

3

Setting Up Kali - Part 2

In the previous chapter, we started building our very own penetration testing lab. However, a lab environment is not complete without the installation of two of the most popular operating systems: Microsoft Windows and Ubuntu. As a penetration tester, it's always recommended to practice your skills on both Windows and Linux environments, since both are used in corporate environments by end users, such as employees and executive staff members, on a daily basis. Usually, system administrators don't always install the latest security updates on their employees' systems, which leaves the computers vulnerable to the latest cyber threats. A penetration tester should learn how to perform various attacks on Windows and Linux.

The following topics will be covered in this chapter:

- Installing Windows as a **virtual machine (VM)**
- Installing Ubuntu 8.10
- Troubleshooting Kali Linux

Technical requirements

The following are the technical requirements for this chapter:

- Oracle VM VirtualBox or VMware Workstation Pro
- Microsoft Windows 10
- Microsoft Windows Server 2016
- Ubuntu Desktop
- Ubuntu Server
- Kali Linux

Installing Windows as a VM

Since more organizations use the Windows operating system as the main operating system for their employees' workstation/desktop, you need to understand how to perform a penetration test on the Windows platform.

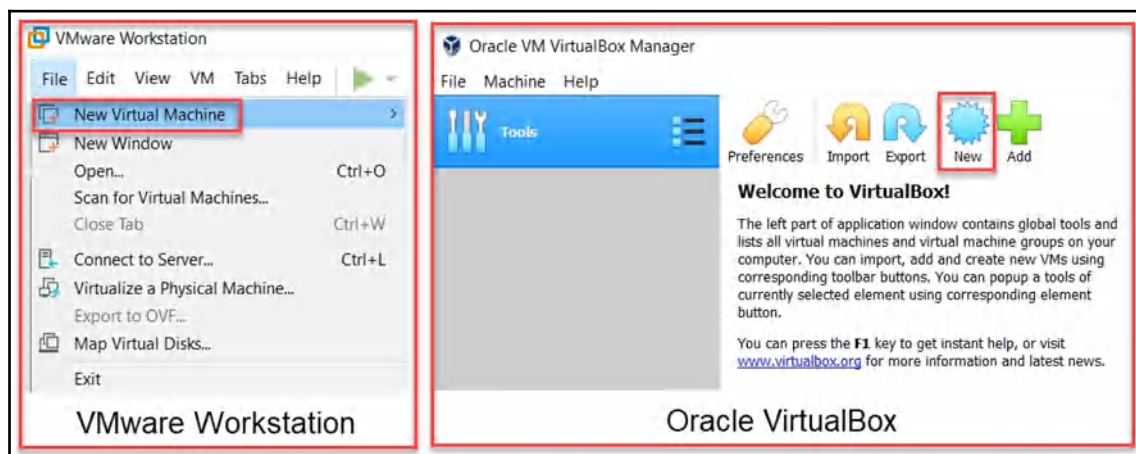
One of the benefits offered by Microsoft is the 90-day trial of their operating systems through the Microsoft Evaluation Center. In this section, I'll demonstrate how to set up a Windows VM in our penetration testing lab:

1. First, you'll need to download the ISO image of Windows 10 and Windows Server 2016 using the following URLs:
 - **Windows 10:** <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>
 - **Windows Server 2016:** <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016>



The installation procedures for Windows Desktop and Windows Server are the same.

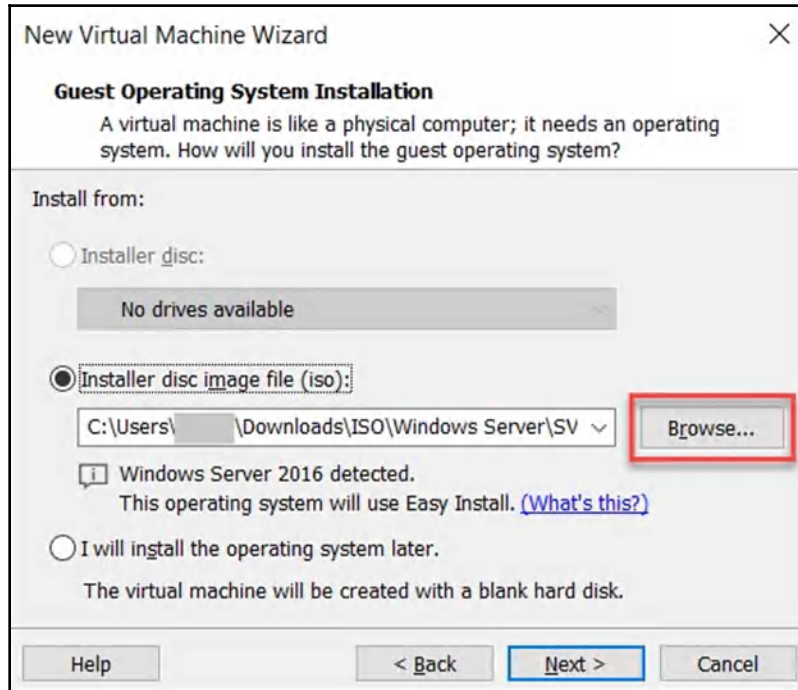
2. Once the ISO file has been downloaded successfully, open your hypervisor and choose **New Virtual Machine**:



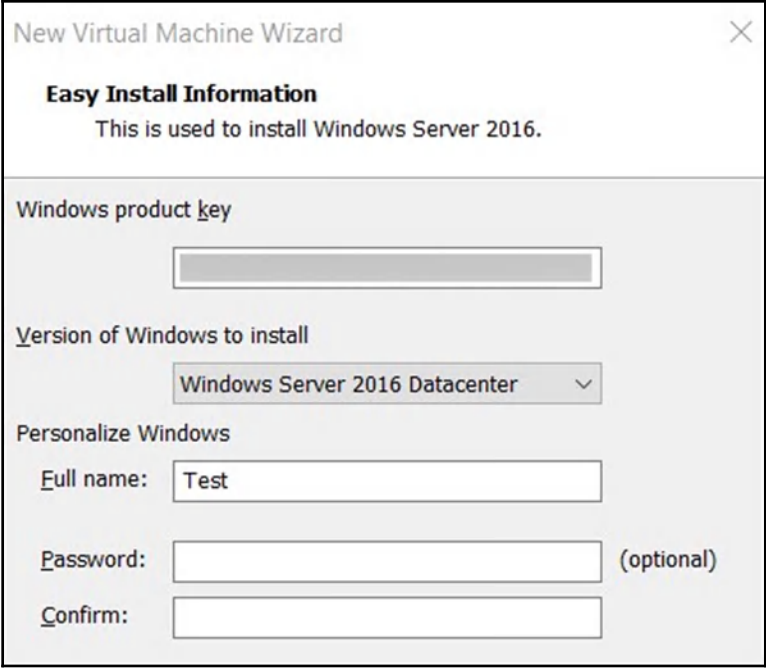
3. If you're using VMware, the **New Virtual Machine Wizard** will prompt you to continue your setup in either the **Typical (recommended)** or **Custom (advanced)** mode. For this exercise, I have chosen the typical option as it comprises a few simple steps:



- Next, choose the **Installer disc image file (iso):** option to add the ISO file by clicking on **Browse**. Once the file has been added successfully, click on **Next** to continue:

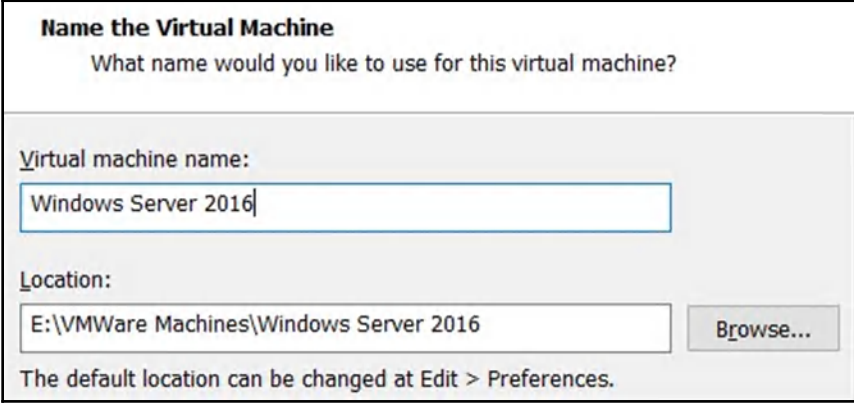


- VMware will present a custom window, allowing you to insert the product key (obtained from the Microsoft Evaluation Center during the registration phase) and create an administrator account during the installation phase. Simply complete the details, use the dropdown box to select the version of the operating system you are about to install, and click on **Next**:



