
Chapter 1. Beginning with Kali Linux

This chapter will guide you through the wonderful world of **Kali Linux**—a specialized Linux distribution for the purpose of penetration testing. In this chapter, we will cover the following topics:

- A brief history of Kali
- Several common usages of Kali
- Downloading and installing Kali
- Configuring and updating Kali

At the end of this chapter, we will describe how to install additional weapons and how to configure Kali Linux.

A brief history of Kali Linux

Kali Linux (Kali) is a Linux distribution system that was developed with a focus on the penetration testing task. Previously, Kali Linux was known as **BackTrack**, which itself is a merger between three different live Linux **penetration testing** distributions: IWHAX, WHOPPIX, and Auditor.

BackTrack is one of the most famous Linux distribution systems, as can be proven by the number of downloads that reached more than four million as of BackTrack Linux 4.0 pre final.

Kali Linux Version 1.0 was released on March 12, 2013. Five days later, Version 1.0.1 was released, which fixed the USB keyboard issue. In those five days, Kali has been downloaded more than 90,000 times.

The following are the major features of Kali Linux (http://docs.kali.org/introduction/what-is-kali-linux):

- It is based on the Debian Linux distribution
- It has more than 300 penetration testing applications
- It has vast wireless card support
- It has a custom kernel patched for packet injection
- All Kali software packages are GPG signed by each developer
- Users can customize Kali Linux to suit their needs
- It supports ARM-based systems

Kali Linux tool categories

Kali Linux contains a number of tools that can be used during the penetration testing process. The penetration testing tools included in Kali Linux can be categorized into the following categories:

- **Information gathering**: This category contains several tools that can be used to gather information about DNS, IDS/IPS, network scanning, operating systems, routing, SSL, SMB, VPN, voice over IP, SNMP, e-mail addresses, and VPN.
- **Vulnerability assessment**: In this category, you can find tools to scan vulnerabilities in general. It also contains tools to assess the Cisco network, and tools to assess vulnerability in several database servers. This category also includes several fuzzing tools.
- **Web applications**: This category contains tools related to web applications such as the content management system scanner, database exploitation, web application fuzzers, web application proxies, web crawlers, and web vulnerability scanners.
- **Password attacks**: In this category, you will find several tools that can be used to perform password attacks, online or offline.
- **Exploitation tools**: This category contains tools that can be used to exploit the vulnerabilities found in the target environment. You can find exploitation tools for the network, Web, and database. There are also tools to perform social engineering attacks and find out about the exploit information.
- **Sniffing and spoofing**: Tools in this category can be used to sniff the network and web traffic. This category also includes network spoofing tools such as Ettercap and Yersinia.
- **Maintaining access**: Tools in this category will be able to help you maintain access to the target machine. You might need to get the highest privilege level in the machine before you can install tools in this category. Here, you can find tools for backdooring the operating system and web application. You can also find tools for tunneling.
- **Reporting tools**: In this category, you will find tools that help you document the penetration-testing process and results.
- **System services**: This category contains several services that can be useful during the penetration testing task, such as the Apache service, MySQL service, SSH service, and Metasploit service.

To ease the life of a penetration tester, Kali Linux has provided us with a category called **Top 10 Security Tools**. Based on its name, these are the top 10 security tools commonly used by penetration testers. The tools included in this category are `aircrack-ng`, `burp-suite`, `hydra`, `john`, `maltego`, `metasploit`, `nmap`, `sqlmap`, `wireshark`, and `zaproxy`.

Besides containing tools that can be used for the penetration testing task, Kali Linux also comes with several tools that you can use for the following:

- **Wireless attacks**: This category includes tools to attack Bluetooth, RFID/NFC, and wireless devices.
- **Reverse engineering**: This category contains tools that can be used to debug a program or disassemble an executable file.
- **Stress testing**: This category contains tools that can be used to help you in stress testing your network, wireless, Web, and VOIP environment.
- **Hardware hacking**: Tools in this category can be used if you want to work with Android and Arduino applications.
- **Forensics**: In this category, you will find several tools that can be used for digital forensics, such as acquiring a hard disk image, carving files, and analyzing the hard disk image. To use the forensics capabilities in Kali Linux properly, you need to navigate to **Kali Linux Forensics** | **No Drives or Swap Mount** in the booting menu. With this option, Kali Linux will not mount the drives automatically, so it will preserve the drives' integrity.

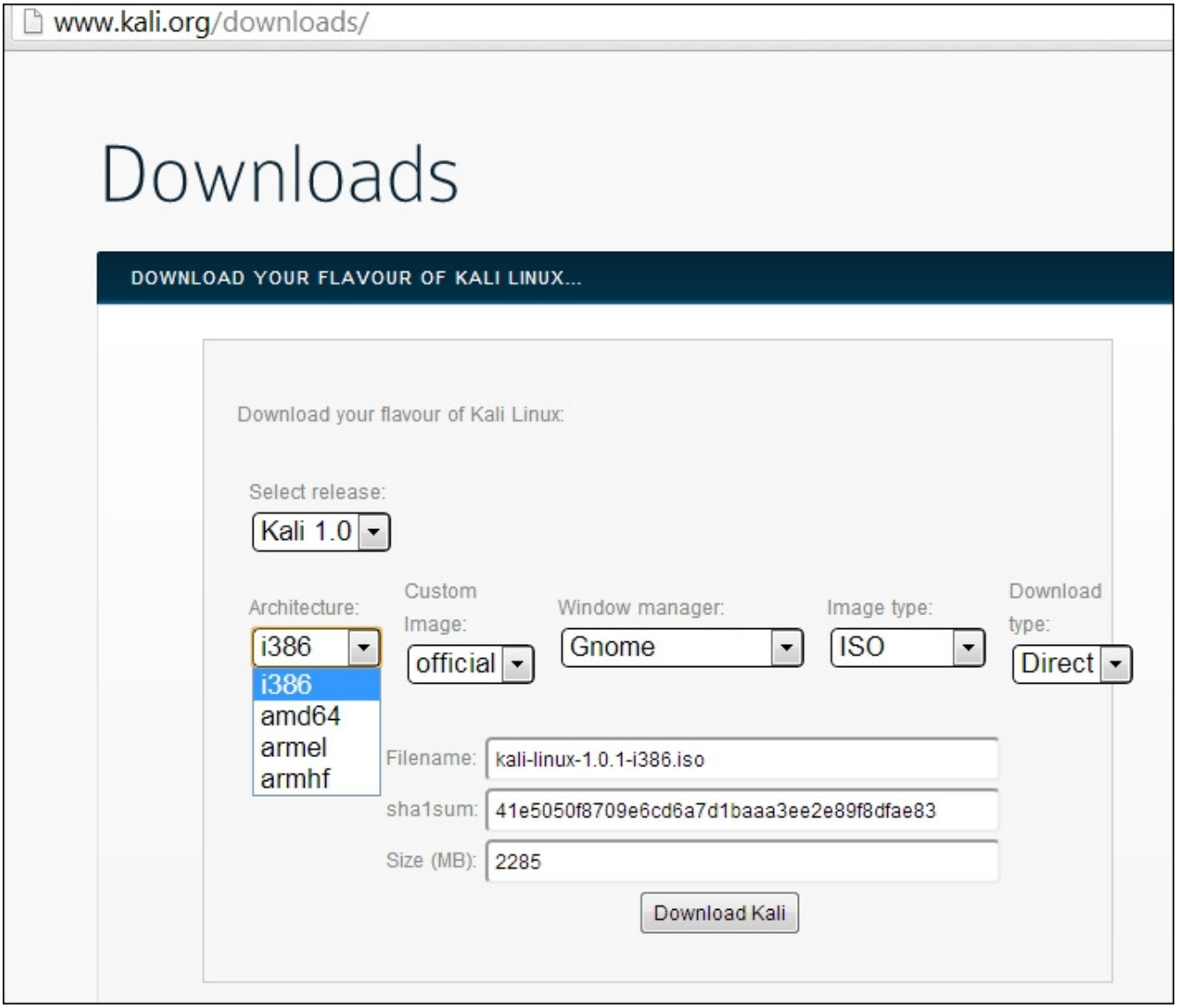
In this book, we are focusing only on Kali Linux's penetration testing tools.

Downloading Kali Linux

The first thing to do before installing and using Kali Linux is to download it. You can get Kali Linux from the Kali Linux website (http://www.kali.org/downloads/).

On the download page, you can select the official Kali Linux image based on the following items, which is also shown in the next screenshot:

- **Machine architecture**: i386, amd64, armel, and armhf
- **Image type**: ISO image or VMware image



If you want to burn the image to a DVD or install Kali Linux to your machine, you might want to download the ISO image version. However, if you want to use Kali Linux for VMWare, you can use the VMWare image file to speed up the installation and configuration for a virtual environment.

After you have downloaded the image file successfully, you need to compare the **SHA1** hash value from the downloaded image with the SHA1 hash value provided on the download page. The purpose of checking the SHA1 value is to ensure the integrity of the downloaded image is preserved. This prevents the user from either installing a corrupt image or an image file that has been maliciously tampered with.

In the UNIX/Linux/BSD operating system, you can use the `sha1sum` command to check the SHA1 hash value of the downloaded image file. Remember that it might take some time to compute the hash value of the Kali Linux image file due to its size. For example, to generate the hash value of the `kali-linux-1.0.1-i386.iso` file, the following command is used:

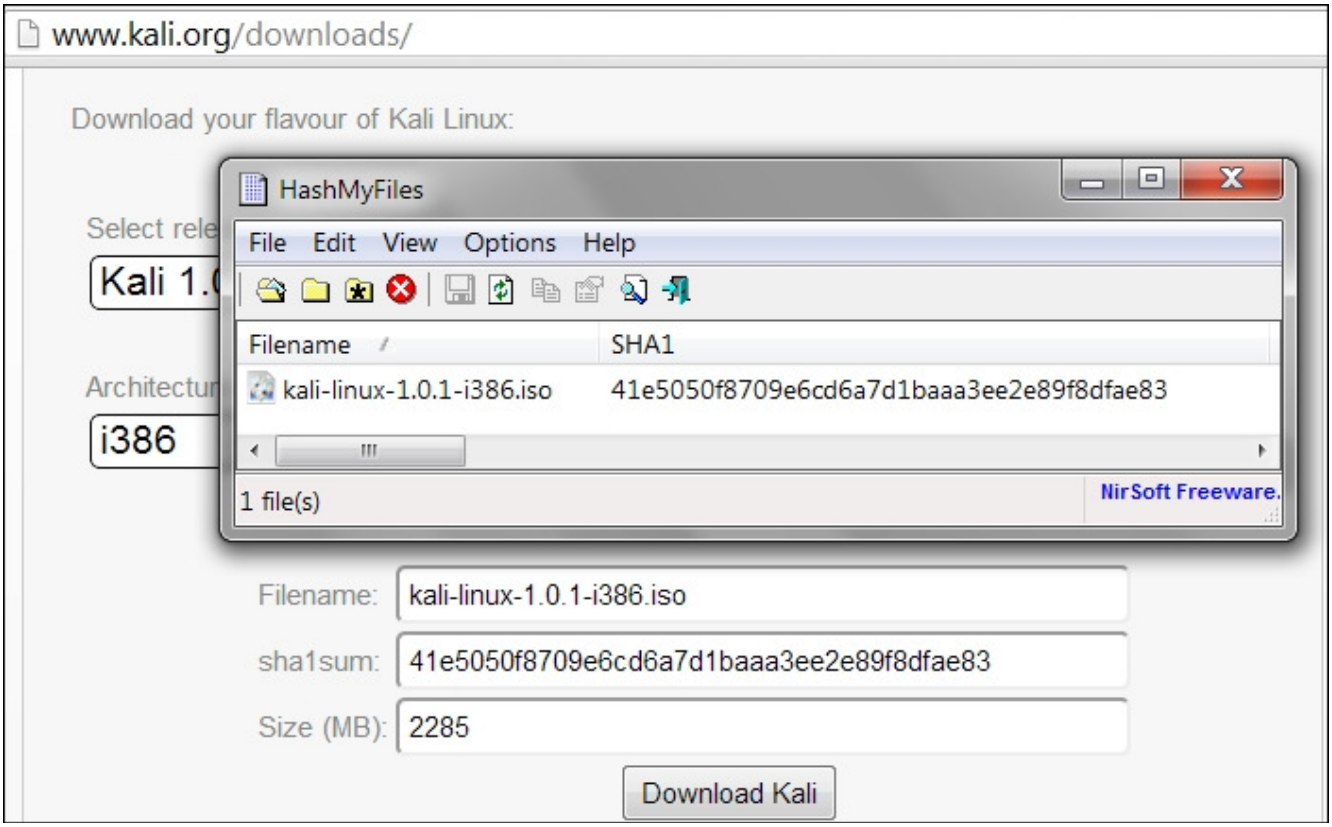
```
sha1sum kali-linux-1.0.1-i386.iso
41e5050f8709e6cd6a7d1baaa3ee2e89f8dfae83  kali-linux-1.0.1-i386.iso
```

In the Windows world, there are many tools that can be used to generate the SHA1 hash value; one of them is `sha1sum`. It is available from http://www.ring.gr.jp/pub/net/gnupg/binary/sha1sum.exe.

