
Configuring the virtual machine

After logging in to the Kali Linux virtual machine, we are going to configure several things. These are important steps if we want to perform penetration testing.

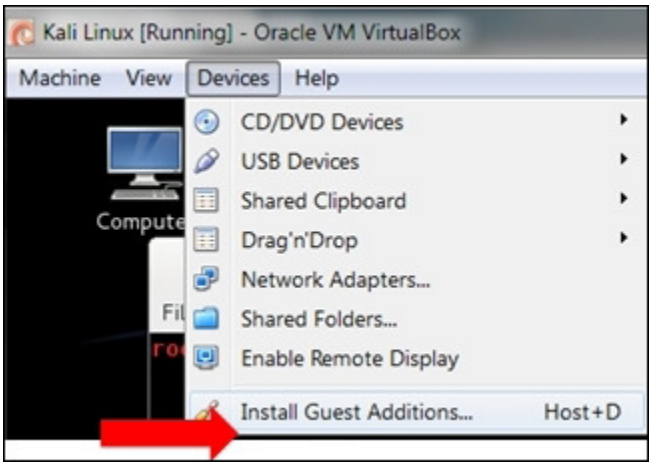
VirtualBox guest additions

We recommend that after you have successfully created the Kali Linux Virtual Machine using VirtualBox, you install **VirtualBox guest additions**. This add-on will provide you with the following additional features:

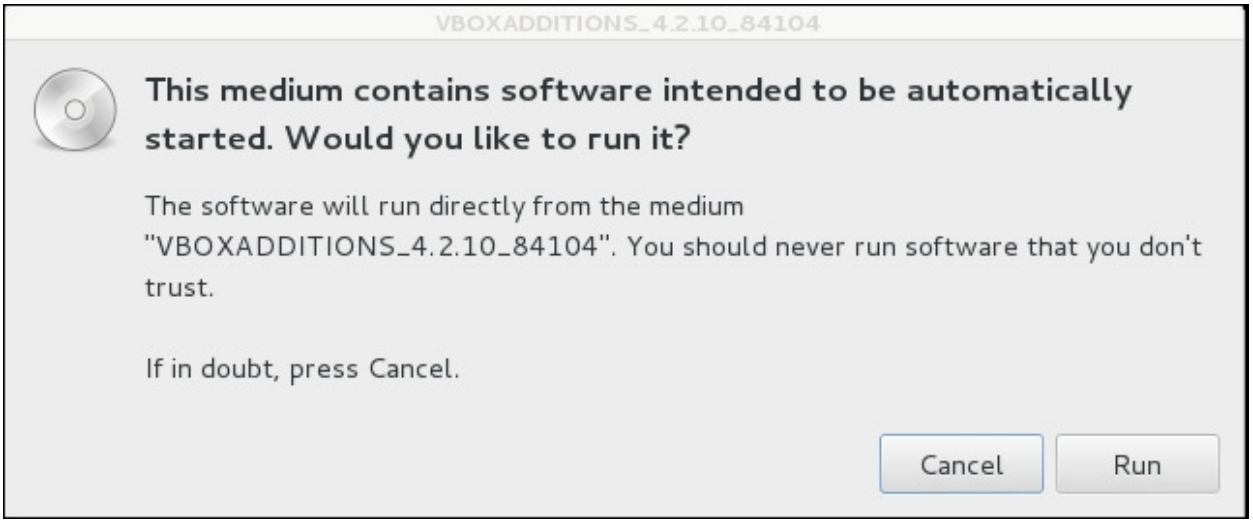
- It will enable the virtual machine to be viewed in full screen
- It will make the mouse move faster in the virtual machine
- It will enable you to copy and paste the text between the host and guest machine
- It will enable the guest and host machine to share folders

To install the guest additions, you can perform the following steps:

1. From the VirtualBox menu, navigate to **Devices** | **Install Guest Additions**. You will then see that the VirtualBox guest addition file is mounted as a disk:



2. Then, VirtualBox will display the following message. Click on **Cancel** to close the window:



3. Open the terminal console and change the VirtualBox guest additions CDROM mount point (`/media/cdrom0`):

```
root@kali:~# cd /media/cdrom0/
root@kali:/media/cdrom0# ls
32Bit          cert                    VBoxSolarisAdditions.pkg
64Bit          OS2                     VBoxWindowsAdditions-amd64.exe
AUTORUN.INF    runasroot.sh            VBoxWindowsAdditions.exe
autorun.sh     VBoxLinuxAdditions.run  VBoxWindowsAdditions-x86.exe
root@kali:/media/cdrom0#
```