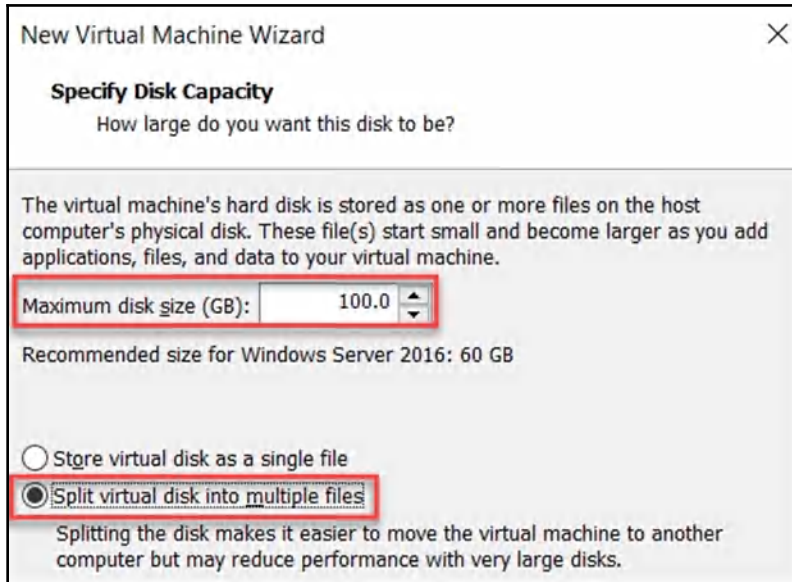
The screenshot shows the 'New Virtual Machine Wizard' window with the 'Easy Install Information' tab selected. The window title is 'New Virtual Machine Wizard' with a close button (X) in the top right corner. Below the title bar, the text 'Easy Install Information' is displayed in bold, followed by 'This is used to install Windows Server 2016.' The form contains several fields: 'Windows product key' with an empty text box; 'Version of Windows to install' with a dropdown menu showing 'Windows Server 2016 Datacenter'; 'Personalize Windows' section with 'Full name:' set to 'Test', 'Password:' (optional) with an empty box, and 'Confirm:' with an empty box.

6. Next, you'll have the option to name the VM and choose a location to store its configurations. This step can be left as the default setting:



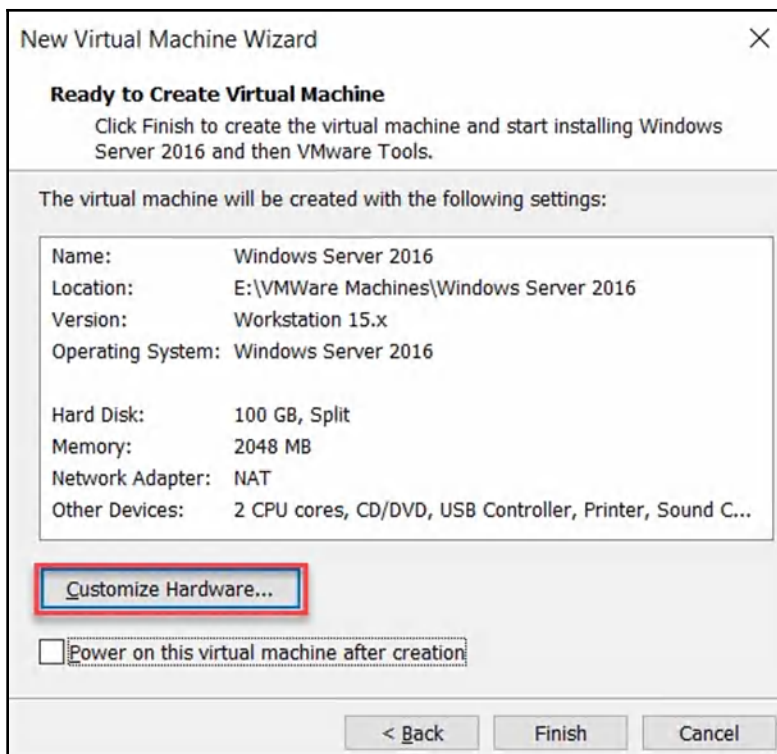
The screenshot shows the 'Name the Virtual Machine' window. The title is 'Name the Virtual Machine' and the subtitle is 'What name would you like to use for this virtual machine?'. The form contains: 'Virtual machine name:' with a text box containing 'Windows Server 2016'; 'Location:' with a text box containing 'E:\VMWare Machines\Windows Server 2016' and a 'Browse...' button; and a note at the bottom: 'The default location can be changed at Edit > Preferences.'

- Next, you'll have the option to create a new virtual hard disk for the Windows VM. I have chosen its size to be 100 GB and to split its files into multiple pieces for easier portability:



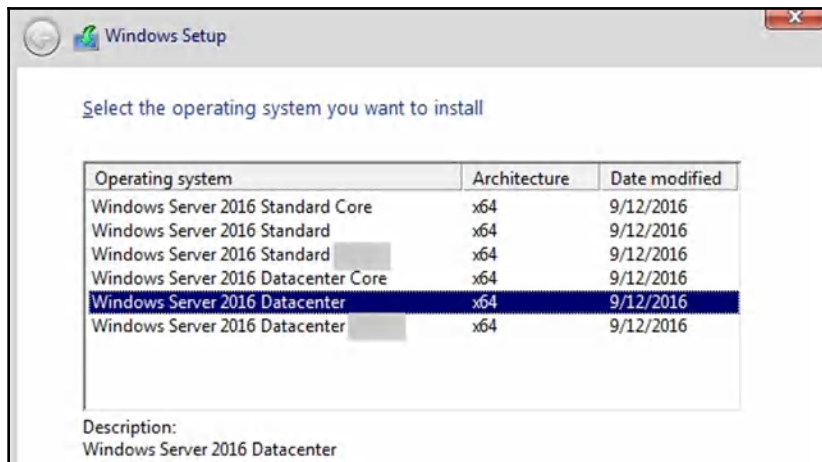
You can choose any size for the hard disk, as long as it's the recommended size or above. The system requirements can be found at <https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements>.

- The final window will show you a summary of the configurations. You can customize the hardware resources by clicking on the **Customize Hardware...** option:

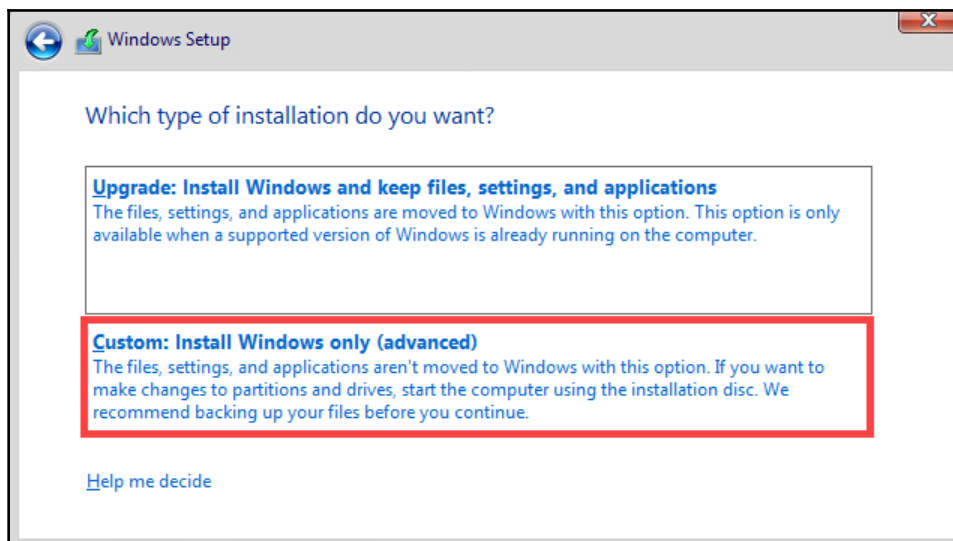


9. Upon clicking **Finish**, the Windows 10/Server 2016 VM will appear in your library. You can also modify the hardware configurations when the VM is powered off.
10. Now, it's time to power on the Windows VM. Ensure that you choose your corresponding language, time, and keyboard format.
11. Choose the **Install now** option to begin the installation phase.

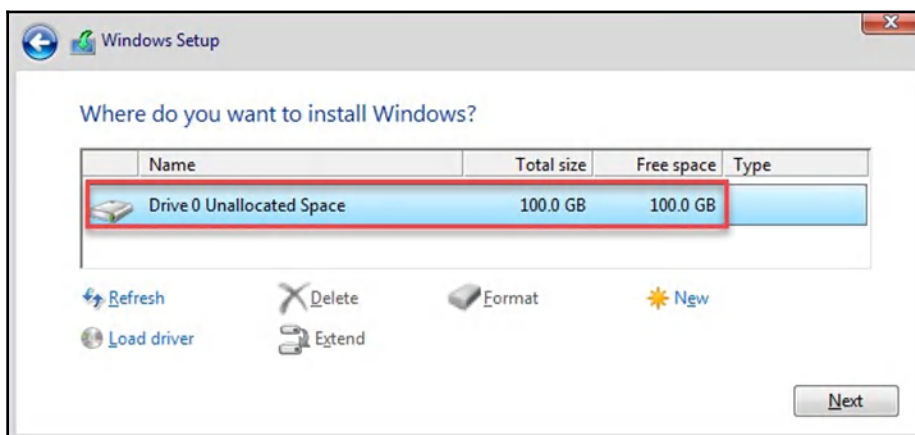
12. Choose the version of Windows you'd like to install. If you're using Windows Server 2016, use the Datacenter edition. If you're using Windows 10, choose the Enterprise edition:



13. Next, you'll need to read and accept the **End User License Agreement (EULA)**, followed by the type of installation on the virtual **hard disk drive (HDD)**. Since it's a new installation, select the **Custom: Install Windows only (advanced)** option, as shown in the following screenshot:



14. Select the virtual HDD as the installation destination, as shown in the following screenshot, and click **Next** to continue:



15. The installation process may take a while, depending on the amount of CPU and RAM resources that have been allocated to the VM.