We like it because of its small size and it just works. If you want an alternative tool instead of `sha1sum`, there is `HashMyFiles` (http://www.nirsoft.net/utils/hash_my_files.html). HashMyFiles supports MD5, SHA1, CRC32, SHA-256, SHA-384, and SHA-512 hash algorithms.

After you have downloaded `HashMyFiles`, just run the `HashMyFiles` and select the file by navigating to **File** | **Add Files** to find out the SHA1 hash value of a file. Or, you can press *F2* to perform the same function. Then, choose the image file you want.

The following screenshot resembles the SHA1 hash value generated by `HashMyFiles` for the Kali Linux i386 ISO image file:



You need to compare the SHA1 hash value generated by `sha1sum`, `HashMyFiles` or other similar tools with the SHA1 hash value displayed on the Kali Linux download page.

If both the values match, you can go straight to the *Using Kali Linux* section. But if they do not match, it means that your image file is broken; you may want to download the file again from an official download mirror. For this case, we can see that the SHA1 hash values match.

Using Kali Linux

You can use Kali Linux in one of the following ways:

- You can run Kali Linux directly from the Live DVD
- You can install Kali Linux on the hard disk and then run it
- You can install Kali Linux on the USB disk (as a portable Kali Linux)

In the following sections, we will briefly describe each of those methods.

Running Kali using Live DVD

If you want to use Kali Linux without installing it first, you can do so by burning the ISO image file to a DVD. After the burn process finishes successfully, boot up your machine with that DVD. You need to make sure that you have set the machine to boot from the DVD.

The advantage of using Kali Linux as a Live DVD is that it is very fast to set up and is very easy to use.

Unfortunately, the Live DVD has several drawbacks; for example, any files or configuration changes will not be saved after the reboot. Additionally, running Kali Linux from the DVD is slow as compared to running Kali Linux from the hard disk because the DVD's reading speed is slower than the hard disk's reading speed.

This method of running Kali is recommended only if you just want to test Kali. However, if you want to work with Kali Linux extensively, we suggest that you install Kali Linux.

Installing on a hard disk

To install Kali Linux on your hard disk, you can choose one of the following methods:

- Installation on a physical/real machine (regular installation)
- Installation on a virtual machine

You can choose whichever method is suitable for you, but we personally prefer to install Kali Linux on a virtual machine.

Installing Kali on a physical machine

Before you install Kali Linux on a physical/real machine, make sure that you install it on an empty hard drive. If your hard drive already has some data on it, that data will be lost during the installation process because the installer will format the hard drive. For easy installation, we suggest that you use all of the available space in the hard disk. If your machine contains another operating system, you need to create a separate disk partition for Kali Linux. Be careful while doing this or you could end up corrupting your operating system.

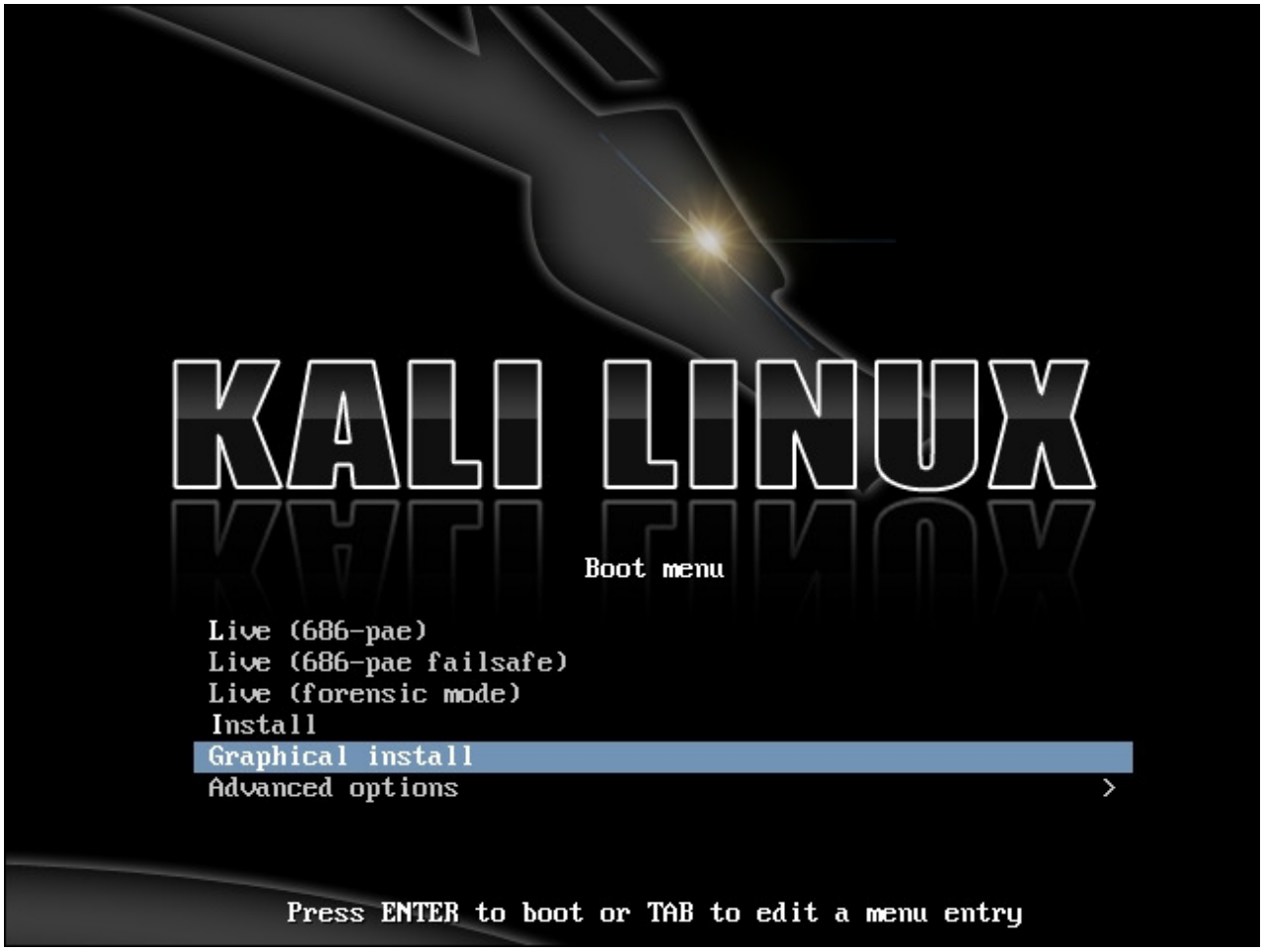
> **Note**
>
> The official Kali Linux documentation that describes how to install Kali Linux with the Windows operating system can be found at http://docs.kali.org/installation/dual-boot-kali-with-windows.

There are several tools that can be used to help you perform disk partitioning. In the open source area, the following Linux Live CDs are available:

- SystemRescueCD (http://www.sysresccd.org/)
- GParted Live (http://gparted.sourceforge.net/livecd.php)
- Kali Linux (http://www.kali.org)

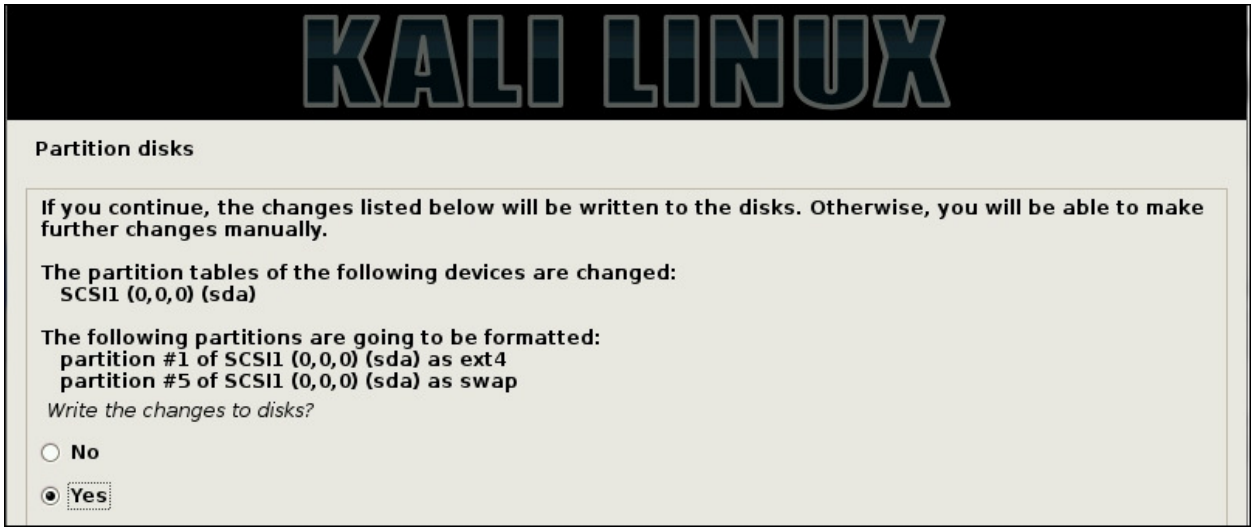
To use the Linux Live CD, you just need to boot it up and you are ready for disk partitioning. Make sure that you back up your data before you use the Linux Live CD disk partitioning tool. Even though they are safe for use in our experience, there is nothing wrong with being cautious, especially if you have important data on the hard disk.

After you are done with the disk partitioning or you just want to use all the hard disk space, you can boot your machine using the Kali Linux Live DVD and select the **Install** or **Graphical install** option when you are prompted with the Kali Linux Live CD menu:



After that, you will see an installation window. You need to set up several things during the installation process:

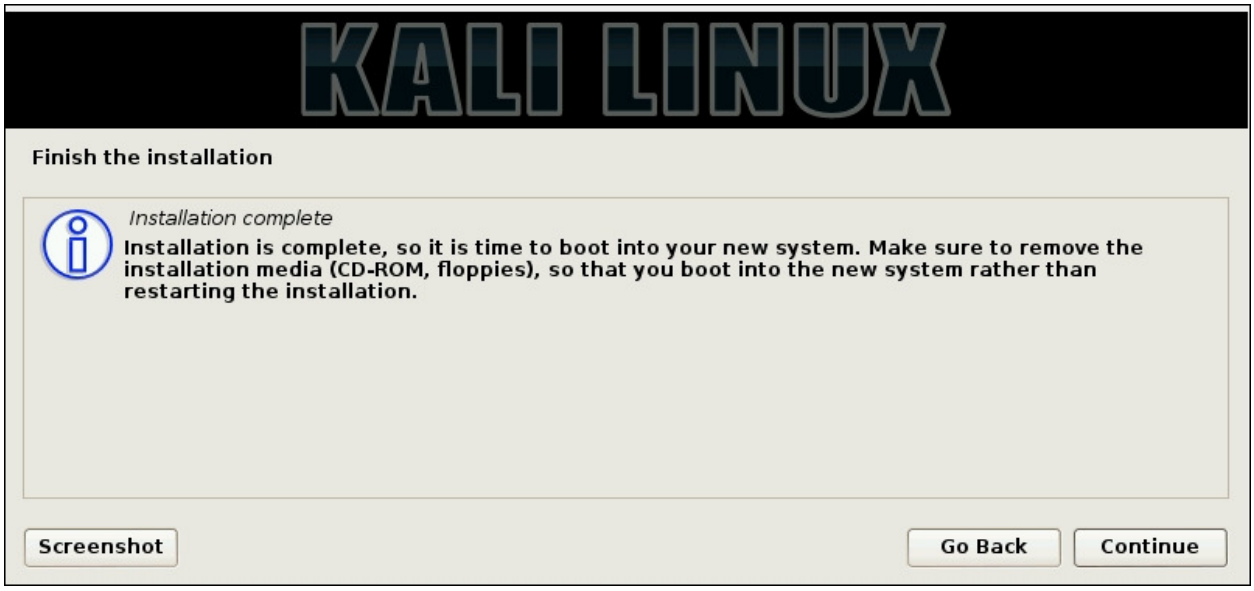
1. First, you need to set the installation language. The default language used is English.
2. Select the country you live in using the drop-down box.
3. Next, set the locale setting. The default value is **United States – en_US.UTF-8**.
4. The keymap value comes next. You can use the suggested keymap value (**American English**) if don't have a specific keyboard layout.
5. Next, you will be asked to configure the network, starting with setting the hostname. Then, you are asked to fill in the domain name.
6. Later on, you will need to set the root password.
7. The installer then asks you to select your time zone.
8. In the disk partitioning segment, the installer will guide you through the disk partitioning process. If you use an empty hard disk, just select the default **Guided - use entire disk** option for better ease. If you have some other operating system installed on your machine, you might first want to create a separate partition for Kali Linux and then select **Manual** in this menu. After you have selected the suitable menu, the installer will create the partition.
9. The installer will ask you about the partitioning scheme; the default scheme is **All files in one partition**. Remember that if you want to store files in the home directory, you should select **Separate /home partition** so that those files won't be deleted if you reinstall the system. The `/home` partition's size really depends on your needs. If you want to put all your data in that directory, you may want a big partition size (more than 50 GB). For average usage, you can go ahead with 10 to 20 GB.
10. The installer will display an overview of your currently configured partitions, as shown in the following screenshot:



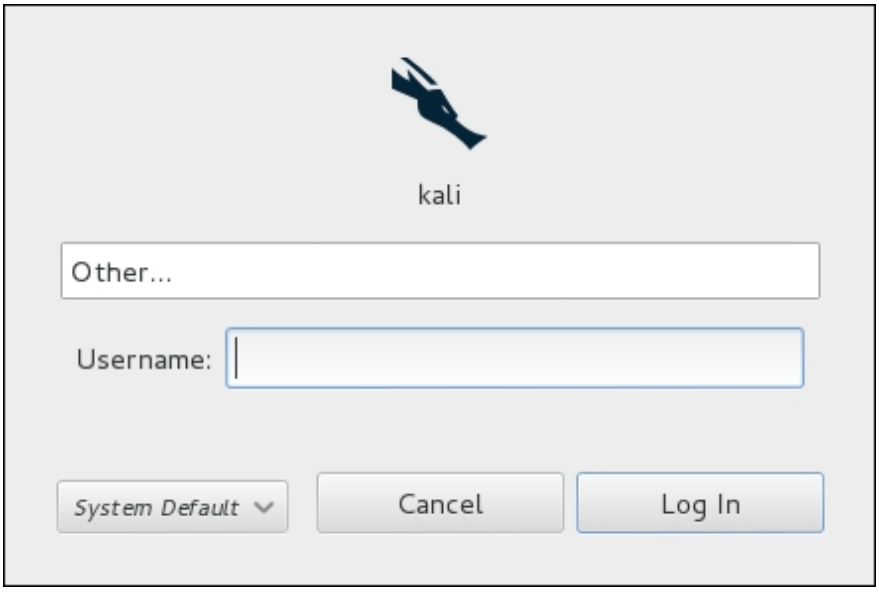
11. Next, the installer will install the Kali Linux system. The installation will be completed in several minutes and you will have Kali Linux installed on your hard disk afterwards. In our test machine, the installation took around 20 minutes.

12. After the installation is finished, the installer will ask you to configure the package manager. Next, it will ask you to install GRUB to the Master Boot Record. You can just choose the default values for these two questions. Beware if you have some other operating system on the same machine, you should *not* choose to install GRUB to the Master Boot Record.

13. If you see the following message, it means that your Kali installation is complete:



14. You can restart the machine to test your new Kali installation by selecting the **Continue** button. After restarting, you will see the following Kali login screen:



15. You can log in using the credentials that you configured in the installation process.

Installing Kali on a virtual machine

You can also install Kali Linux to a virtual machine environment as a guest operating system. The advantages of this type of installation are that you do not need to prepare a separate physical hard disk partition for the Kali Linux image and can use your existing operating system as is.

> **Note**
>
> We will use **VirtualBox** (http://www.virtualbox.org) as the virtual machine software. VirtualBox is an open source virtualization software that is available for Windows, Linux, OS X, and Solaris operating systems.

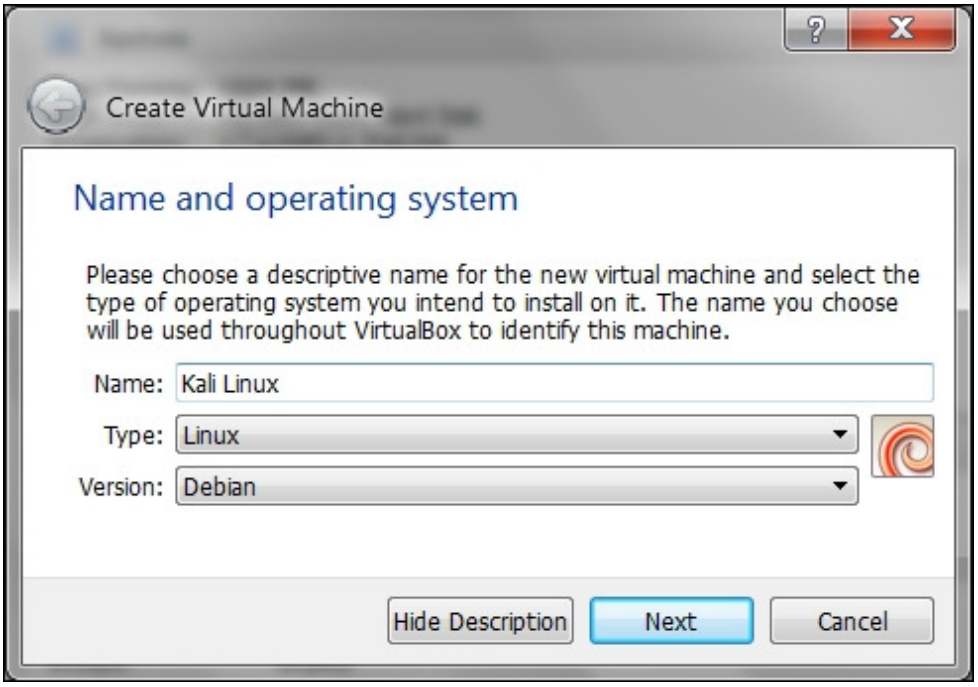
Unfortunately, there is also a disadvantage of running Kali Linux on a virtual machine; it is slower as compared to running Kali Linux on a physical machine.

There are two options that can be utilized for installing Kali Linux on a virtual machine. The first option is to install the Kali Linux ISO image into a virtual machine. This option will take more time compared to the VMware image installation. The advantage of this method is that you can customize your Kali installation.

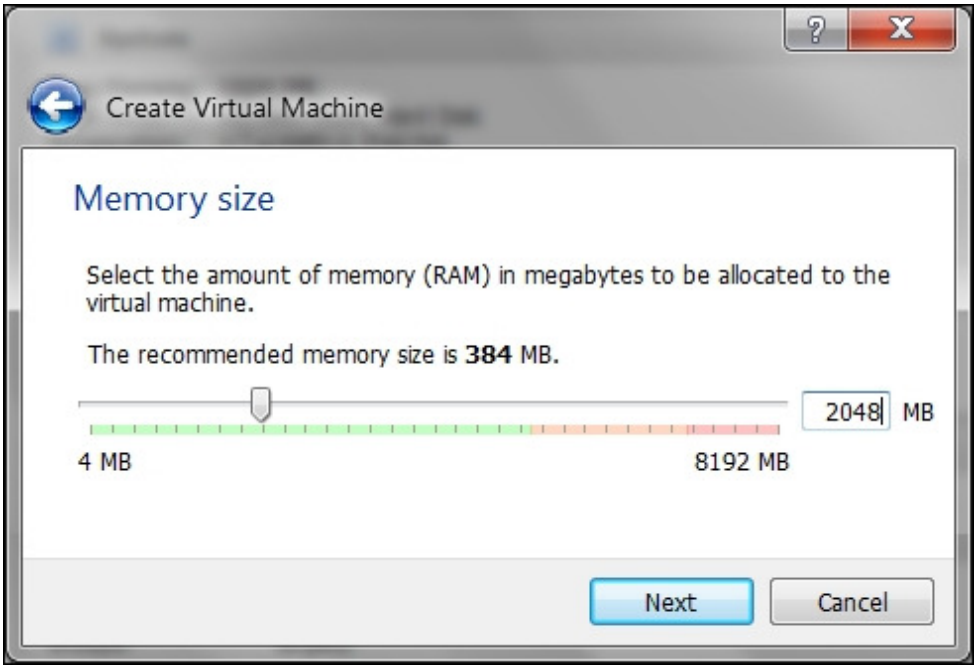
Installing Kali on a virtual machine from the ISO image

To install a Kali Linux ISO image on a virtual machine, the following steps can be used:

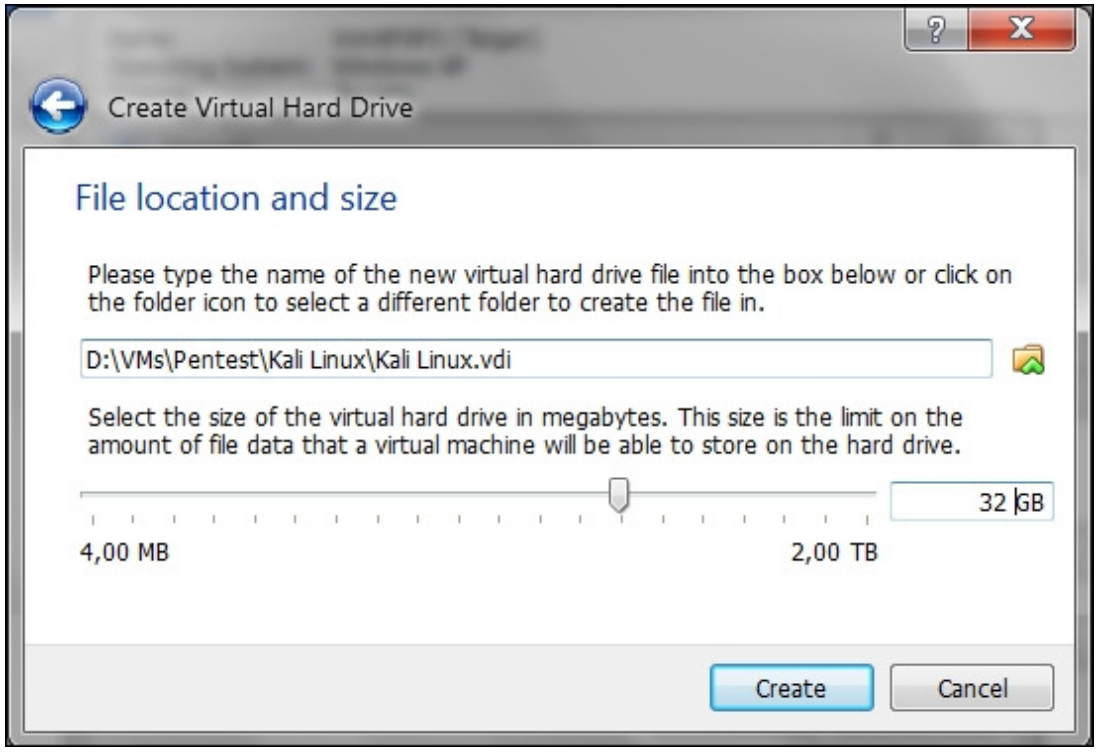
1. Create a new virtual machine by selecting **New** from the VirtualBox toolbar menu.
2. After that, you need to define the virtual machine's name and the operating system's type. Here, we set the VM's name to `Kali Linux` and we choose **Linux** for the OS type and **Debian** for the version:



3. Then, you need to define the VM's base memory size. The more memory you provide, the better the virtual machine will be. Here, we allocated 2048 MB of memory to the Kali Linux virtual machine. Remember that you can't give all of your physical memory to the VM because you still need the memory to run your host operating system:

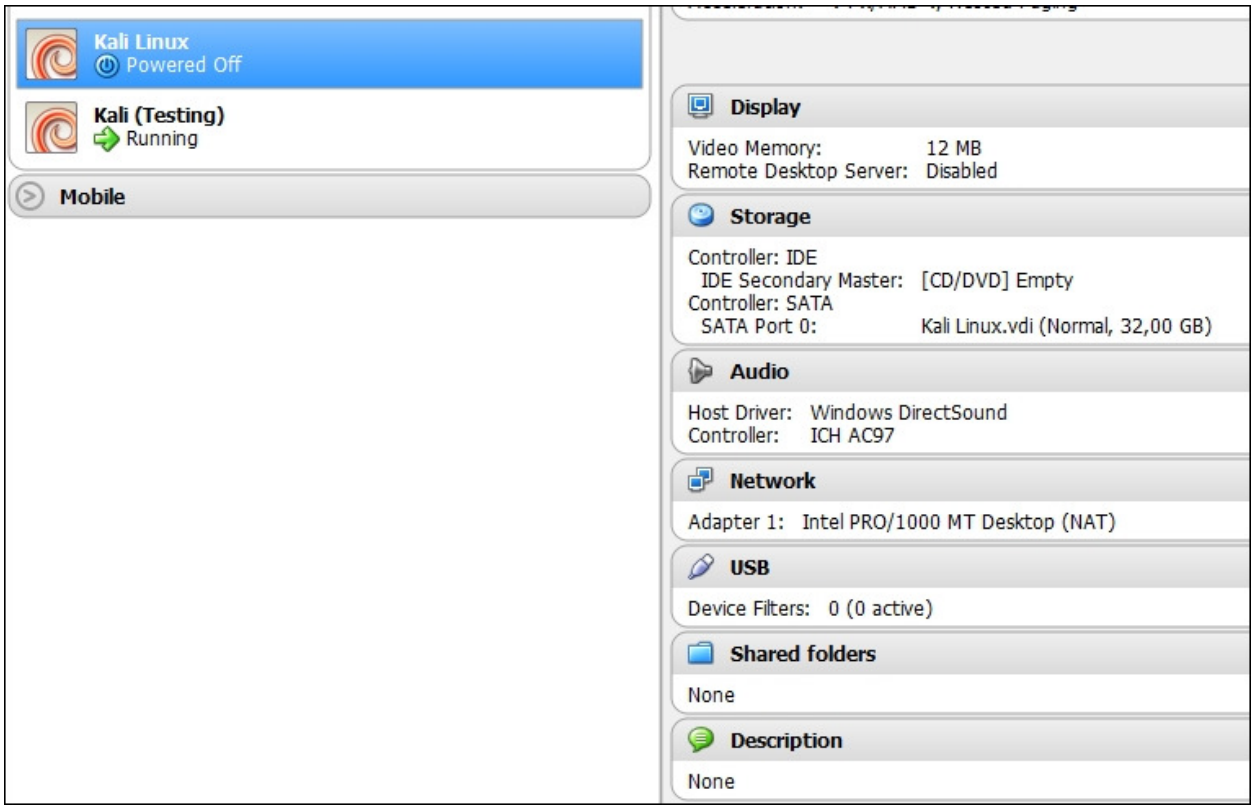


4. Next, you will be asked to create a virtual hard disk. You can just select the VDI as the hard disk type along with a dynamically allocated virtual disk file. We suggest creating at least a 32 GB virtual hard disk. If you want to install some software packages later on, you may want to create a larger virtual hard disk:

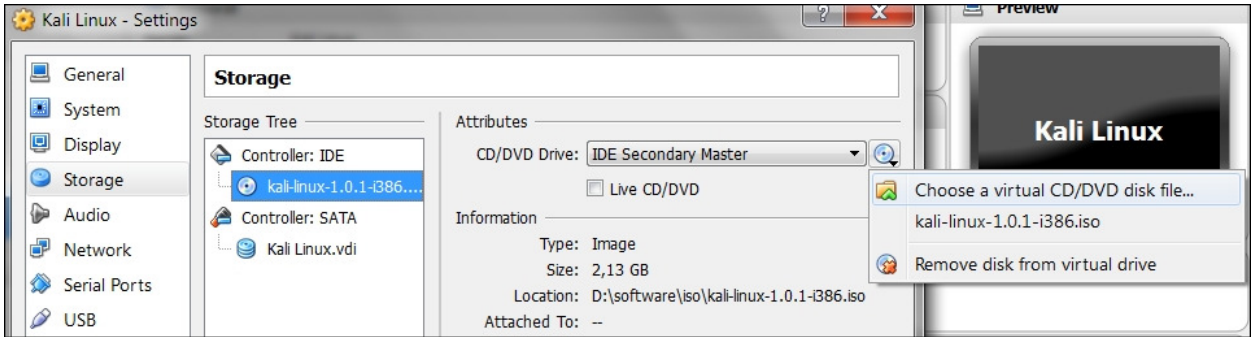


5. After this, your newly created VM will be listed on the VirtualBox menu.

6. To use the Kali Linux ISO image, select the VM from the VirtualBox menu and then click on the **Storage** menu to configure it:



7. From **Storage Tree**, select **IDE Controller** and in the **Attributes**, select Kali Linux ISO image file; in this case the filename for the CD/DVD drive is `kali-linux-1.0.1-i386.iso` . If successful, you will see the ISO image name in the **Controller: IDE** field:



8. To install the Kali Linux ISO image, just run your new virtual machine. You can refer to the *Installing Kali on a physical machine* section for guidance on how to install Kali Linux.

Installing Kali in a virtual machine using the provided Kali VM image

The second option is using the VMWare image provided by Kali Linux.

> **Note**
>
> The Kali Linux team only provides Kali Linux GNOME VMware image for an i386 machine.

With this option, you can install Kali Linux on a virtual machine with ease.

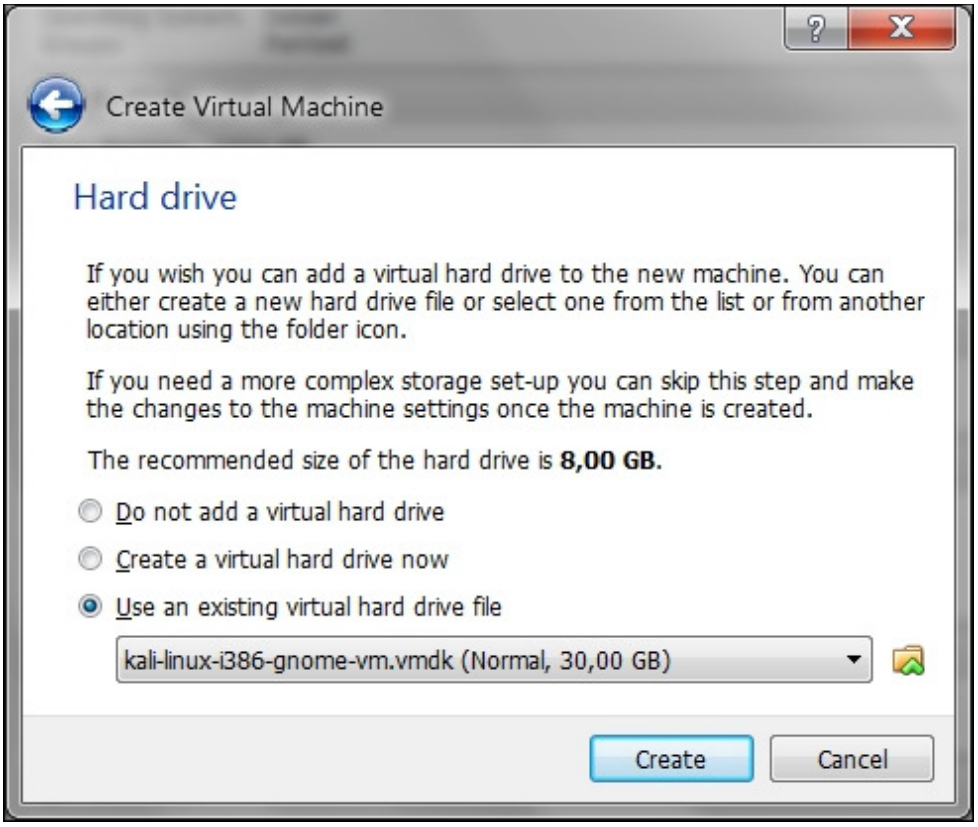
After downloading the Kali Linux VMware image (`kali-linux-1.0-i386-gnome-vm.tar.gz`), you need to verify the SHA1 hash of the downloaded file with the hash value provided in the download page. If the hash value is the same, you can extract the image file to the appropriate folder.

As the VMware image is compressed in the GZ format, you can use any software that can extract a `.gz` file such as gzip or 7-Zip if you use a Windows operating system. If you have extracted it successfully, you will find 21 files in the directory:

kali-linux-i386-gnome-vm	nvram	8.684	11/03/2013 23:25	-a—
kali-linux-i386-gnome-vm	vmdk	1.358	11/03/2013 23:19	-a—
kali-linux-i386-gnome-vm	vmsd	0	09/03/2013 02:59	-a—
kali-linux-i386-gnome-vm	vmx	2.736	11/03/2013 23:25	-a—
kali-linux-i386-gnome-vm	vmxf	382	09/03/2013 03:26	-a—
kali-linux-i386-gnome-vm-s001	vmdk	1.936.130.048	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s002	vmdk	953.548.800	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s003	vmdk	100.007.936	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s004	vmdk	1.101.004.800	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s005	vmdk	586.285.056	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s006	vmdk	337.772.544	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s007	vmdk	830.144.512	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s008	vmdk	565.968.896	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s009	vmdk	390.529.024	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s010	vmdk	299.565.056	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s011	vmdk	196.411.392	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s012	vmdk	364.773.376	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s013	vmdk	203.292.672	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s014	vmdk	294.191.104	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s015	vmdk	1.441.792	11/03/2013 23:36	-a—
kali-linux-i386-gnome-vm-s016	vmdk	65.536	11/03/2013 23:36	-a—

To create the new virtual machine using this VM image file, select **New** from the VirtualBox icon toolbar. Next, you will need to answer the following questions:

1. We use `kali-gnome-vm-32` as the VM name and choose **Linux** as the operating system and **Debian** as the version.
2. We configure the Kali Linux virtual machine to use 2048 MB as its memory size.
3. Next, we define the virtual hard disk to **Use an existing virtual hard drive file**. Then, we select the `kali-linux-i386-gnome-vm.vmdk` file for the hard disk. After that, we choose **Create** to create the virtual machine, as shown in the following screenshot:



Note

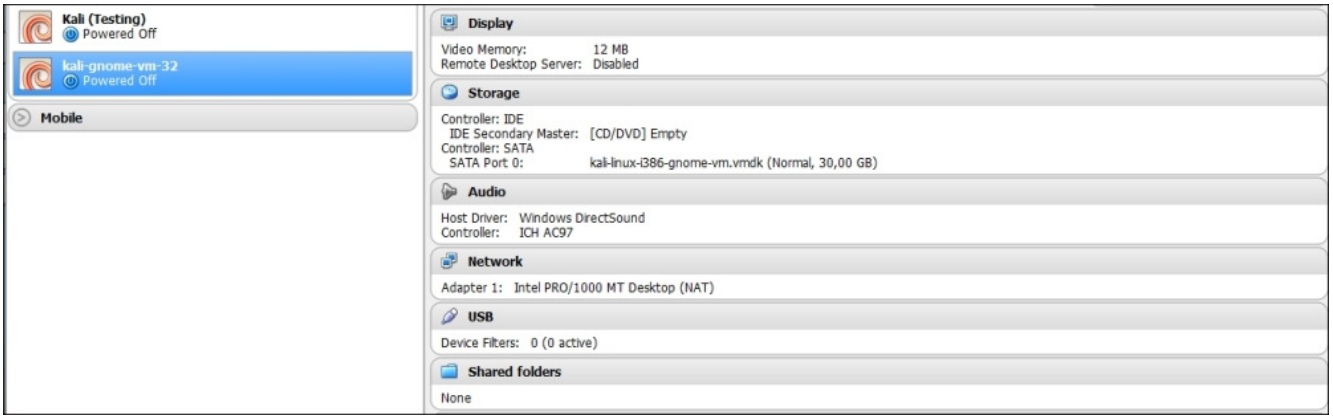
The following is the default configuration of the Kali Linux VMware image:

- Hard disk size: 30 GB
- Network type: NAT
- Username: `root`
- Password: `toor`

For penetration purposes, we should avoid using NAT as the network type. The recommended network type is bridged.

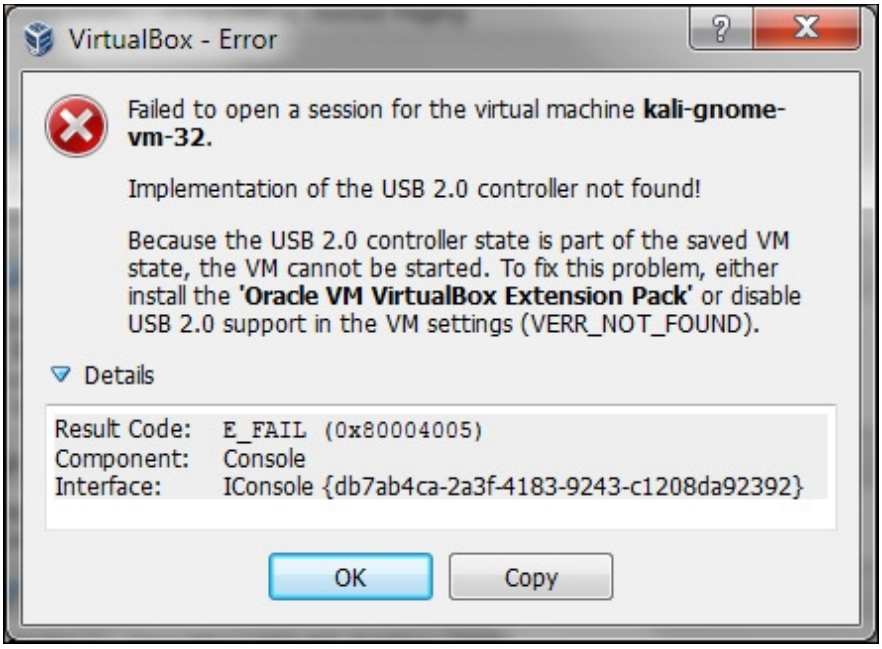
Change the default password for Kali when you configure the Kali VM.

If successful, you will see the new virtual machine in the virtual manager list:



To run the Kali Linux virtual machine, click on the Start icon at the top of the VirtualBox menu bar. After the boot process, Kali Linux will display its login prompt.

If you got the following error message, you need to install the **VirtualBox Extension Pack** . You can get it from http://www.virtualbox.org/wiki/Downloads.