4. Execute `VBoxLinuxAdditions.run` to run the VirtualBox guest additions installer:

```
sh ./VBoxLinuxAdditions.run
```

5. You may need to wait for several minutes until all of the required modules are successfully built and installed:

```
root@kali:/media/cdrom0# sh ./VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 4.2.10 Guest Additions for Linux.........
VirtualBox Guest Additions installer
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the following
module compilation fails then this could be the reason.

Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.12 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the hal service and the Window System (or just restart
the guest system) to enable the Guest Additions.

Installing graphics libraries and desktop services components ...done.
```

6. Change to the root home directory.
7. Eject the VBoxAdditions CD Image by right-clicking on the icon and selecting **Eject** from the menu. If successful, the VBoxAdditions icon will disappear from the desktop.
8. Reboot the virtual machine by typing the `reboot` command in the terminal console.
9. After the reboot, you can switch to full screen (**View** | **Switch to fullscreen**) from the VirtualBox menu.

Setting up networking

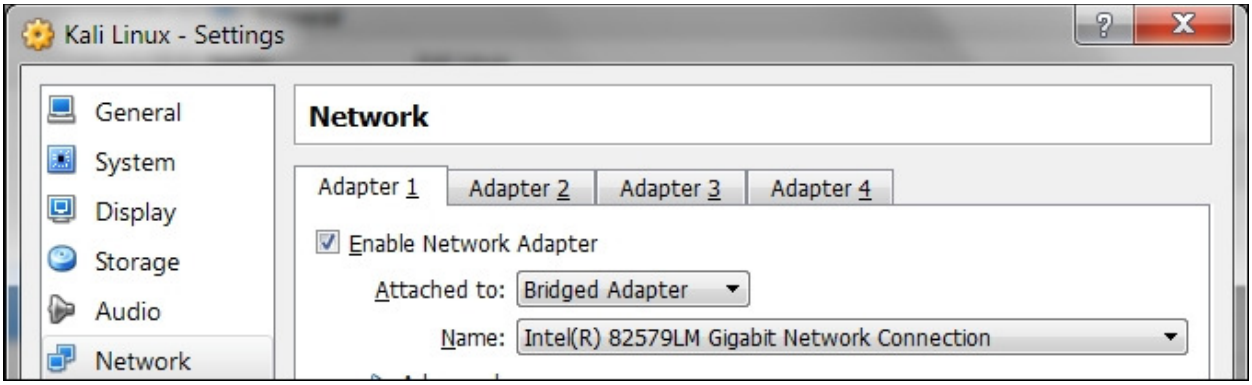
In the following section, we will discuss how to set up the networking in Kali Linux for the wired and wireless network.

Setting up a wired connection

In the default Kali Linux VMware image or ISO configuration, Kali Linux uses **NAT** (**Network Address Translation**) as the network's connection type. In this connection mode, the Kali Linux machine will be able to connect to the outside world through the host operating system whereas the outside world, including the host operating system, will not be able to connect to the Kali Linux virtual machine.

For the penetration testing task, you might need to change this networking method to **Bridged Adapter**. The following are the steps to change it:

1. First, make sure you have already powered off the virtual machine.
2. Then, open up the VirtualBox Manager, select the appropriate virtual machine—in this case we are using the Kali Linux virtual machine—and then click on the **Network** icon on the right-hand side and change the **Attached to** drop-down box from **NAT** to **Bridged Adapter** in Adapter 1. In the **Name** field, you can select the network interface that is connected to the network you want to test, as shown in the following screenshot:



To be able to use the bridge network connection, the host machine needs to connect to a network device that can give you an IP address via DHCP, such as a router or a switch.

As you may be aware, a DHCP IP address is not a permanent IP address; it's just a lease IP address. After several times (as defined in the DHCP lease time), the Kali Linux virtual machine will need to get a lease IP address again. This IP address might be the same as the previous one or might be a different one.

If you want to make the IP address permanent, you can do so by saving the IP address in the `/etc/network/interfaces` file.