Once this process has been completed, Windows will present a login window to you.

Now that we have installed a Windows VM, we will look at how to create additional user accounts on Microsoft Windows.

Creating a user account

In this section, I'll guide you through creating a user account on Windows:

1. Firstly, you need to access the **Control Panel** and click on the **User Accounts** option.
2. You'll see all the local user accounts on your system. Select **Manage another account**.
3. Next, click on **Add a user account**.
4. Windows 10/Server 2016 will provide you with a window asking for various details such as username, password, and a hint (to help you remember your password) so that you can create a new user account on the local system.

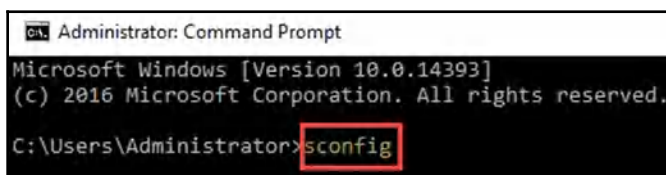
Now that you have the knowledge to create new user accounts, we will look at disabling automatic updates on Microsoft Windows Server.

Opting out of automatic updates

Vendors deliver updates to their software products and operating systems for many reasons, such as adding new features, improving performance, and fixing issues such as security bugs and crashes. Disabling automatic updates on Windows will ensure that your operating system maintains the same level of security that was established at installation while you practice in your lab.

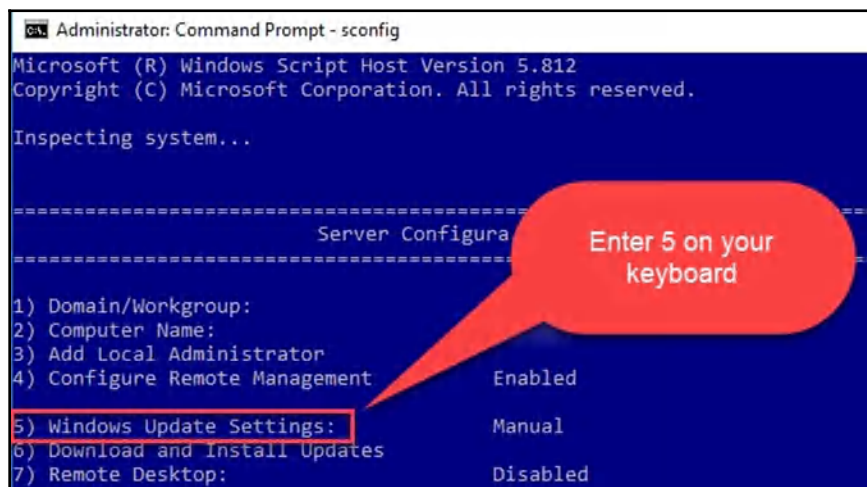
Using Windows 10 and Windows Server 2016, Microsoft has removed the function of disabling Windows Update from the Control Panel. In this section, I'll demonstrate how to disable the Windows Update function within Windows Server 2016:

1. Firstly, open **Command Prompt** and enter `sconfig`, as shown in the following screenshot:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>sconfig
```

2. The following screen will appear. Use option 5 to access Windows Update Settings:



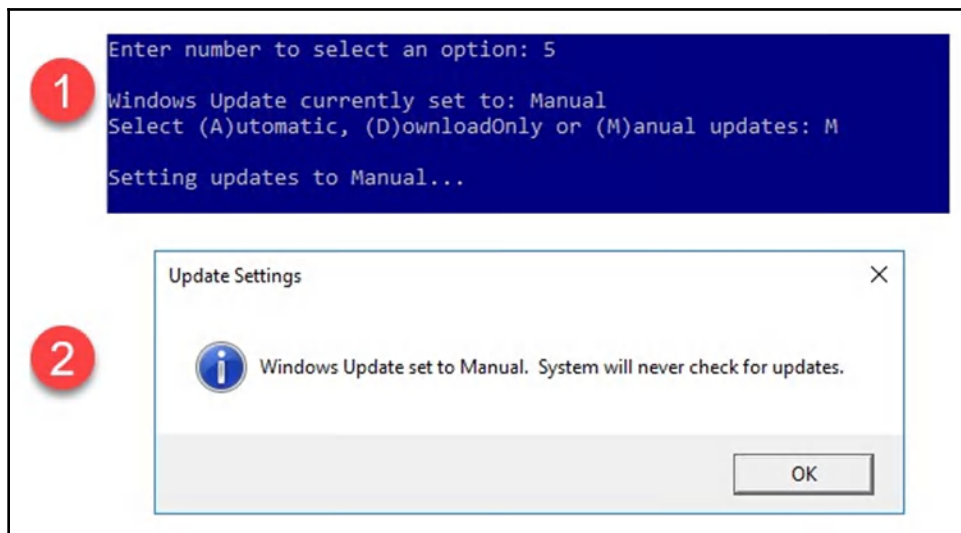
```
Administrator: Command Prompt - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

