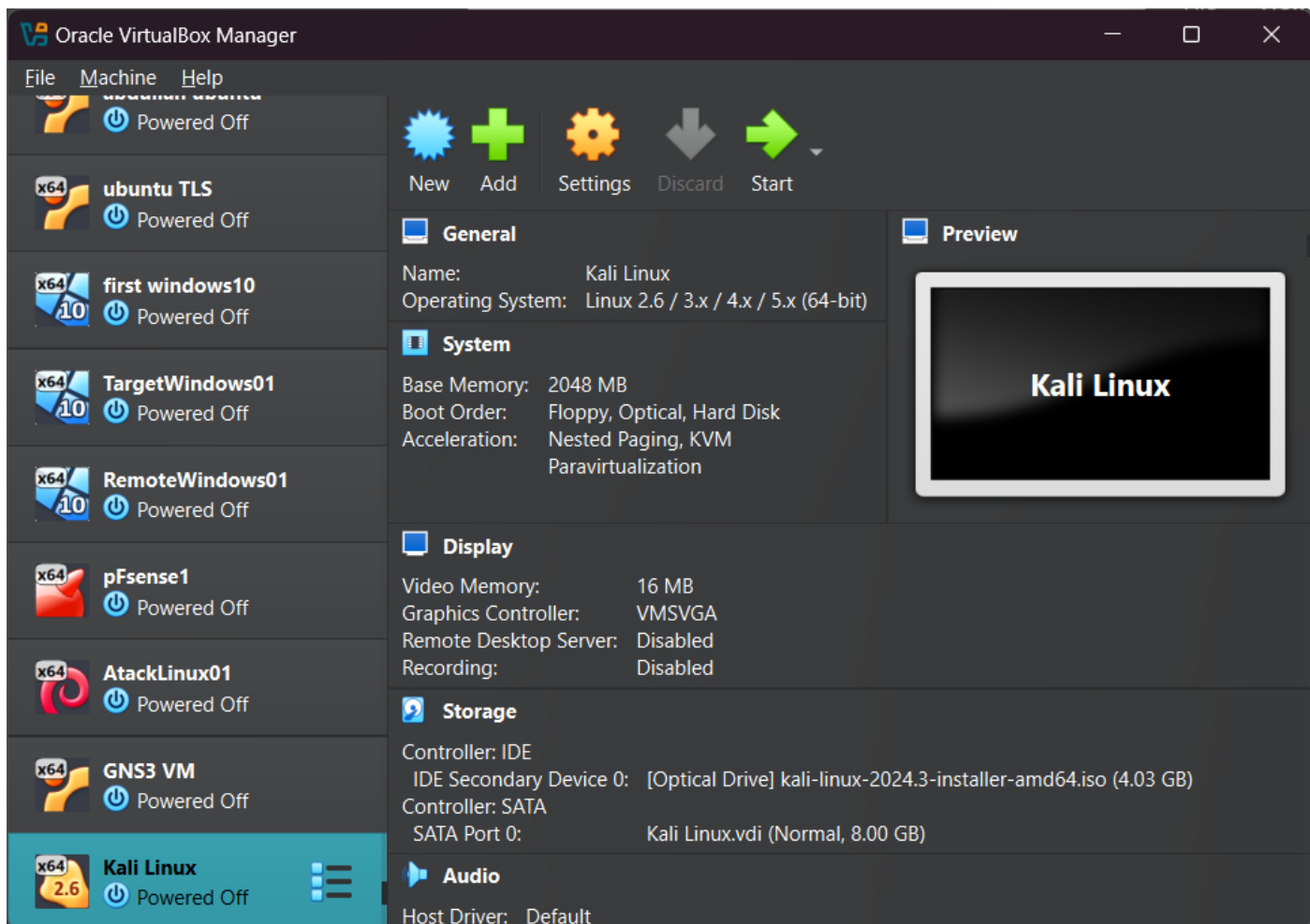
2. When the **Kali Linux boot menu** appears, select **Graphical Install** and press **Enter**.

3. Choose your language, location, and keyboard layout.

4. Set up your network, hostname, and user account as prompted.

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Abdullah

Screenshot   Go Back   Continue

Set up users and passwords

Make sure to select a strong password that cannot be guessed.

Choose a password for the new user:

●●●●

☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

●●●●

☐ Show Password in Clear

Screenshot   Go Back   Continue

5. When asked about disk partitioning, select **Guided – use the entire disk**.

Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk
Guided - use entire disk and set up LVM
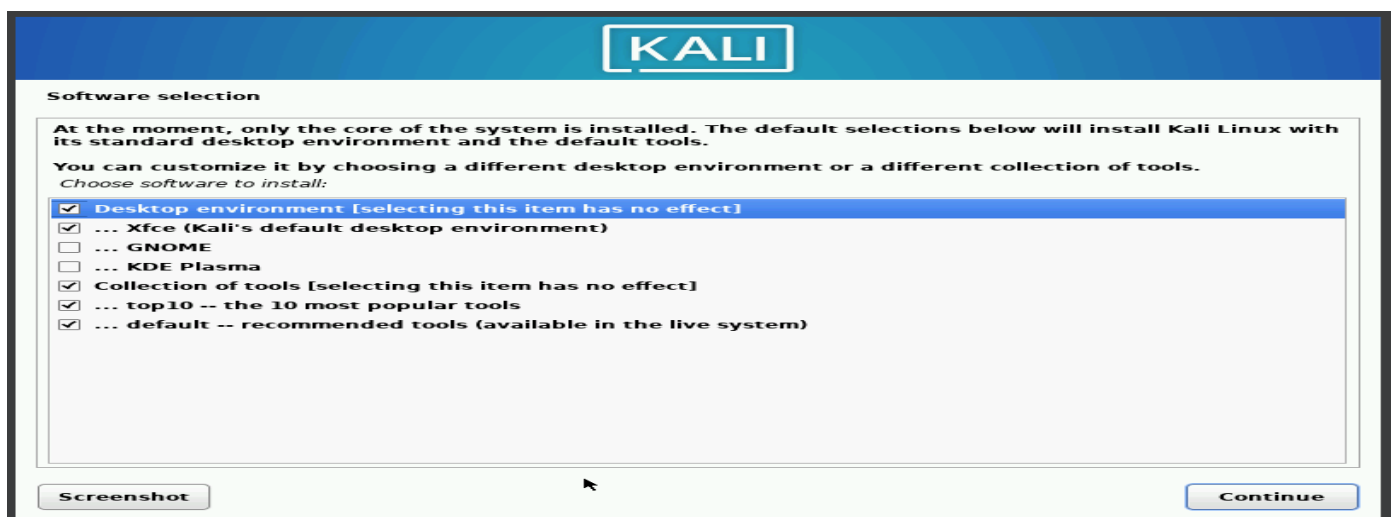Guided - use entire disk and set up encrypted LVM
Manual

Screenshot   Go Back   Continue

6. Continue following the on-screen instructions to complete the installation.

Step 6: Finish Installation and Remove the ISO

1. After the installation is complete, the system will ask you to reboot.

2. Before restarting, return to **Settings** > **Storage** in VirtualBox and remove the Kali Linux ISO file by clicking **Remove Disk from Virtual Drive**.
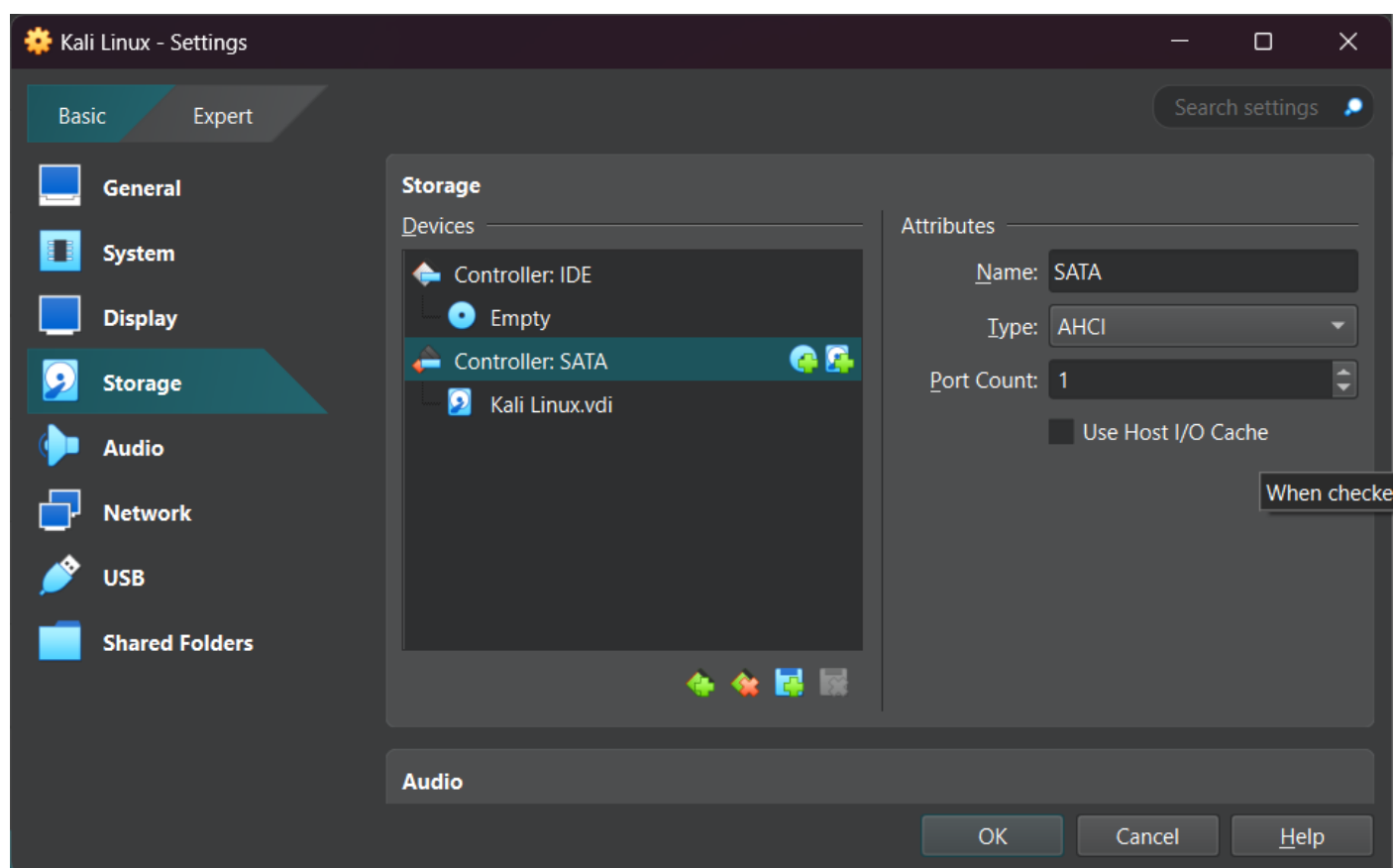
3. Now restart your virtual machine. Kali Linux will boot up!