The following is the default content of this file in Kali Linux:

```
auto lo
iface lo inet loopback
```

In the default configuration, all of the network cards are set to use DHCP to get the IP address. To make a network card bind to an IP address permanently, we have to edit that file and change the content to the following:

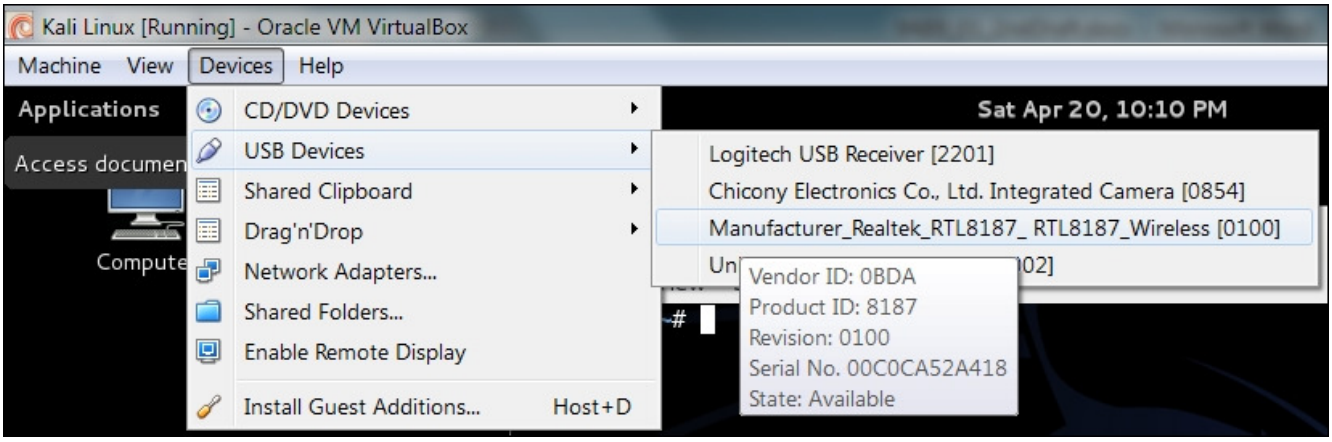
```
auto eth0
iface eth0 inet static
address 10.0.2.15
netmask 255.255.255.0
network 10.0.2.0
broadcast 10.0.2.255
gateway 10.0.2.2
```

Here, we set the first network card (`eth0`) to bind to the IP address of `10.0.2.15` . You may need to adjust this configuration according to the network environment you want to test.

Setting up a wireless connection

By running Kali Linux as a virtual machine, you cannot use the wireless card that is embedded in your laptop. Fortunately, you can use an external USB-based wireless card.

To activate your USB-based wireless card in the Kali virtual machine, plug in the wireless card to a USB port, navigate to **Devices** | **USB Devices**, and select your wireless card from the VirtualBox menu:

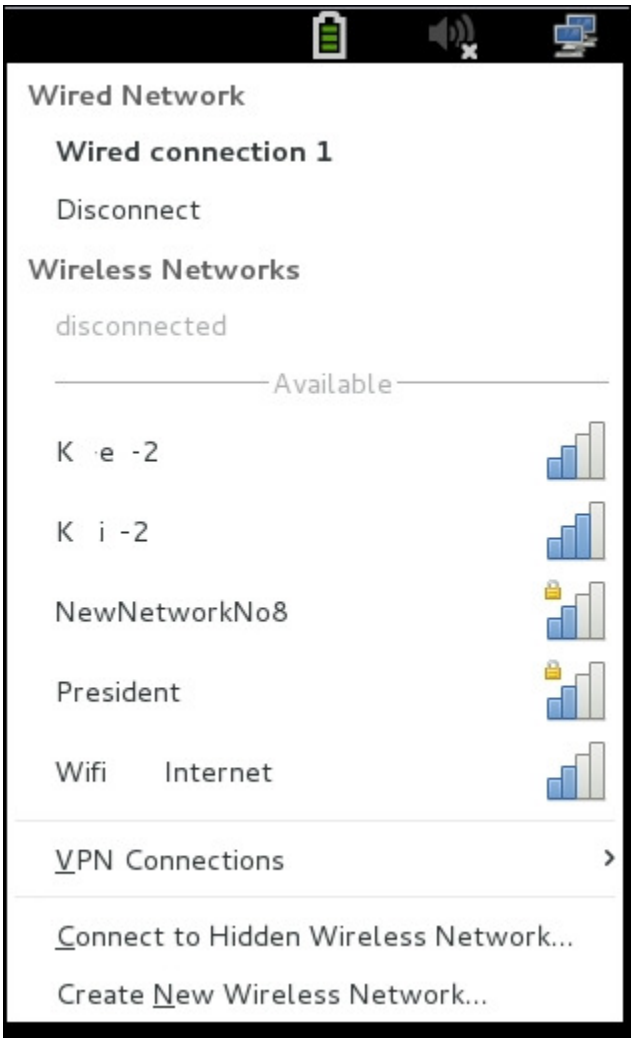


In this screenshot, we select the wireless card that uses the Realtek chipset.