=====
Server Configuration
=====

1) Domain/Workgroup:
2) Computer Name:
3) Add Local Administrator
4) Configure Remote Management      Enabled
5) Windows Update Settings:      Manual
6) Download and Install Updates
7) Remote Desktop:                Disabled
```

3. The interactive menu will ask how you would like Windows to handle the checking and installation of updates—(A)utomatic, (D)ownloadOnly, or (M)anual. We will choose the Manual option:



Windows will then provide confirmation of our selection. `Manual` ensures that Windows does not check for any updates without our permission.

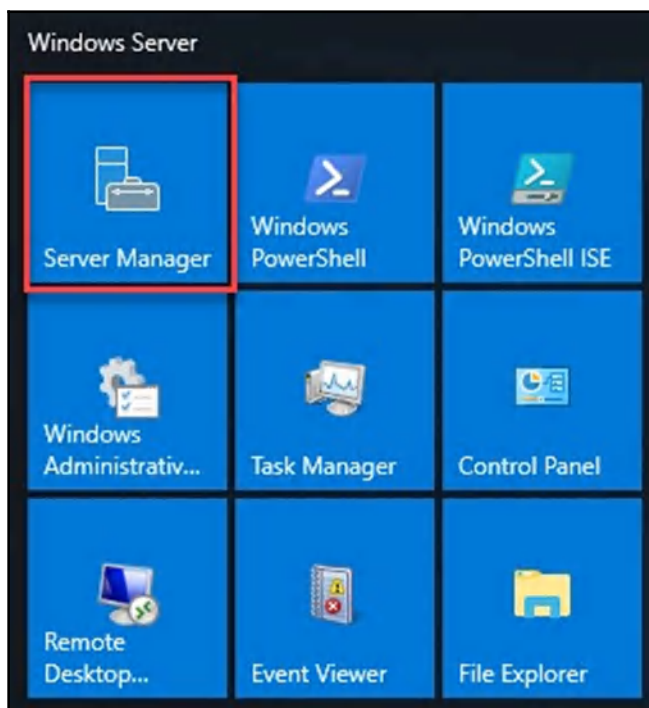
Now that you can disable automatic updates, let's take a look at setting a static IP address on your Windows VM.

Setting a static IP address

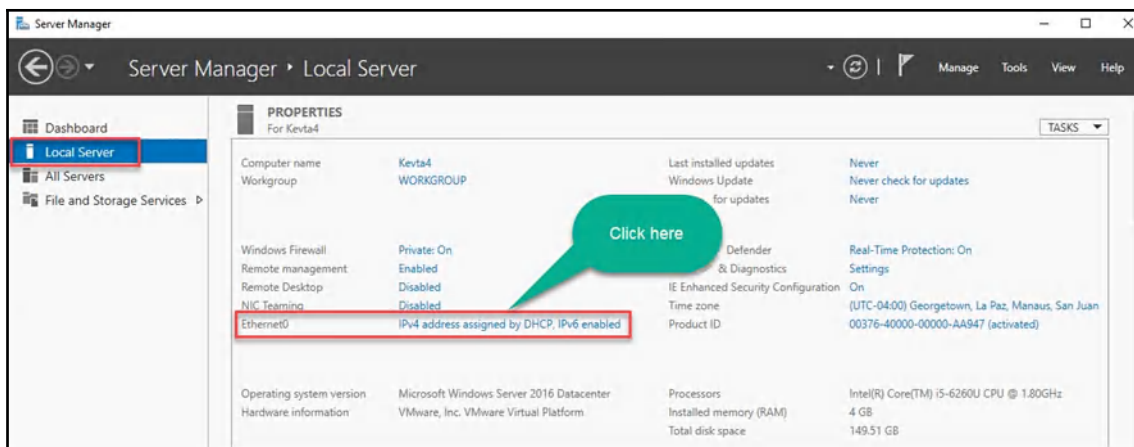
It's quite important to set static IP addresses on network resources and appliances. A static IP address will ensure that the IP address does not change and, therefore, that users on the network will always be able to access the resources/server once network connectivity is established.

Having a server within an organization or within our lab will definitely require an address that does not change. To do this, follow these steps:

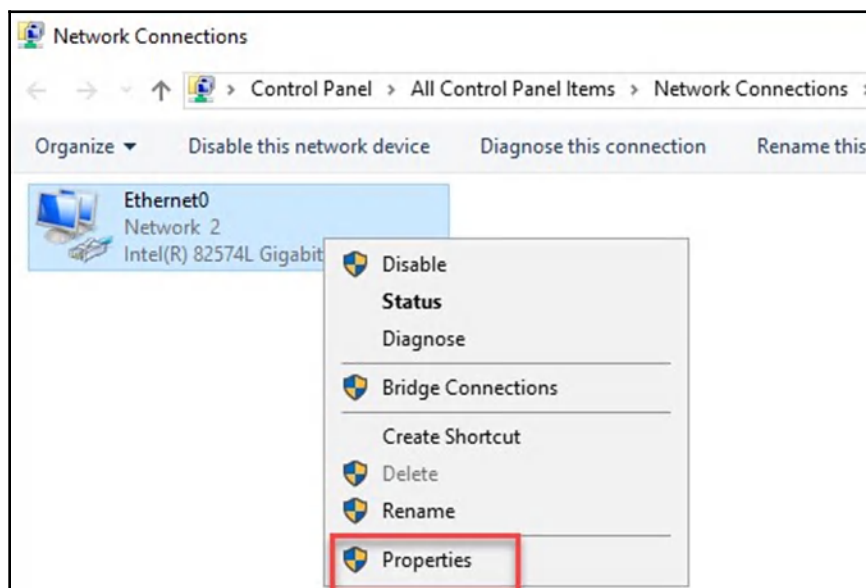
1. To begin, log on to your Windows Server 2016 and click the Windows icon in the bottom-left corner to view the **Start** menu. Click on **Server Manager**, as shown in the following screenshot:



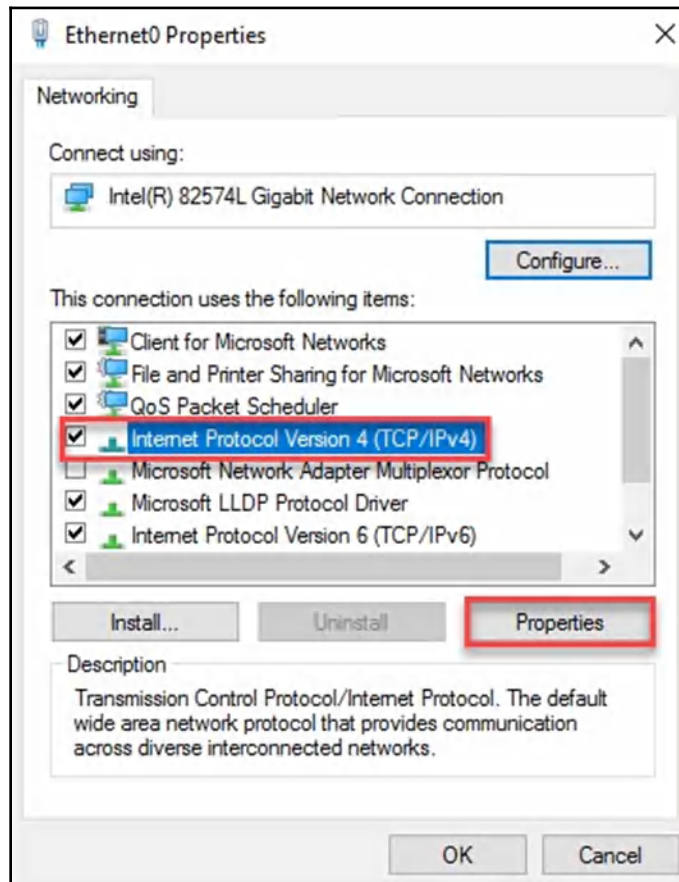
2. **Server Manager** is a single dashboard that allows a server administrator to control, manage, and monitor Windows Server using a **graphical user interface (GUI)**. On the left-hand side of the window, select **Local Server**, and then click the **Ethernet0** section, as shown in the following screenshot:



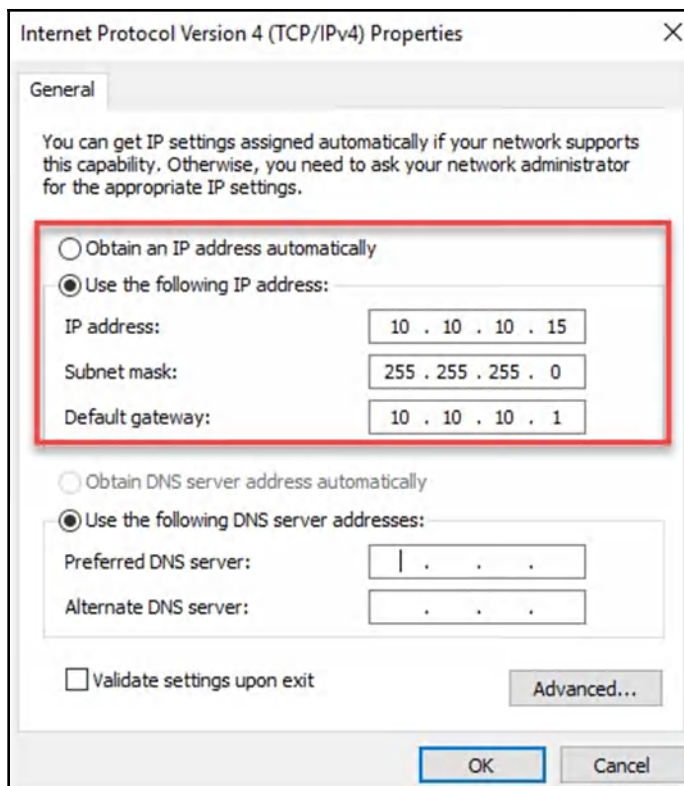
3. The **Network Connections** window will open, displaying all the network adapters that are available on your virtual Windows Server 2016 machine. To add a static IP address to a network adapter, simply right-click on the adapter and select **Properties**, as shown in the following screenshot:



4. Select **Internet Protocol Version 4 (TCP/IPv4) | Properties**, as shown in the following screenshot:



5. Now, you'll have the option to assign a static IP address, subnet mask, and default gateway, as well as **Domain Name Server (DNS)** configurations:



Please ensure that your IP address configurations are within the same subnet as your DHCP server (of your hypervisor) and the other VMs. Your IP address should be between 10.10.10.2 and 10.10.10.254, the subnet mask should be 255.255.255.0, and the default gateway should be 10.10.10.1 for each of the VMs in your lab.

Now that you are able to configure static IP addresses for Windows, let's look at how to add additional network interfaces.

Adding additional interfaces