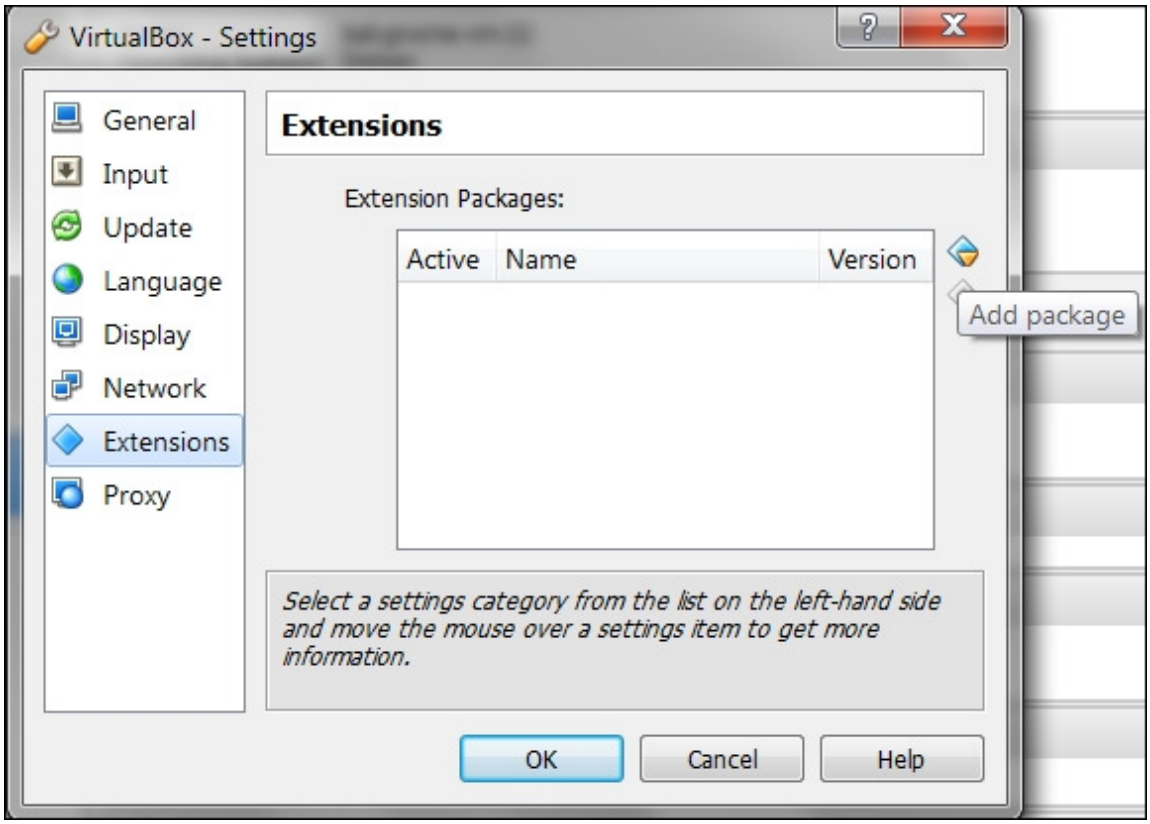


Note

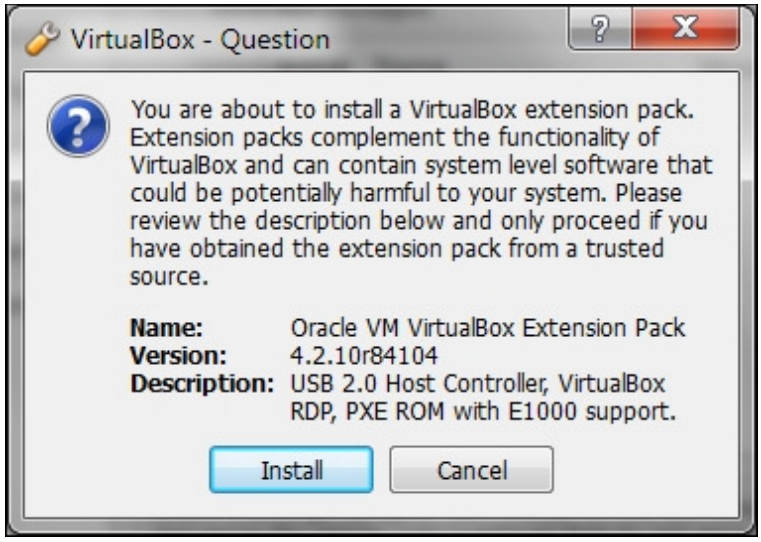
Remember to download the VirtualBox Extension Pack with the same version as the VirtualBox. For example, if you use VirtualBox Version 4.3.0, you should use the Extension Pack Version 4.3.0 too.

To install the extension pack from the VirtualBox Manager, perform the following steps:

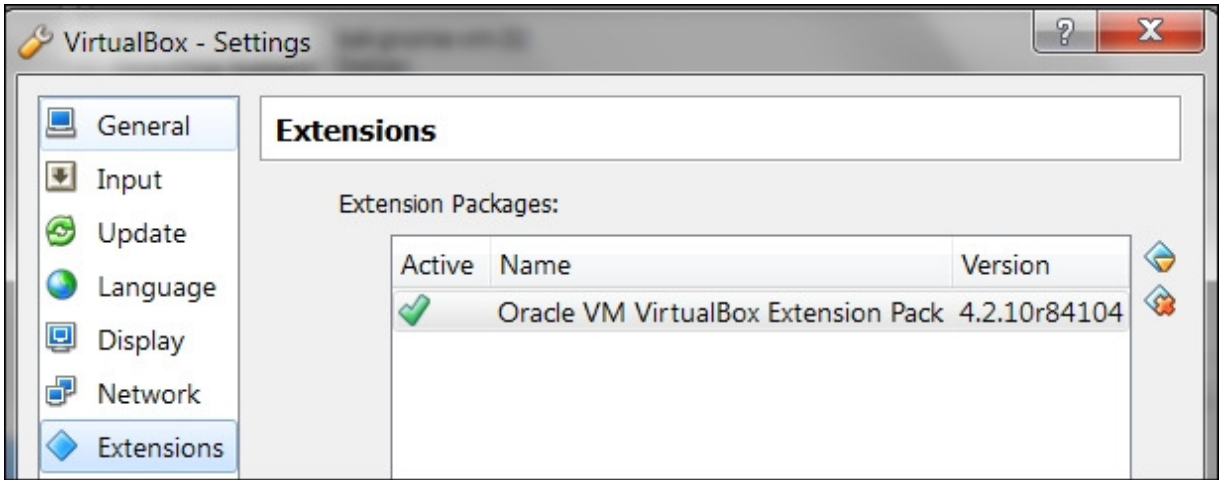
1. Navigate to **File** | **Preferences**; it will then display the **Settings** window. Next, select the **Extensions** menu:



2. Click on the **Add package** button to select the VirtualBox Extension Pack. VirtualBox will then display a pop-up window that will ask you to review the description and then proceed:



3. Select **Install** to install the extension pack and follow the given instructions. If the installation is successful, you will see the extension pack in the list:



4. You can then log in to Kali Linux using the default username and password.

Installing Kali on a USB disk

The third option to use Kali Linux is by installing it to a USB flash disk; we call this method **Portable Kali Linux** . According to the official Kali documentation, this is the Kali developers' favorite and fastest method of booting and installing Kali. Compared to the hard disk installation, you can run Kali Linux using any computer that supports booting from the USB flash disk with this method.

> **Note**
>
> The installation procedure for the USB flash disk is also applicable to the installation of memory cards (SSD, SDHC, SDXC, and so on).

There are several tools available to create portable Kali Linux. One of them is **Rufus** (http://rufus.akeo.ie/). This tool can be run only from a Windows operating system.

You can use other tools to create a bootable disk from the ISO image, such as:

- **Win32DiskImager** (https://launchpad.net/win32-image-writer)
- **Universal USB Installer** (http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/)
- **Linux Live USB Creator** (http://www.linuxliveusb.com)

Before creating portable Kali Linux, you need to prepare a couple of things:

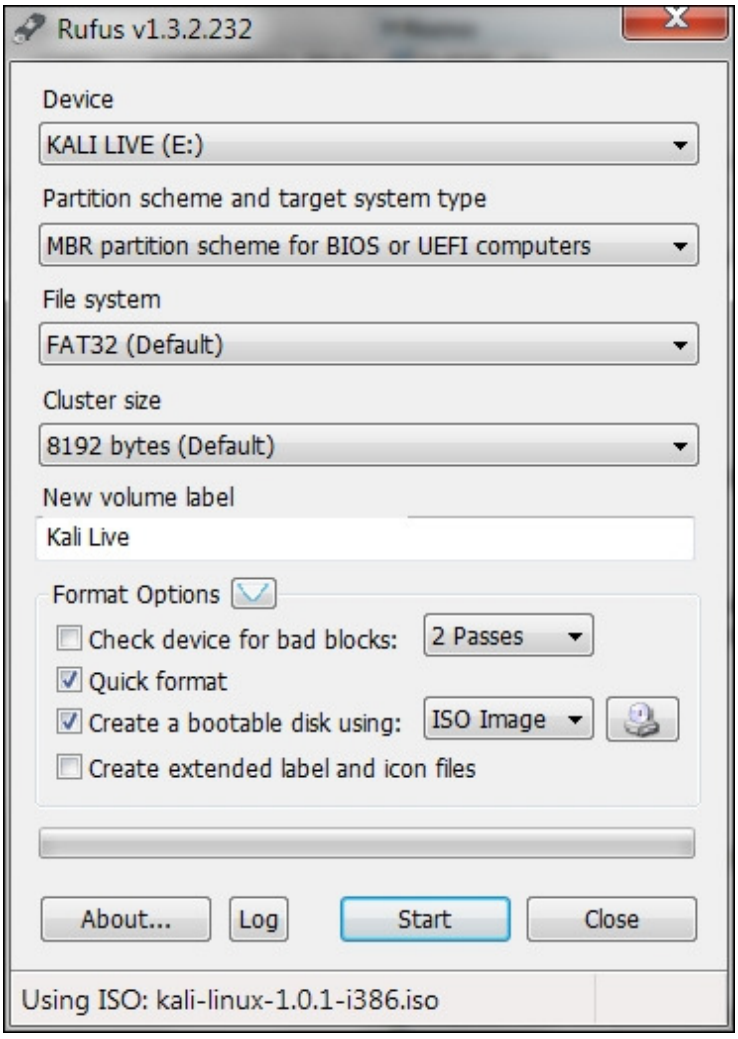
- **Kali Linux ISO image**: Even though you can use the portable creator tool to download the image directly while making the Kali Linux portable, we think it's much better to download the ISO first and then configure Rufus to use the image file.
- **USB flash disk**: You need an empty USB flash disk with enough space on it. We suggest using a USB flash disk with a minimum size of 16 GB.

After downloading Rufus, you can run it on your Windows computer by double-clicking on the `rufus.exe` file. You will then see the Rufus window.

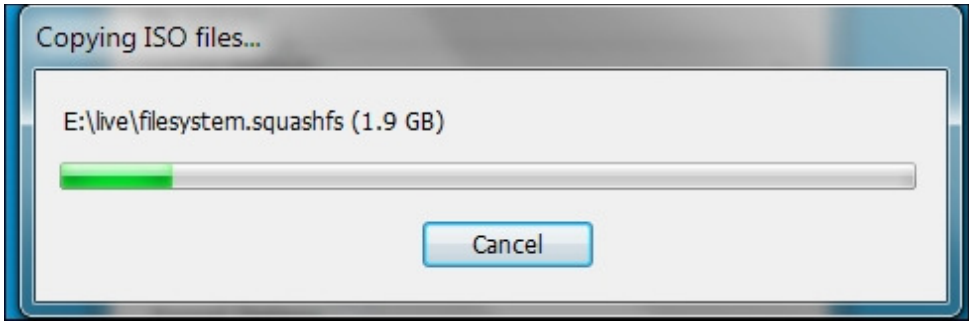
> **Note**
>
> If you use a UNIX-based operating system, you can create the image using the `dd` command. The following is an example of imaging:
>
> ```
> dd if=kali-linux-1.0.1-i386.iso of=/dev/sdb bs=512k
> ```
>
> Here, `/dev/sdb` is your USB flash disk.

To create a bootable Kali USB flash disk, we need to fill in the following options:

- For **Device**, we choose the location of the USB flash disk. In my case, it is the E drive in my Windows system.
- For **Partition scheme and target system type**, set it to **MBR partition scheme for BIOS or UEFI computers**.
- In the **Create a bootable disk using** option, set the value to **ISO image** and select the ISO image using the disk icon:



Click on **Start** to create the bootable image:



After the process is complete, save all your work first and then reboot your system if you want to try the USB flash disk right away. You may want to configure your **Basic Input Output System** (**BIOS**) to boot it from the USB disk. If there is no error, you can boot up the Kali Linux from the USB flash disk.

Note

If you want to add persistence capabilities to the USB flash disk, you can follow the steps described in the documentation section **Adding Persistence to Your Kali Live USB** located at http://docs.kali.org/installation/kali-linux-live-usb-install.

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.