If your USB wireless card has been successfully recognized by Kali, you can use the `dmesg` program to see the wireless card's information.

In the top-right section of the Kali menu, you will see the Network Connections icon. You can click on it to display your network information.

You will see several networks' names, wired or wireless, available for your machine:



To connect to the wireless network, just select the particular SSID you want by double-clicking on its name. If the wireless network requires authentication, you will be prompted to enter the password. Only after you give the correct password are you allowed to connect to that wireless network.

Starting the network service

To control the networking process' startup or shutdown process, you can use a helper script called `service` .

To start a networking service, just give the following command:

```
service networking start
```

To stop a networking service, type the following command:

```
service networking stop
```

> **Note**
>
> To issue these commands, you need the root privilege.

You can test whether your network is working correctly by sending an ARP ping request to a host in the same network segment using the `arping` command.

You may find that after you reboot your Kali Linux machine, the networking service needs to be started again. To make the networking service start automatically after the reboot, you need to give the following command:

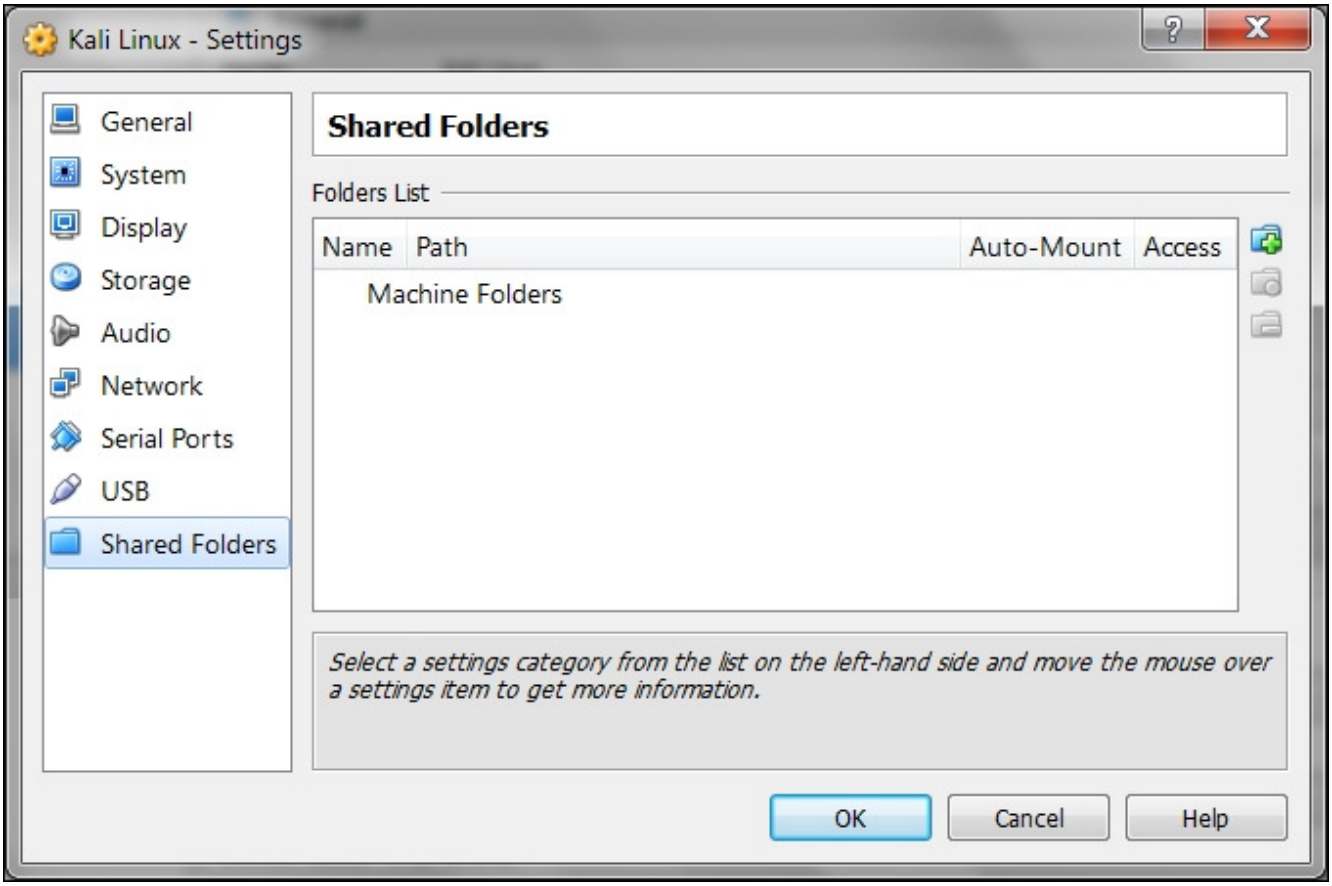
```
update-rc.d networking defaults
```

This command will insert the necessary links to the `/etc/rc*.d` directories to start the networking script automatically after Kali has been rebooted.

Configuring shared folders