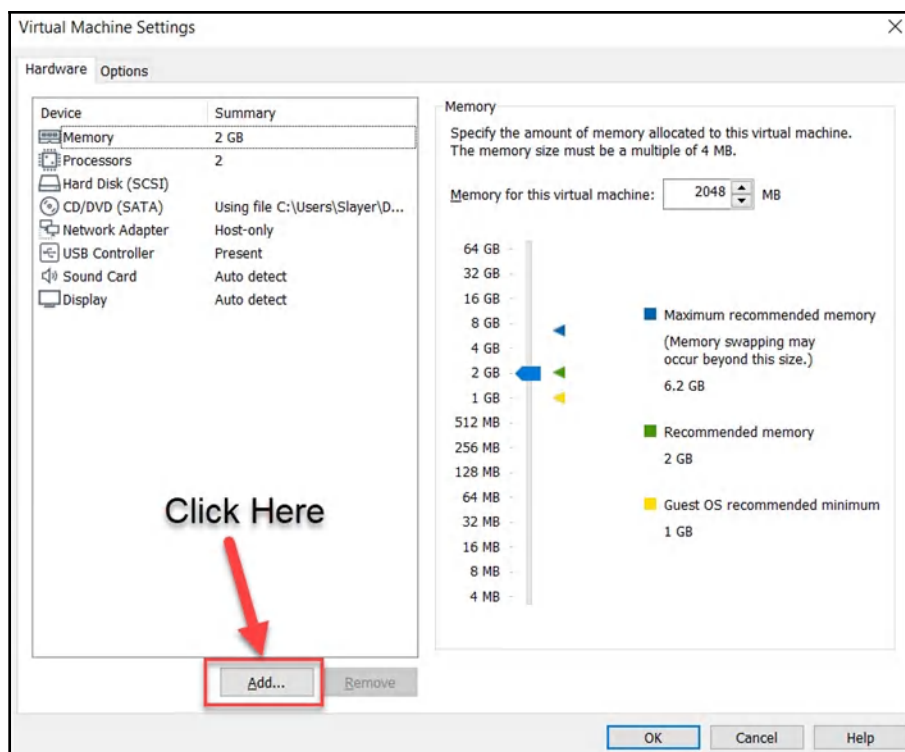
At times, having an additional **network interface card (NIC)** can be useful in many ways, such as ensuring network redundancy and even enabling NIC Teaming, which combines more than one NIC into one logical interface for combined throughput.

Let's add an additional NIC to a VM:

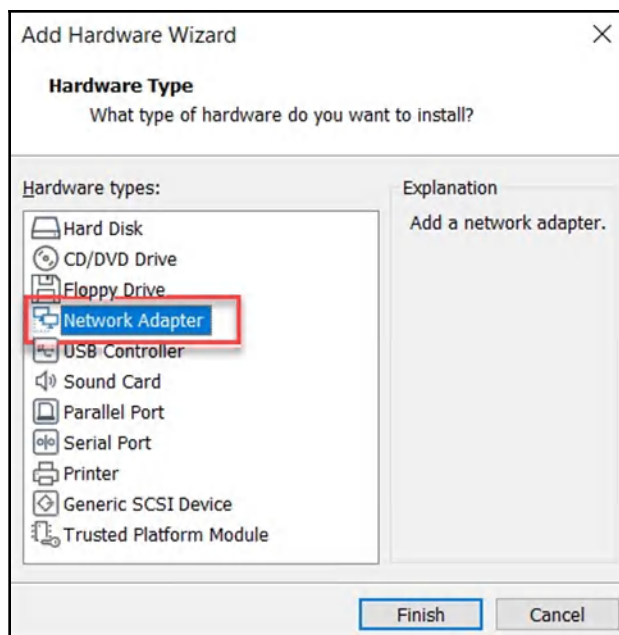
1. To add an additional NIC to your VM, simply access the settings for the VM:



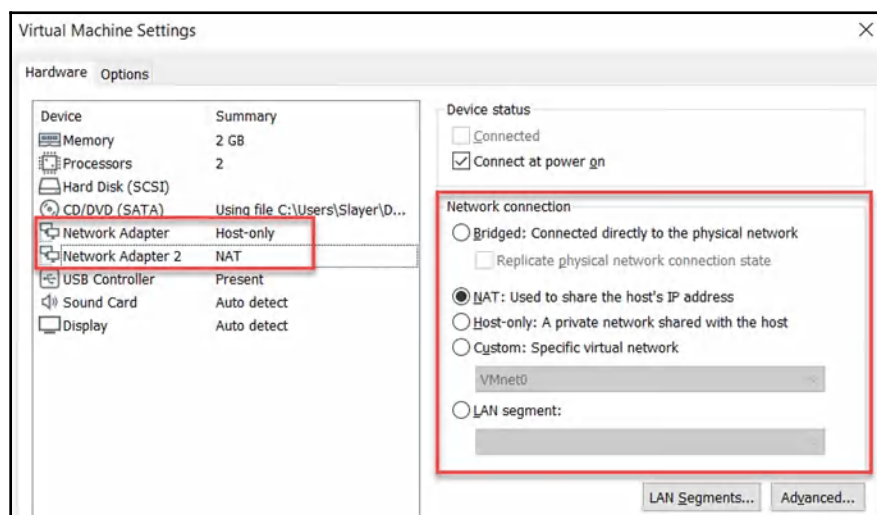
2. Click on **Add....** This will allow you to choose from a variety of virtual hardware components:



3. Select **Network Adapter** and click **Finish**, as shown in the following screenshot:



4. The new NIC will be added to the VM and you'll have the option to configure it as per your preferences:



When the operating system has rebooted, the virtual NIC will be present within the Network Sharing Center in Windows.

Having completed this section, you have now done the following:

- Installed Microsoft Windows
- Created a user account
- Disabled Windows automatic updates
- Configured a static IP address on Windows Server
- Added additional interfaces for a VM via the hypervisor

In the next section, we will take a deep dive into installing Ubuntu within our penetration testing lab.

Installing Ubuntu 8.10

In this section, we will be installing an Ubuntu (Linux) VM in our lab environment for testing purposes. As I mentioned previously, an awesome penetration tester or ethical hacker is someone who has a lot of knowledge and experience of many operating systems.

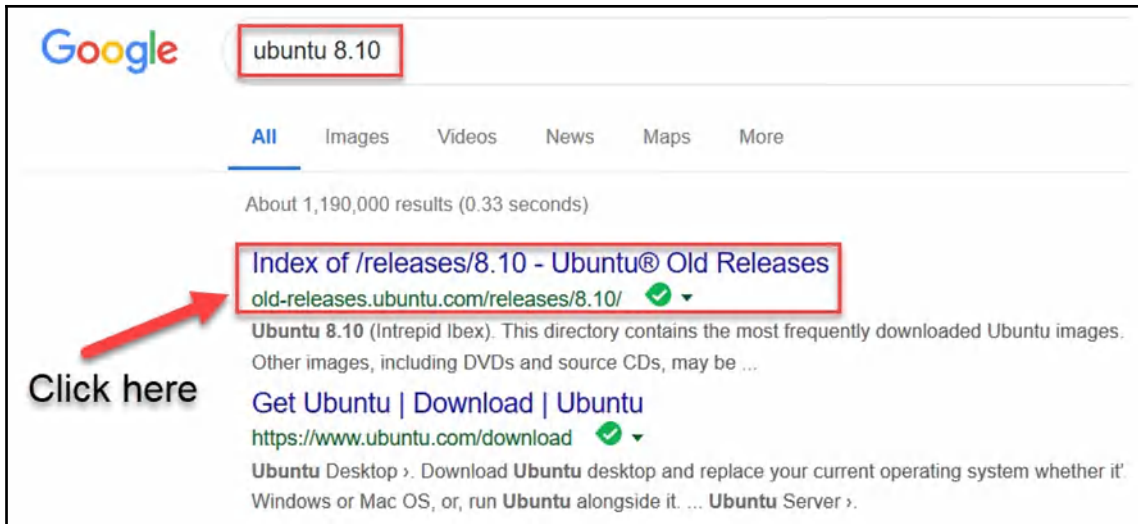
It's quite good to have a broad understanding and knowledge of various types of environments and operating systems as it will make security auditing and penetration testing much easier for you. We are going to use the Ubuntu 8.10 operating system within our lab.



The Linux operating system comes in many flavors, such as Fedora, CentOS, Arch Linux, openSUSE, Mint Linux, Ubuntu, and RedHat.

There are three ways to get started installing Ubuntu on your lab, as follows:

- Navigate to Ubuntu's website at www.ubuntu.com and go to the **Download** page to obtain a copy of the latest version of Ubuntu.
- Since our exercise is going to use a specific version of Ubuntu, we will search for `Ubuntu 8.10` on Google to quickly find the official relevant repository:



- You can also use <http://old-releases.ubuntu.com/releases/8.10/> to download both Ubuntu Server and Desktop ISO images.

Once the ISO file has been successfully downloaded onto your desktop computer, create a virtual environment within Oracle VM VirtualBox or VMware Workstation using the following parameters:

- **CPU:** 1 core
- **RAM:** 1-2 GB
- **HDD:** 60 GB
- **NIC:** VMnet1

You can also adjust the hardware configurations as you see fit.