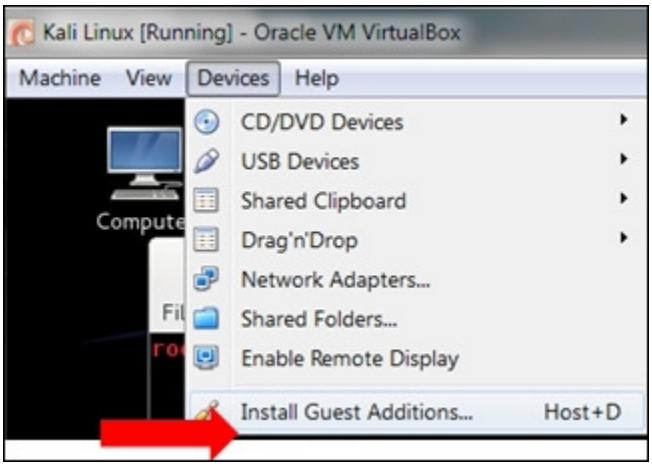
VirtualBox guest additions

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:

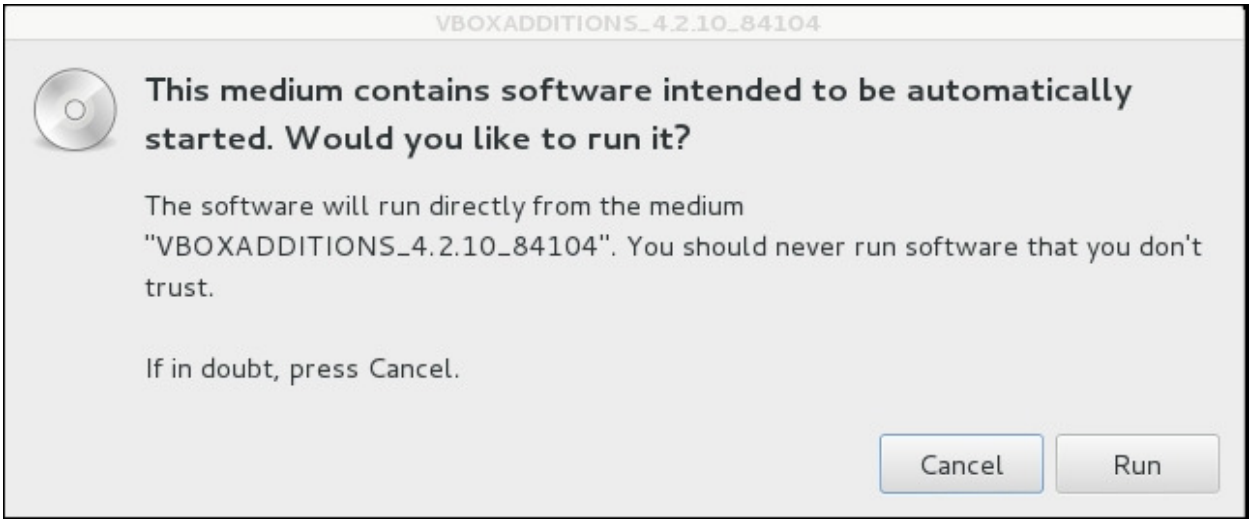
- It will enable the virtual machine to be viewed in full screen
- It will make the mouse move faster in the virtual machine
- It will enable you to copy and paste the text between the host and guest machine
- It will enable the guest and host machine to share folders

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

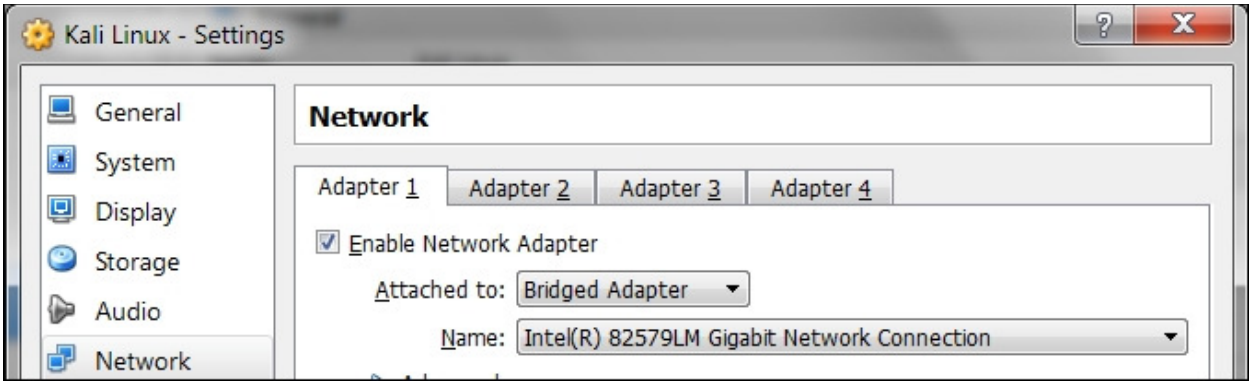
In the following section, we will discuss how to set up the networking in Kali Linux for the wired and wireless network.

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:

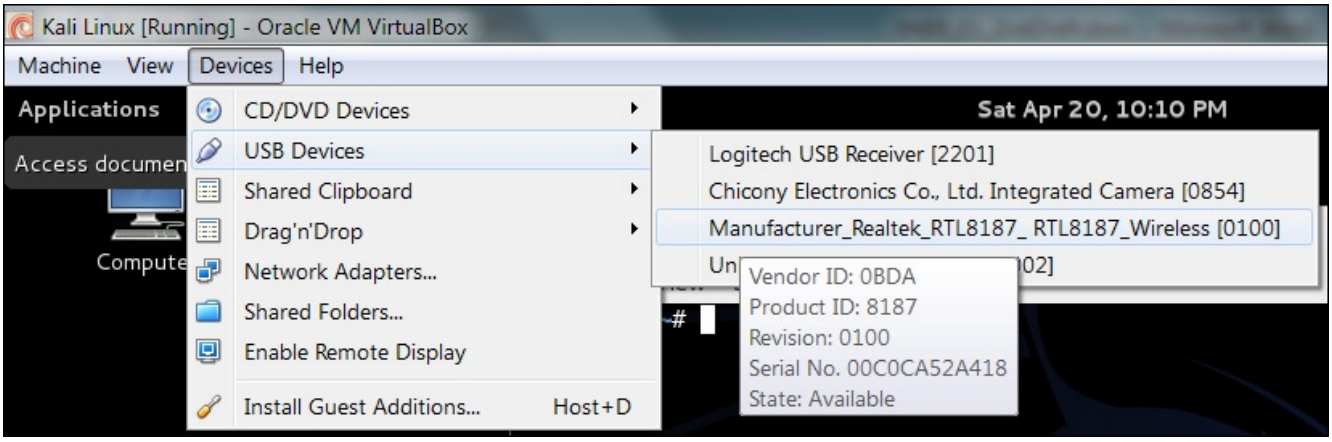
```
auto eth0
iface eth0 inet static
address 10.0.2.15
netmask 255.255.255.0
network 10.0.2.0
broadcast 10.0.2.255
gateway 10.0.2.2
```

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:

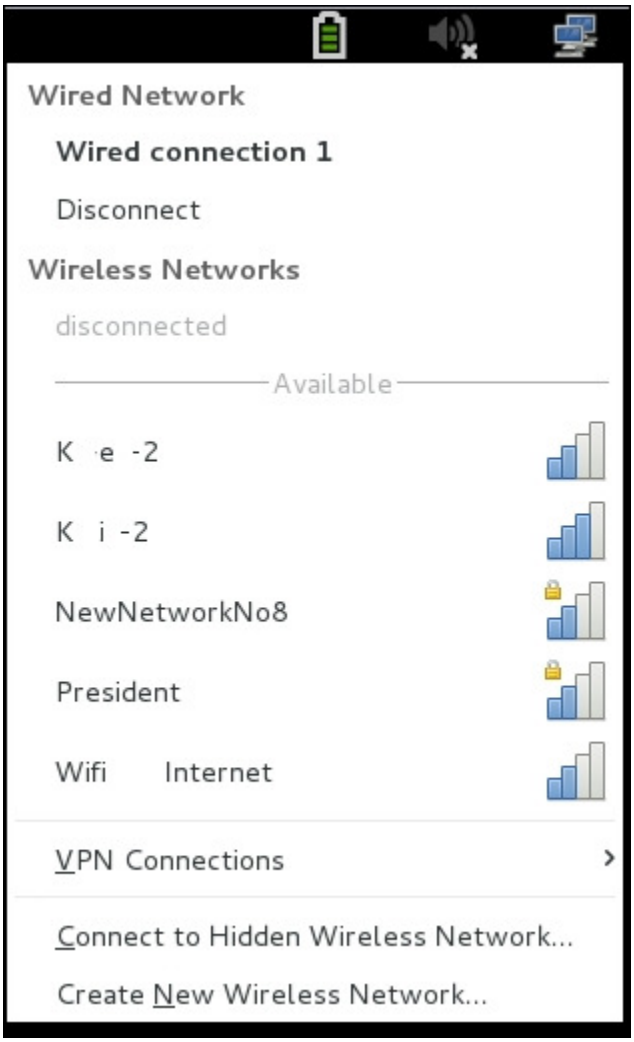


In this screenshot, we select the wireless card that uses the Realtek chipset.

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:

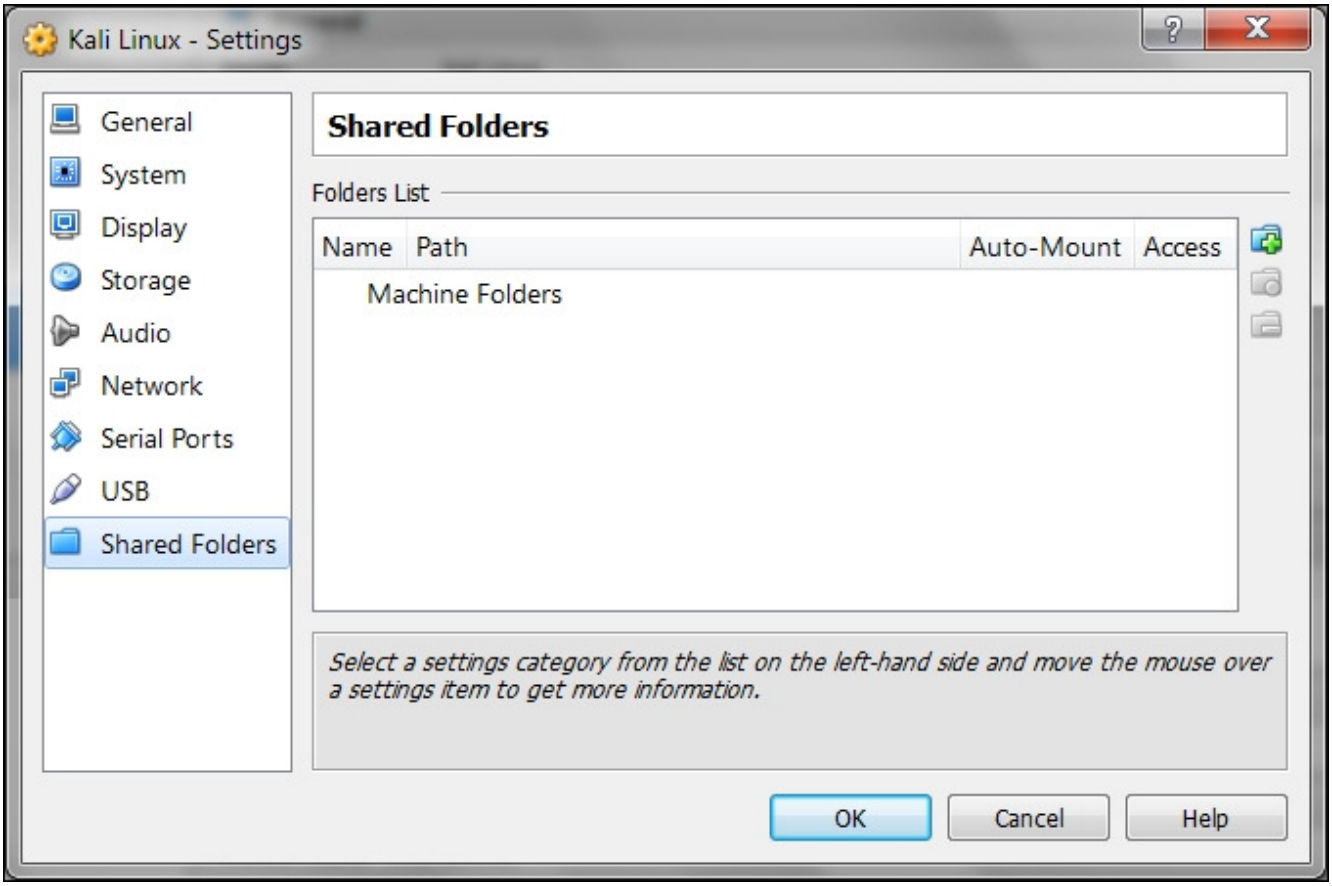
```
update-rc.d networking defaults
```

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**.