During a penetration testing process, we may find that we need to share files between the host OS and the guest OS, such as to store penetration testing results on the host machine. One of the mechanisms that can be used for this requirement is to use VirtualBox's **Shared Folders**.

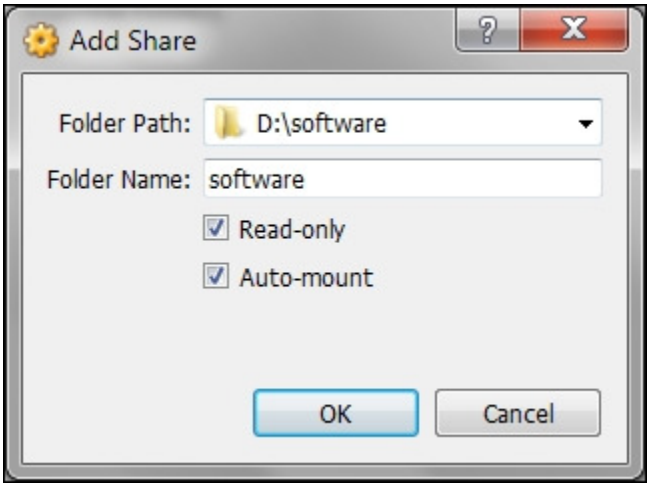
To configure the shared folder from the VirtualBox menu, you need to power off the virtual machine that you want to configure. After that, you need to select the appropriate guest machine's name and click on the **Shared Folders** menu in the window on the left. You will then see the following screen:



To add the folder from the host OS, click on the **+** icon on the right-hand side. After that, select the appropriate folder that you want to share in the host OS. The selected folder path will be displayed in the **Folder Path** field.

For the **Folder Name** field, you can choose a name that is suitable for the folder. This name will be used by the guest OS to identify the host OS' shared folder.

If you do not want the guest OS to write to the specified shared folder, you can check the option to **Read-only**. If the **Auto-mount** option is checked, the guest OS will try to mount the folder automatically after its startup, as shown in the following screenshot:



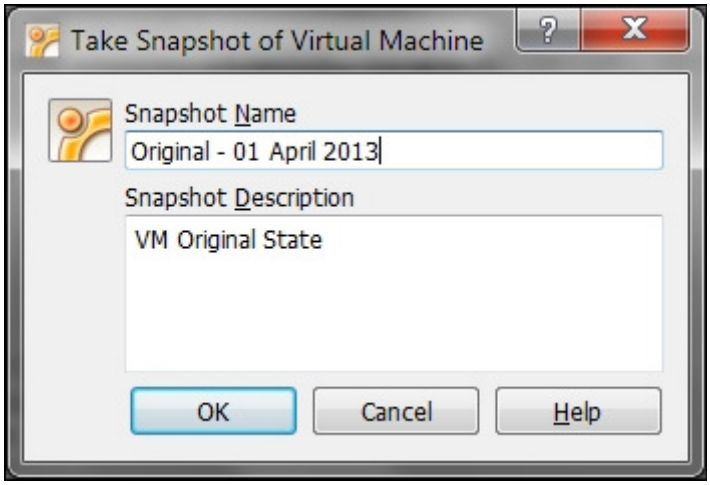
In the preceding screenshot, we shared a **D:\software** folder to the guest OS as a read-only folder.

The shared folder can be accessed from the virtual machine as a `/media/sf_software` directory.

Saving the guest machine state

If you have correctly configured your guest OS, we suggest that you save your OS state. The purpose of this action is that in case you mess up your virtual machine badly, you can still restore it to the previous good state.