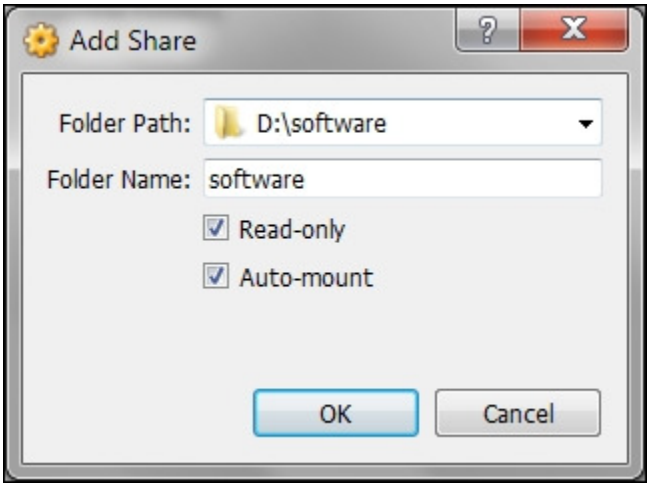
To configure the shared folder from the VirtualBox menu, you need to power off the virtual machine that you want to configure. After that, you need to select the appropriate guest machine's name and click on the **Shared Folders** menu in the window on the left. You will then see the following screen:



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:



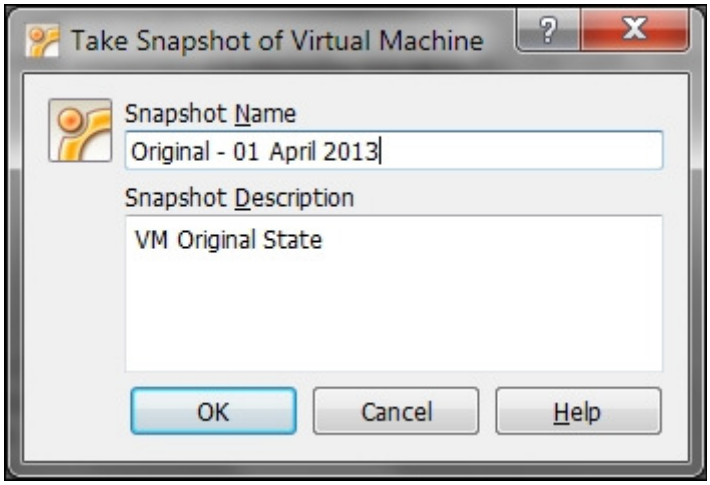
In the preceding screenshot, we shared a **D:\software** folder to the guest OS as a read-only folder.

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:



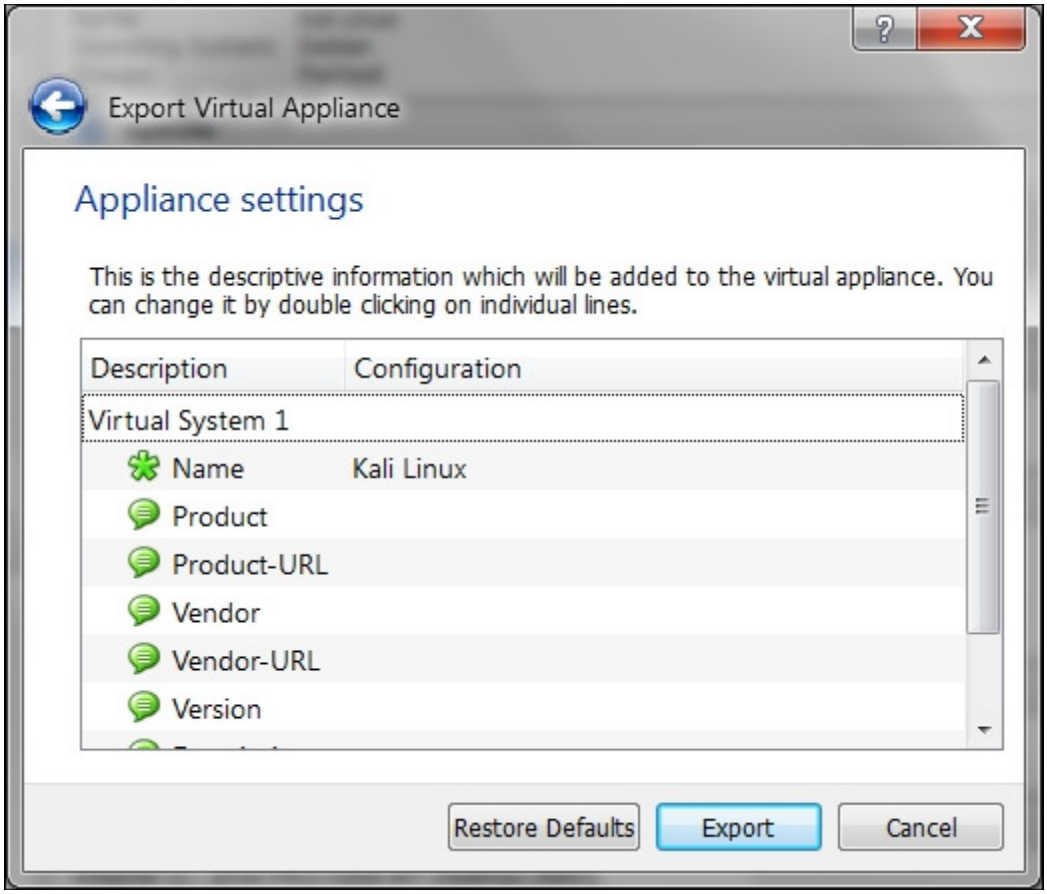
For the **Snapshot Name**, you can use any name but we suggest that you put in the information about the date. You can give detailed information in the **Snapshot Description** field. After you fill in all the information, VirtualBox will store the virtual machine state; this process will take some time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

Updating Kali Linux

Kali Linux consists of hundreds of pieces of application software and an operating system kernel. You may need to update the software if you want to get the latest features.

We suggest that you only update the software and kernel from the Kali Linux software package repository.

The first thing to do after you have successfully installed and configured Kali Linux is to update it. As Kali is based on Debian, you can use the Debian command (`apt-get`) for the updating process.

The `apt-get` command will consult the `/etc/apt/sources.list` file to get the update servers. You need to make sure that you have put the correct servers in that file.

The default `sources.list` file included in Kali Linux contains the following entries:

```
# deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386
LIVE/INSTALL Binary 20130315-11:39]/ kali contrib main non-free

#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386
LIVE/INSTALL Binary 20130315-11:39]/ kali contrib main non-free

deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib

## Security updates
deb http://security.kali.org/kali-security kali/updates main contrib
non-free
```

You need to synchronize the package's index files from the repository specified in the `/etc/apt/sources.list` file before you can perform the update process. The following is the command for this synchronization:

```
apt-get update
```

Make sure that you always run `apt-get update` before performing a software update or installation in Kali.

After the package index has been synchronized, you can perform software updates.

There are two command options that are available to perform an upgrade:

- `apt-get upgrade` : This command will upgrade all of the packages that are currently installed on the machine to the latest version. If there is a problem in upgrading a package, that package will be left intact in the current version.
- `apt-get dist-upgrade` : This command will upgrade the entire Kali Linux distribution; for example, if you want to upgrade from Kali Linux 1.0.1 to Kali Linux 1.0.2, you can use this command. This command will upgrade all of the packages that are currently installed and will also handle any conflicts during the upgrade process; however, some specific action may be required to perform the upgrade.

After you choose the appropriate command option to update Kali Linux, the `apt-get` program will list all of the packages that will be installed, upgraded, or removed. The `apt-get` command will then wait for your confirmation.

If you have given the confirmation, the upgrade process will start. Beware, the upgrade process might take a long time to finish depending on your Internet connection speed.

Network services in Kali Linux

There are several network services available in Kali Linux; in this section, we will describe only some of them: the HTTP, MySQL, and SSH service. You can find the other services by navigating to **Kali Linux** | **System Services**.

HTTP

In your penetration testing works, you may want to have a web server for various reasons, such as to serve malicious web application scripts. In Kali Linux, there is already an Apache web server installed; you just need to start the service.

The following are the steps that are required to activate your HTTP server in Kali Linux:

1. To start the **Apache HTTP** service from the graphical menu, navigate to **Kali Linux** | **System Services** | **HTTPD** | **apache2 start**; or, from the command line, type the following command to start the Apache server:

```
service apache2 start
```

2. If there are no errors, the system will reply with the following message:

```
[....] Starting web server: apache2 ok
```

3. After this, you can browse to the web page; it will display the **It works!** page by default:

To stop the Apache HTTP service, perform the following steps:

1. From the menu, navigate to **Kali Linux** | **System Services** | **HTTPD** | **apache2 stop**; or, from the command line, type the following command to start the Apache server:

```
service apache2 stop
```

2. If there are no errors, the system will reply with the following message:

```
[....] Stopping web server: apache2 [ ok waiting .
```

3. Remember that the previous command will not survive the boot up. After the boot up, you need to give the command again. Fortunately, there is a way to start the Apache HTTP service automatically after the Kali Linux boots up by giving the following command:

```
update-rc.d apache2 defaults
```

   The command will add the apache2 service to be started on boot up.

MySQL

The second service that we will discuss is **MySQL**. It is one of the relational database systems. MySQL is often used with the PHP programming language and Apache web server to create a dynamic, web-based application. For the penetration testing process, you can use MySQL to store your penetration testing

results; for example, the vulnerability information and network mapping result. Of course, you need to use the application to store those results.

To start the MySQL service in Kali Linux, you can perform the following steps:

1. In the graphical menu, navigate to **Kali Linux** | **System Services** | **MySQL** | **mysql start**; or, from the command line, type the following:

```
service mysql start
```

2. Then, the system will respond with the following message:

```
[ ok ] Starting MySQL database server: mysqld . . ..
[info] Checking for tables which need an upgrade, are corrupt or were
not closed cleanly..
```

3. To test whether your MySQL has already started, you can use the MySQL client to connect to the server. We define the username (`root`) and the password to log in to the MySQL server:

```
mysql -u root –p
```

4. The system will respond with the following:

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 42
Server version: 5.5.30-1 (Debian)
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type ''help;'' or ''\h'' for help. Type ''\c'' to clear the current
input statement.

mysql>
```

5. After this MySQL prompt, you can give any SQL commands. To exit from MySQL, just type `quit` .

> **Note**
>
> By default, for security reasons, the MySQL service in Kali Linux can be accessed only from a local machine. You can change this configuration by editing the `bind-address` stanza in the MySQL configuration file located in `/etc/mysql/my.cnf` . We don't recommend that you change this behavior unless you want your MySQL to be accessed from other machines.

To stop the MySQL service, you can perform the following steps:

1. In the graphical menu, navigate to **Kali Linux** | **System Services** | **MySQL** | **mysql stop**; or, from the command line, type the following:

```
service mysql stop
```

2. Then, the system will respond with the following message:

```
[ ok ] Stopping MySQL database server: mysqld.
```

To start the MySQL service automatically after Kali Linux's boots up, you can give the following command:

```
update-rc.d mysql defaults
```

This command will make the MySQL service start after the boot up.

SSH

For the next service, we will look into the **Secure Shell** (**SSH**). SSH can be used to log in to a remote machine securely; apart from that, there are several other usages of SSH, such as securely transferring a file between machines, executing a command in a remote machine, and X11 session forwarding.

To manage your SSH service in Kali Linux, you can perform the following steps:

1. To start the SSHD service from the graphical menu, navigate to **Kali Linux** | **System Services** | **SSH** | **sshd start**; or, from the command line, type the following:

```
service ssh start
```

2. The system will then respond with the following message:

```
[ ok ] Starting OpenBSD Secure Shell server: sshd.
```

3. To test your SSH, you can log in to the Kali Linux server from another server using a SSH client such as putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/) if you are using the Microsoft Windows operating system.

4. To stop the SSHD service from the graphical menu, navigate to **Kali Linux** | **System Services** | **SSH** | **sshd stop**; or, from the command line, type the following:

```
service ssh stop
```

5. The system will then respond with the following message:

```
[ ok ] Stopping OpenBSD Secure Shell server: sshd.
```

6. To start the SSH service automatically after Kali Linux boots up, you can give the following command:

```
update-rc.d ssh defaults
```

   This command will add the SSH service to be started on boot up.

Installing a vulnerable server

In this section, we will install a vulnerable virtual machine as a target virtual machine. This target will be used in several chapters of the book when we explain particular topics. The reason we chose to set up a vulnerable server in our machine instead of using vulnerable servers available on the Internet is because we don't want you to break any laws. We should emphasize that you should never pen test other servers without written permission. Another purpose of installing another virtual machine would be to improve your skills in a controlled manner. This way, it is easy to fix issues and understand what is going on in the target machine when attacks do not work.

In several countries, even port scanning a machine that you don't own can be considered a criminal act. Also, if something happens to the operating system using a virtual machine, we can repair it easily.

The vulnerable virtual machine that we are going to use is **Metasploitable 2** . This vulnerable system is created by the famous HD Moore of Rapid7.

> **Note**
>
> There are other deliberately vulnerable systems besides Metasploitable 2 that you can use for your penetration testing learning process, as can be seen on the following site: http://www.felipemartins.info/2011/05/pentesting-vulnerable-study-frameworks-complete-list/.

Metasploitable 2 has many vulnerabilities in the operating system, network, and web application layers.

> **Note**
>
> Information about the vulnerabilities contained in Metasploitable 2 can be found on the Rapid7 site at https://community.rapid7.com/docs/DOC-1875.

To install Metasploitable 2 in VirtualBox, you can perform the following steps:

1. Download the Metasploitable 2 file from http://sourceforge.net/projects/metasploitable/files/Metasploitable2/.
2. Extract the Metasploitable 2 ZIP file. After the extraction process is completed successfully, you will find five files:
    - `Metasploitable.nvram`
    - `Metasploitable.vmdk`
    - `Metasploitable.vmsd`
    - `Metasploitable.vmx`
    - `Metasploitable.vmxf`
3. Create a new virtual machine in VirtualBox. Set **Name** to `Metasploitable2` , **Operating System** to **Linux**, and **Version** to **Ubuntu**.
4. Set the memory to **1024MB**.
5. In the **Virtual Hard Disk** setting, select **Use existing hard disk**. Choose the Metasploitable files that we have already extracted in the previous step:

6. Change the network setting to **Host-only adapter** to make sure that this server is accessible only from the host machine and the Kali Linux virtual machine. The Kali Linux virtual machine's network setting should also be set to **Host-only adapter** for pen-testing local VMs.

7. Start the Metasploitable 2 virtual machine. After the boot process is finished, you can log in to the Metasploitable 2 console using the following credentials:

   - Username: `msfadmin`
   - Password: `msfadmin`

8. The following is the Metasploitable 2 console after you have logged in successfully:

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Jun 30 23:52:28 EDT 2012 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Installing additional weapons

Although the latest version of Kali Linux always comes with many security tools, sometimes you need to add additional software tools due to the following reasons:

- The latest version of the tool has not been included in Kali Linux yet
- You want to have the latest version of the software that is not available in the Kali Linux repository

Our suggestion is to try to search for the software package in the repository first. If you can find the package in the repository, just use that package. However, if you can't find it in the repository, you may want to get the software package from the author's website and install it yourself.

Based on our experience, we suggest that you use the software in the repository as much as you can to ease the package management process.

There are several package management tools that can be used to help you manage the software package in your system, such as `dpkg`, `apt`, and `aptitude`. Kali Linux comes with `dpkg` and `apt` installed by default.

> **Note**
>
> If you want to find out more about the `apt` and `dpkg` command, you can go through the following references: https://help.ubuntu.com/community/AptGet/Howto/ and http://www.debian.org/doc/manuals/debian-reference/ch02.en.html.

In this section, we will briefly discuss the `apt` command in a practical way that is related to the software package installation process.

To search for a package name in the repository, you can use the following command:

```
apt-cache search <package_name>
```

This command will display the entire software package that has the name `package_name`. For example, let's search for a software package called `nessus`; the following is the command to do that:

```
apt-cache search nessus
```

To display more detailed information about a software package such as its description, size, and version, you can use the following command:

```
apt-cache show <package_name>
```

If you want install the package or upgrade an individual software package, you can use the `apt-get` command to install the package. The following is the basic syntax for `apt-get` to do that:

```
apt-get install <package_name>
```

If you can't find the package in the Kali Linux repository and are sure that the package will not cause any problems in the future, you can install the package manually.

Download the software package only from trusted sources such as the software developer's site. If the developer provides the `.deb` (the Debian package format) packages, you can use the `dpkg` command to install the additional software. If the `.deb` package is not provided, you can install the software from the source code. The actual process may vary but the general steps are usually similar to the following:

1. Extract the software package using archiver programs such as Tar and 7-Zip.
2. Change to the extracted directory.
3. Run the following commands:

```
./configure
make
```

```
make installh
```

In this section, we will provide you with examples on how to install several additional security tools that are not available from the Kali Linux repository. We will give various mechanisms that can be used to install the software:

- Downloading the Debian package and installing it
- Downloading from the source package and installing it

Installing the Nessus vulnerability scanner

As an example, we want to install the latest Nessus vulnerability scanner (Version 5) for the first installation mechanism. We have searched the Kali Linux repository but are unable to find Nessus.

Nessus Version 5 has many new features as compared to Nessus Version 4, such as more flexible results filtering and report creation and simplified policy creation; we chose to use this version instead of Nessus Version 4.

> **Note**
>
> You can find more information about the features and enhancement in Nessus Version 5 from http://www.tenable.com/products/nessus/nessus-product-overview/why-upgrade-to-nessus-5.

We can download the latest Nessus package generated for Debian 6 Linux distribution from the Nessus website (http://www.nessus.org/products/nessus/nessus-download-agreement). To install this package, we issue the following command:

```
dpkg -i Nessus-x.y.z-debian6_i386.deb
```

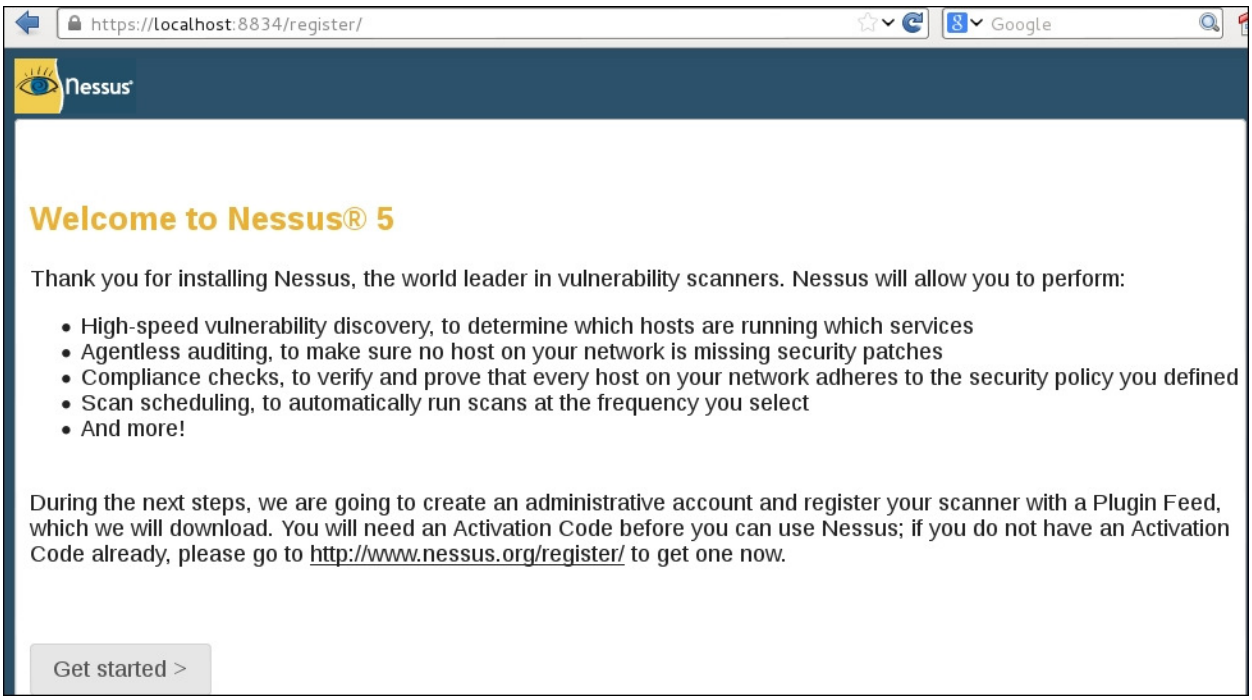
> **Note**
>
> We used `x.y.z` in the previous command to denote the Nessus version number. You need to change those numbers to the Nessus version that you just downloaded successfully.

You can then follow the instructions given on the screen to configure your Nessus server:

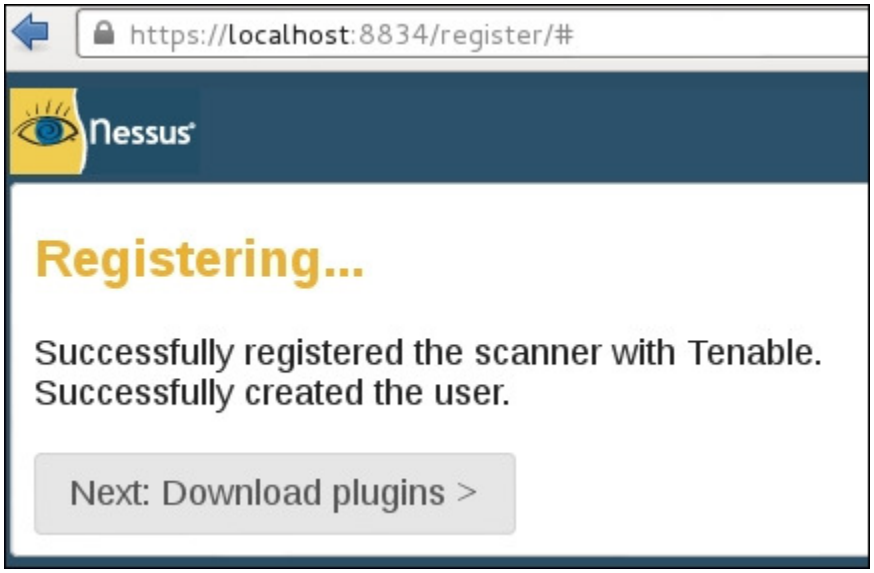
1. Start the Nessus server by typing the following if it has not started yet:

```
/etc/init.d/nessusd start
```

2. Open your browser and connect to `https://localhost:8834`. You will then be prompted with a warning about an invalid SSL certificate used by Nessus. You need to check the SSL certificate and then store the exception for that SSL certificate. The following is the Nessus page that will be shown after you have stored the SSL certificate exception:



3. After that, you will be guided to create a Nessus admin credential. Next, you will be asked to enter your activation code to register the Nessus scanner to Tenable. You need to register at http://www.nessus.org/register/ to obtain the activation code:



4. After you have registered successfully, you will be able to download the newest Nessus plugins. The plugins download process will take some time to complete; you can do something else while waiting for the download process to finish.

Installing the Cisco password cracker

For the second example, we will use a simple program called `cisco_crack` (http://insecure.org/sploits/cisco.passwords.html). This tool is used to crack the Cisco type 7 password.

> **Note**
>
> Cisco type 7 password is a very weak password, so it should not be used anymore. However, for penetration testing, we see that it is still being used, although it's not widespread anymore. This tool will be a help for this occasion.

After downloading the source code, the next step is to compile it. Before you can compile the source code cleanly, you need to add the following `include` statements:

```
#include <string.h>
#include <stdlib.h>
```

Now, you have four `include` statements in the source code.

To compile the code, you can just give the following command:

```
gcc cisco_crack.c -o cisco_crack
```

If there is no error, an executable file with the name of `cisco_crack` will be created. The following is the help screen of `cisco_crack` :

```
# ./cisco_crack  -h
Usage: ./cisco_crack -p <encrypted password>
       ./cisco_crack <router config file> <output file>
```

Summary

This chapter introduced you to the amazing world of Kali Linux, which is a Live DVD Linux distribution that has been specially developed to help you in the penetration testing process. Kali is the successor of BackTrack, a famous Linux distribution focused on the purpose of penetration testing.

The chapter started with a brief description of Kali Linux's history. Next, it moved on to see what functionalities Kali Linux has to offer. The latest version of Kali Linux has many tools to help in penetration testing. Additionally, it also has tools for digital forensics, wireless, reverse engineering, and hardware hacking tasks.

The discussion continues on how to get Kali Linux and the several ways to install it. Kali Linux can be used as a Live DVD without installing it to the hard disk. It can be installed to the hard disk and can also be used as a portable distribution by installing it to a USB flash disk.

Before Kali Linux can be used properly in penetration testing, it needs to be configured for the network connection, using either a wired or wireless connection. We also discussed how to use several features in the VirtualBox machine to make it easier to work with the virtual machine; for example, installing additional tools, configuring shared folders, exporting the virtual machine for a backup purpose or to share it with other people, and taking a snapshot to back up the virtual machine temporarily.

As with any other software, Kali Linux also needs to be updated, whether we only update the software applications or the Linux kernel included in the distribution.

You may need to test your penetration testing skills; unfortunately, you don't have permission to do this to other servers as it is considered illegal in several countries. To help you with this, there are several intentionally vulnerable systems that can be installed and used on your own machine. In this chapter, we looked into Metasploitable 2 from Rapid7.

We also discussed several network services included with the latest Kali Linux, such as HTTP, MySQL, and SSH. We started by giving you a brief introduction to each service and then we continue with how to manage the service; for example, how to start or stop the service.

At the end of the chapter, we looked at installing additional information security tools that are not included in the latest Kali Linux version by default, such as the Nessus network scanner and Cisco password cracker.

In the next chapter, we will introduce you to several penetration testing methodologies.