To save the virtual machine's state, VirtualBox has provided you with this capability under the menu of **Machine – Take Snapshot**. You need to start the virtual machine before you can take its snapshot:



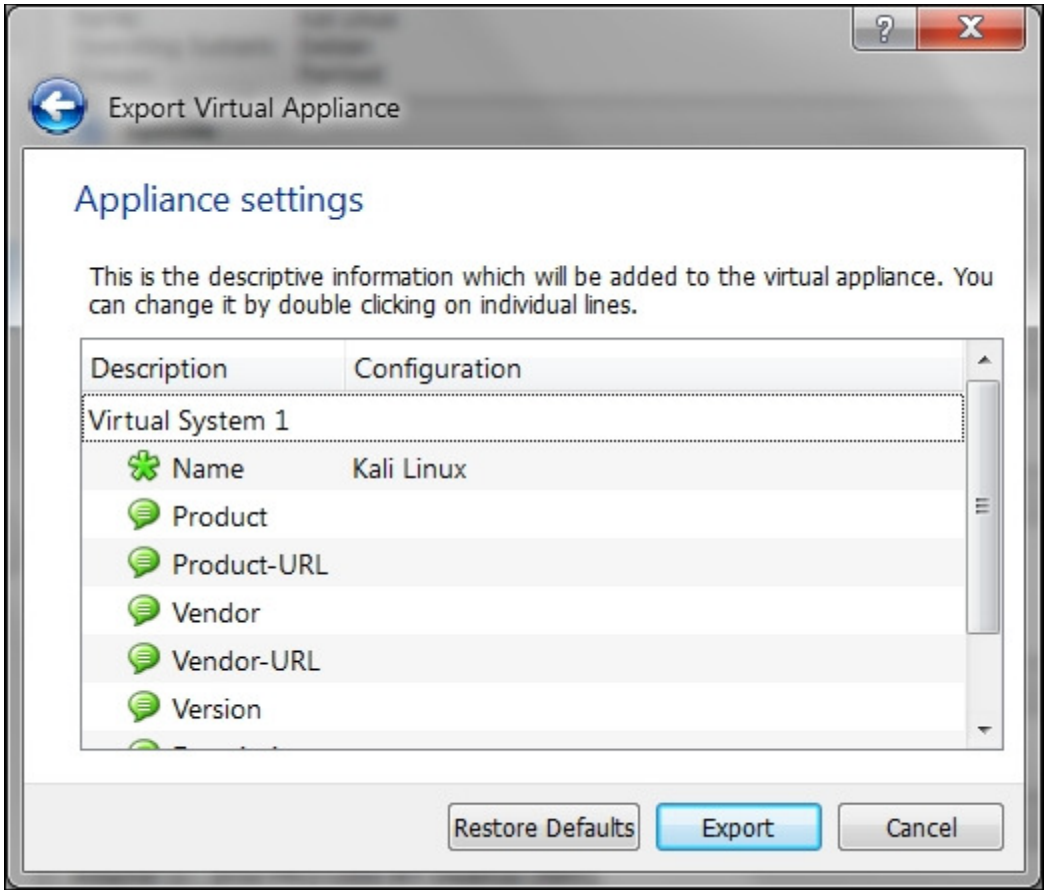
For the **Snapshot Name**, you can use any name but we suggest that you put in the information about the date. You can give detailed information in the **Snapshot Description** field. After you fill in all the information, VirtualBox will store the virtual machine state; this process will take some time depending on how much information is available to be saved.

Exporting a virtual machine

There are times when you need to back up your virtual machine to a file or share your virtual machine with other people. VirtualBox allows you to do that easily. For this action, you need to turn off the virtual machine that you want to export, and then navigate to **File** | **Export Appliance**.

The following steps will help you export an appliance:

1. Select the **Export Appliance** menu; VirtualBox will display an **Appliance Export Wizard** screen.
2. Next, choose the virtual machine that you want to export.
3. Later on, you will be asked for the output file's location. By default, the location will be your directory and the file format will be **ova** (**Open Virtualization Format Archive**). We suggest that you use the default file format if you don't know which file format to choose.
4. Next, you are prompted for the appliance export's configuration values. You can configure the properties here. However, you can usually just leave them empty unless you need to set specific values:



After this, the exporting process will take place. The time required to finish the export depends on the size of the virtual machine. The bigger the virtual machine size, the longer the exporting time. On my system, it took around 20 minutes to export the Kali Linux virtual machine.