As you may recall, in the previous section, *Installing Windows as a VM*, we walked through the process of setting up a virtual environment. The procedure for creating a virtual environment for Linux is essentially the same as that for Windows when using a hypervisor, the only differences being in choosing the Ubuntu ISO (Linux operating system) and using the previously specified parameters (that is, for the CPU, RAM, and so on).

The following are the instructions for installing Ubuntu Server in our lab:

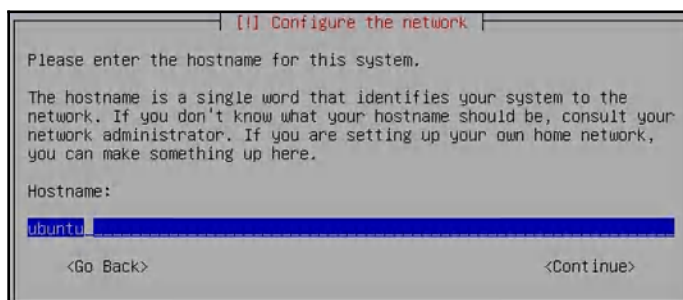
1. Once you have powered on the VM, you'll be presented with the following screen. Choose **Install Ubuntu Server** and hit *Enter*:



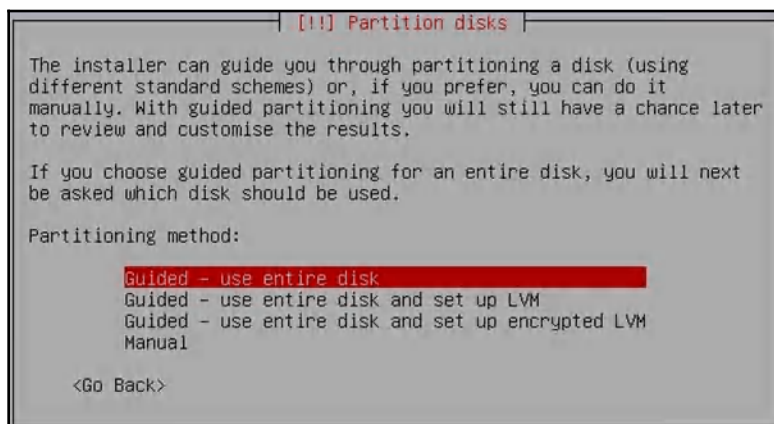
2. The setup wizard will ask to specify your language.
3. Then, you'll be asked to choose your country or territory.
4. The installation wizard will ask whether you want your keyboard layout detected. Choose **No** and continue:



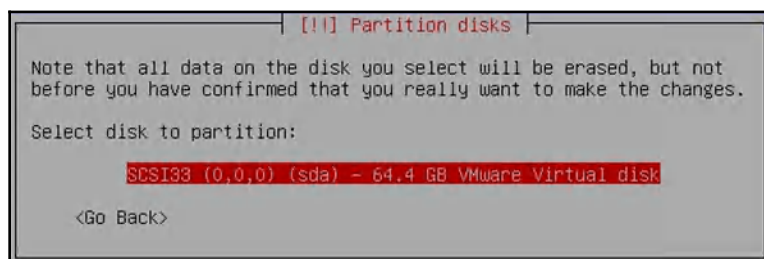
5. During the setup process, you will be asked to assign a hostname to the Ubuntu server, which you can leave as the default, as shown in the following screenshot:



6. During this phase, you'll also be asked to specify your time zone. Choose an appropriate zone.
7. Select the **Guided – use entire disk** option and hit *Enter* to continue. This will allow the Ubuntu operating system to wipe the entire disk drive and install itself on it, thereby occupying the entire disk:

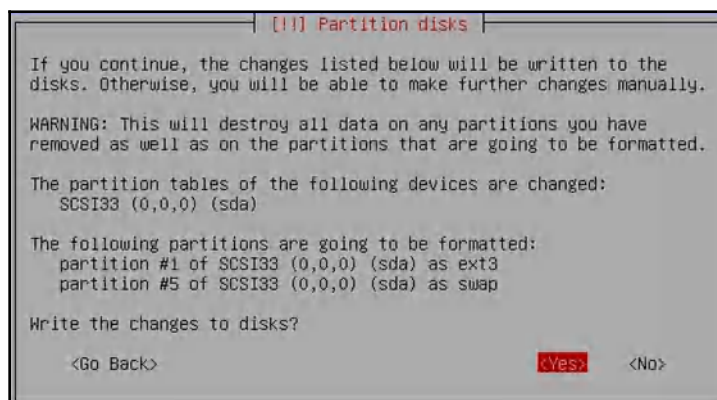


8. You will be asked to choose the destination where you wish to install the Ubuntu server; choose the disk that has **sda** (primary disk partition) in brackets:

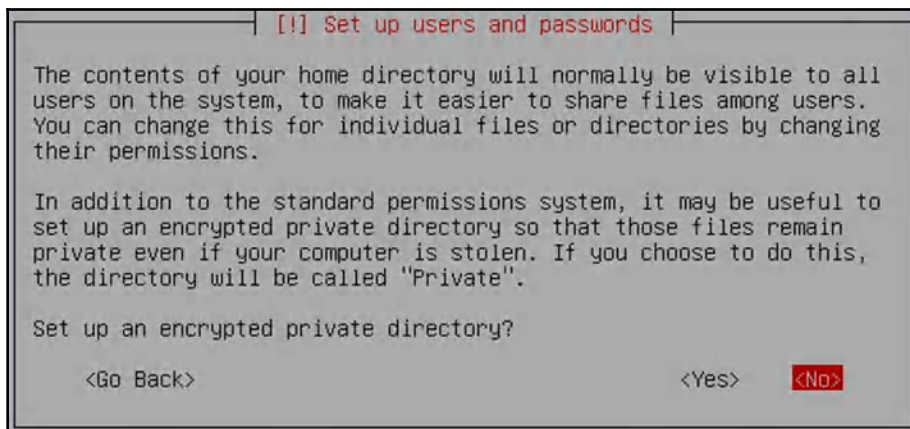


sda is used to represent the primary partition of the primary disk drive on the Linux operating system. This is the location where you would normally install any operating system on a disk drive.

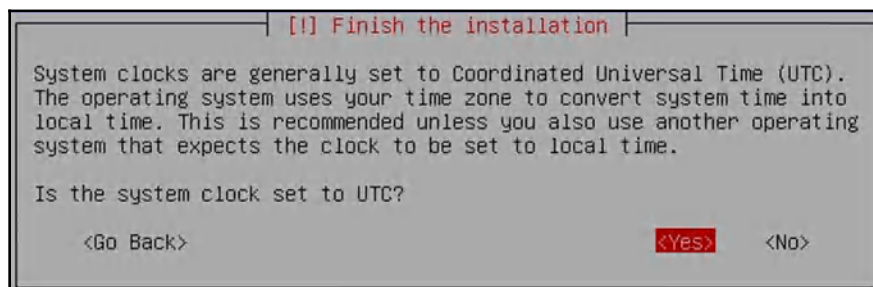
9. Before the installation is executed, select **Yes** to confirm the configurations:



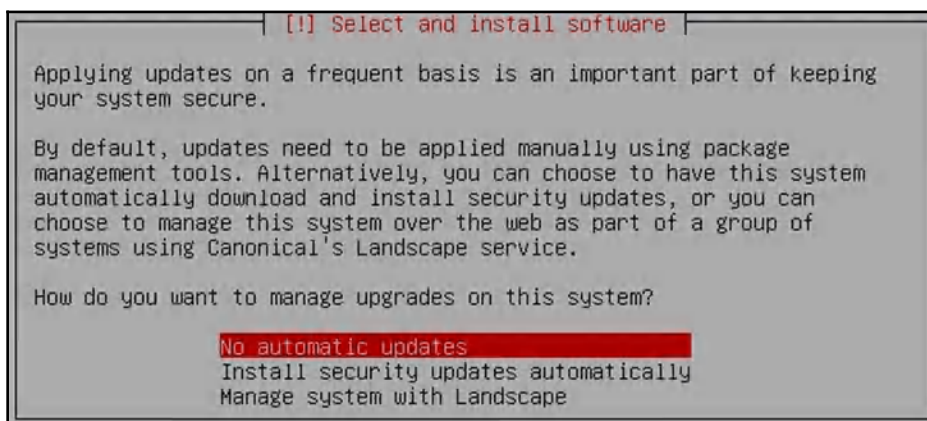
10. You will then be asked to provide your full name and you'll also be required to create a user account. Next, assign a password to the user account.
11. Once the user account creation process has been completed, you will be asked whether you would like to set up an encrypted private directory. I have used the default (**No**), as shown in the following screenshot:



12. At this point, the installation process will take a few minutes to complete. Afterward, you'll be required to set the system clock:



13. Next, specify how the operating system should check for updates. I have chosen the **No automatic updates** option, as shown in the following screenshot:



14. On the following screen, you can still choose to install various services. I have used the default setting (no software/service selected) once again and selected **Continue**:



15. Once the installation has been completed, the Ubuntu server will boot into its login window, as shown in the following screenshot:


```
* Starting system log daemon... [ OK ]
* Starting kernel log daemon... [ OK ]
* Starting system message bus dbus [ OK ]
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]

Ubuntu 8.10 ubuntu tty1

ubuntu login: glen
Password:
Linux ubuntu 2.6.27-7-server #1 SMP Fri Oct 24 07:20:47 UTC 2008 x86_64

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/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

glen@ubuntu:~$
```

Your Ubuntu VM is now all set up and ready for future exercises.

Now that you have installed a few VMs in your virtual lab environment, let's take a few more minutes to walk through and discuss the importance of creating **snapshots** regularly when working with virtualization.

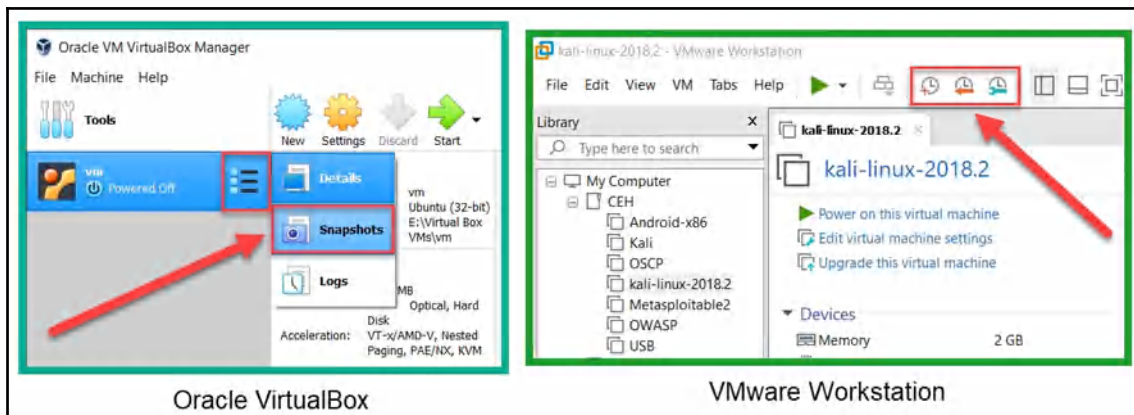
Creating and using snapshots

Creating a snapshot can save you a lot of time in restoring the previous state of a VM. A snapshot works like an instant system restore point. Taking snapshots of a VM prior to and after major changes will help you recover from any critical issues you may be experiencing within a VM.

To create a snapshot on both VirtualBox and VMware Workstation, perform the following steps:

1. On VirtualBox, select the VM of your choice.
2. Click the menu icon, as highlighted in the following screenshot, and select **Snapshots**.

3. Using VMware Workstation, select a VM of your choice. The snapshot menu on VMware Workstation Pro is located in the toolbar, as indicated in the following screenshot, on the right-hand side:



I would recommend creating a snapshot once the installation of a VM is successful, and before and after any major changes or configurations are made on a VM. Creating a snapshot uses disk space on your local storage drive. However, snapshots can be deleted at any time.

Having completed this section, you are now able to efficiently install Linux within a virtualized environment and understand the benefits of working with snapshots.

Troubleshooting Kali Linux

Now that you have access to Kali Linux, you may find yourself encountering some problems. These may include the following:

- Network adapter and USB incompatibility
- VM memory problems

Let's go through how to resolve these issues should they come up.

Network adapter and USB incompatibility

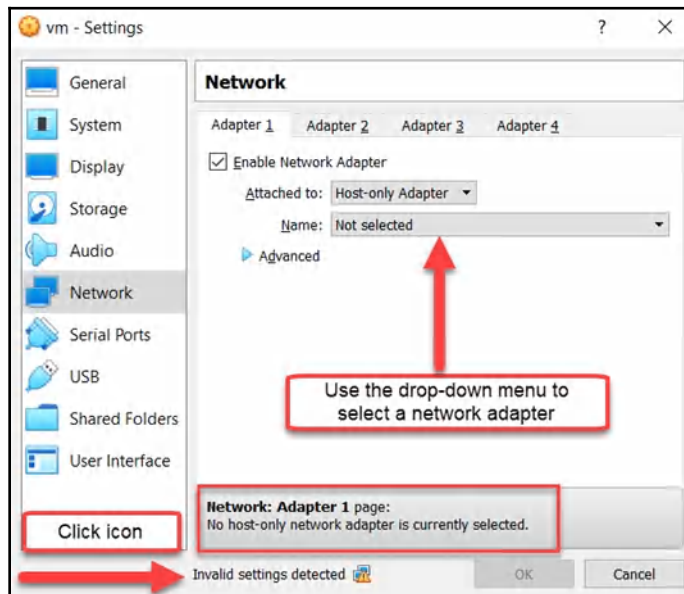
One of the most commonly found issues that students encounter after importing the Kali Linux VM within VirtualBox is incompatibility. This incompatibility is usually to do with the network adapter or USB settings on VirtualBox. If these issues aren't resolved, the VM will not be able to start.

To determine whether there is an issue, we can perform the following actions:

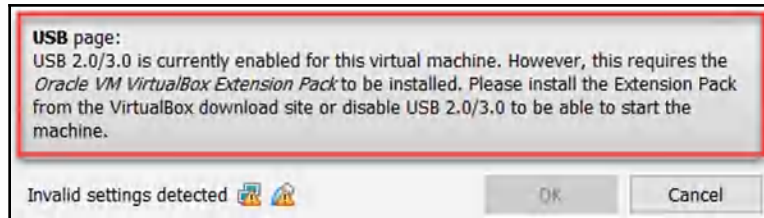
1. Open the VM settings on Oracle VM VirtualBox.
2. If you see **Invalid settings detected**, the VM will be unable to start. Click on one of the icons (such as the network icon or the USB icon) and the relevant error message will appear.

The following screenshot indicates that there's an issue with the virtual network adapter on the VM. As we can see, there is no actual adapter attached. Perform the following actions:

1. Simply click the **Name** drop-down menu, as shown in the following screenshot.
2. Select an appropriate network adapter, such as **Adapter 1**, to resolve the issue:

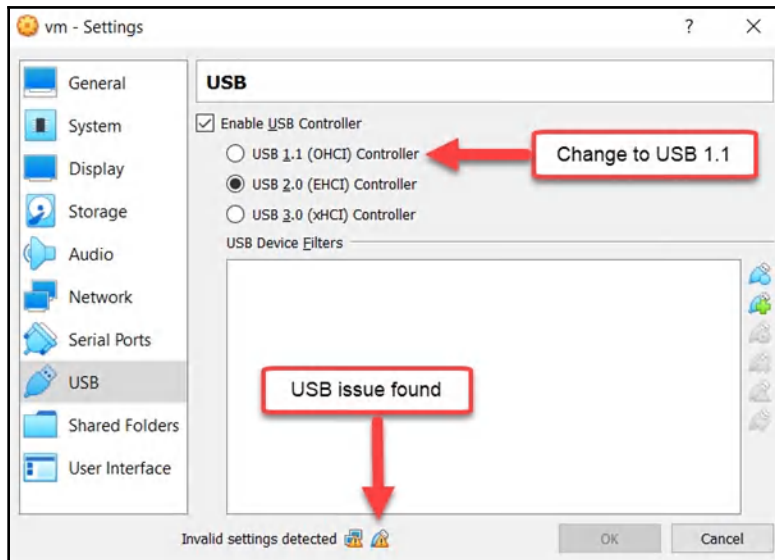


Now that we have fixed the potential problem with the network adapter, let's look at what happens if the USB software bus is incompatible. You would usually see a USB icon displayed at the bottom of the **Settings** window. Clicking on it will display the following message:



The use of the VirtualBox extension pack will resolve this issue by enabling USB 2.0 or 3.0. This will ensure that the VM is compatible and is able to send and receive data to the host's USB ports.

To resolve this issue, simply access the USB settings and select the appropriate USB controller (preferably USB 1.1 or 2.0), as shown in the following screenshot:

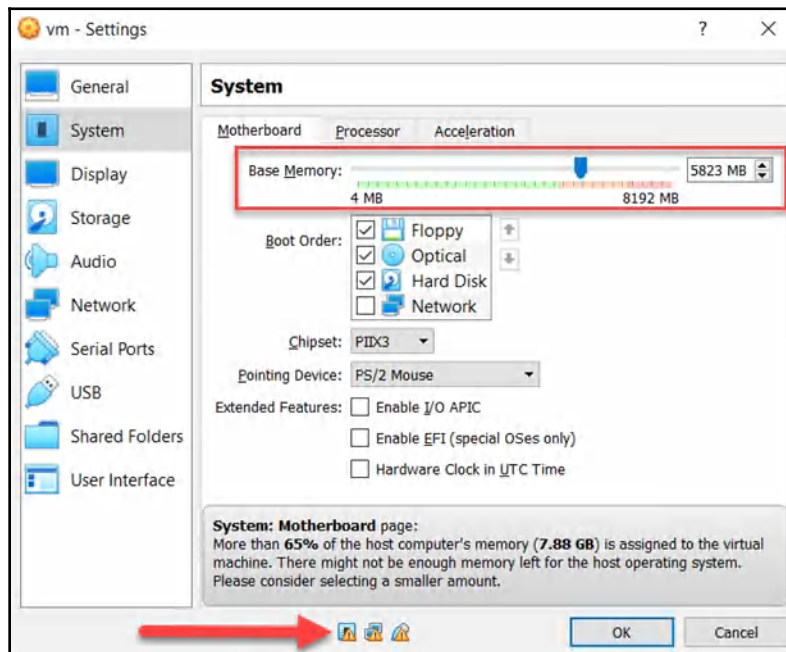


Within the Oracle VM VirtualBox settings interface, if you look carefully, the bottom of the window includes icons with warning signs on each. Hovering over each icon at the bottom will provide you with a description of the issue that is preventing the VM from starting.

VM memory problems

A lot of students sometimes create a VM and assign more memory than is available to the hypervisor. This can cause either the VM to not start or instability on your host operating system. To resolve this issue, do the following:

1. Open the VM settings.
2. Open the **System** tab.
3. Next, adjust the base memory so that it sits within the green zone (random access memory is what we're talking about here):



The hypervisor will always inform you of any issues. However, please ensure that you enable the virtualization feature in your processor. To do this, you'll need to access your computer's BIOS/UEFI settings to turn on virtualization.

If you encounter any of these problems, you are now equipped with the answers to fix them.

Summary

During the course of this chapter, we continued from the previous chapter and expanded our lab environment by deploying and setting up both Windows and Ubuntu VMs. Additionally, we took a look at the two most commonly found issues when deploying Kali Linux in a virtual environment.

Having completed this chapter, you have the skills to install Windows and Ubuntu servers in a virtual lab environment, create user accounts and opt out of automatic updates, add additional network interfaces to a VM, and create snapshots using the hypervisor manager, VirtualBox, and VMware Workstation Pro. This concludes our objective of building a virtual penetration testing lab environment.

Now that we have our own lab set up and ready, it's time to dive into our next chapter, which is about getting comfortable with Kali Linux 2019.

Further reading

The following links are recommended for additional reading:

- **Kali Linux documentation:** <https://docs.kali.org/>
- **Windows 10:** <https://docs.microsoft.com/en-us/windows/windows-10/>
- **Windows Server 2016:** <https://docs.microsoft.com/en-us/windows-server/index>
- **Ubuntu:** <https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-desktop> and <https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server>

4

Getting Comfortable with Kali Linux 2019

If you're getting started in the field of cybersecurity—especially in offensive security testing (penetration testing)—it's likely that you'll encounter the Kali Linux operating system. Kali Linux has a lot of features and tools that make a penetration tester's or security engineer's job a bit easier when they're in the field or on a job. There are many tools, scripts, and frameworks for accomplishing various tasks, such as gathering information on a target, performing network scanning, and even exploitation, to name just a few. The challenge we face as beginners is learning about, and adapting to, a new environment.

In this chapter, we'll learn how to use Kali Linux more efficiently as a user and as a penetration tester. Furthermore, you will learn how to use the Linux operating system to perform various tasks and become more familiar with it. Without understanding how Kali Linux works, you may face challenges in the later and more advanced chapters on penetration testing.

In this chapter, we will be covering the following topics:

- Understanding Kali Linux
- What's new in Kali Linux 2019?
- Basics of Kali Linux

Technical requirements

Kali Linux is the only technical requirement for this chapter.

Understanding Kali Linux

Let's go over a little bit of the history of BackTrack (<https://www.backtrack-linux.org/>). The BackTrack operating system was developed and maintained by the Auditor Security Collection and Whax organizations back in 2006. At the time, BackTrack was based on the Linux operating system, Ubuntu. Being Linux-based meant that BackTrack provided many opportunities for the penetration tester, with one of its benefits being the ability to boot from a live CD and live USB bootable media. However, the latest version of the BackTrack operating system is **BackTrack 5**, which was released in 2011 before the project was archived. In 2012, the next-generation operating system, and now successor to BackTrack, was announced, known as **Kali Linux**, which was built from the ground up. In March 2013, Kali Linux was officially released to the public.

In the field of cybersecurity, particularly in the field of penetration testing, the majority of the most awesome tools are created for the Linux operating system rather than for Microsoft Windows. Hence, in most cybersecurity training programs, you will notice that Linux is the preferred operating system for performing security testing.

Some benefits of using Kali Linux are as follows:

- It supports open source penetration testing tools.
- It contains over 300 tools by default.
- Being Linux-based allows it to be installed on a disk drive or used via live boot media (DVD or USB).
- It has support for installation on mobile devices such as OnePlus smartphones and Raspberry Pi.
- It doesn't require much in the way of resources, such as RAM or CPU.
- Kali Linux can be installed as a virtual machine, on a local disk drive, bootable USB flash drive, Raspberry Pi, and various other devices.

The Kali Linux operating system is built on Debian and consists of over 300 preinstalled tools, with functions ranging from reconnaissance to exploitation and even forensics. The Kali Linux operating system has been designed not only for security professionals but also IT administrators and even network security professionals in the field of IT. Being a free security operating system, it contains the tools necessary to conduct security testing.

Within the Kali Linux operating system, there are many popular tools that are currently being used in the industry, such as **network mapper (Nmap)**, aircrack-ng, and the Metasploit Framework. Deployment and utilization of the operating system is very flexible and only limited by your imagination.

Kali Linux, being a prepacked all-in-one operating system filled with tools for penetration testing, digital forensics, reverse engineering, and much more, is definitely a preferred choice among penetration testers. In the next section, we will dive into the new features in Kali Linux 2019.

What's new in Kali Linux 2019?

Kali Linux 2019 comes with an upgraded kernel of 4.19.13 and many updated packages and bug fixes within the operating system. One of the major upgrades is for the Metasploit Framework. The previous version of Metasploit was version 4.0, released in 2011, but, in Kali Linux 2019, it was upgraded to version 5.0.

The new Metasploit version 5.0 brings new evasion techniques, updates to its database, and the automation of APIs. Kali Linux 2019 also contains upgrades for the following tools:

- theHarvester
- dbeaver
- Metasploit
- exe2hex
- msfpc
- SecLists



Further information on the new evasion techniques in Metasploit 5.0 can be found at <https://www.rapid7.com/info/encapsulating-antivirus-av-evasion-techniques-in-metasploit-framework/>.

The community of developers and users of the Kali Linux operating system continues to grow as it's one of the most popular penetration testing Linux distributions currently available. There will be many more updates and improvements in the future.

Now that you are up to date with the changes in Kali Linux 2019, we will learn how to use Kali Linux.

Basics of Kali Linux

Being accustomed to an operating system for most of your digital life is both a good and bad thing at times. Most likely, you're either a Windows or macOS user and are very comfortable with the features and functionalities, and you know how to find your way around your current operating system of choice. However, learning a new platform or even a new user interface can prove quite challenging for some. It's like being an Android user and switching to the Apple iOS or vice versa. In the beginning, it will be a bit tough, but with continuous practice, you'll become a Jedi master.

Over the next few sections, we will dive deep into learning the fundamentals of navigating the Linux operating system as a penetration tester.

The Terminal and Linux commands

The Linux Terminal is pretty much the most powerful interface in the Linux operating system as this is where all the magic happens. Most Linux tools are command-line based. Most penetration testing tools are also command line-based, and this can sometimes be intimidating to new users and people who are just starting in the field of cybersecurity or directly in penetration testing.

The following exercises will help you become a bit more familiar with using the Linux Terminal and commands:

- To change the password on your current user account, execute the `passwd` command. Whenever you type passwords on a Linux Terminal/shell, the password itself is invisible.
- To view your current working directory in the Terminal, use the `pwd` command.
- To view a list of files and folders in your current directory, use the `ls` command. Additionally, the `ls -la` command can be used to provide a list of all files (including hidden files) with their permissions.
- To change directory or navigate the filesystem, use the `cd` command followed by the directory.

The following is a screenshot demonstrating the use of these commands. We can see the current working directory after executing the `pwd` command, a list of files and folders using the `ls -l` command, and the option to change the working directory using the `cd` command:

```

File Edit View Search Terminal Help
root@kali:~# pwd
/root
root@kali:~#
root@kali:~# ls -l
total 100
drwxr-xr-x 2 root root 4096 Aug  5 22:30 Desktop
drwxr-xr-x 2 root root 4096 Apr 26  2018 Documents
drwxr-xr-x 2 root root 4096 Apr  9 11:32 Downloads
drwxr-xr-x 9 root root 4096 Aug  6 21:11 EyeWitness
drwxr-xr-x 6 root root 4096 Apr 13 14:40 InSpy
drwxr-xr-x 2 root root 4096 Apr 26  2018 Music
drwxr-xr-x 2 root root 4096 Apr 26  2018 Pictures
-rw-r--r-- 1 root root 33614 Aug  5 22:40 profiles.csv
drwxr-xr-x 2 root root 4096 Apr 26  2018 Public
drwxr-xr-x 4 root root 4096 Aug  5 20:41 recon-ng
-rw-r--r-- 1 root root  52 Apr 13 15:21 S3list.txt
drwxr-xr-x 5 root root 4096 Apr 13 15:17 S3Scanner
-rw-r--r-- 1 root root 8192 Aug  5 22:38 stash.sqlite
drwxr-xr-x 4 root root 4096 Aug  5 22:44 Sublist3r
drwxr-xr-x 2 root root 4096 Apr 26  2018 Templates
drwxr-xr-x 2 root root 4096 Apr 26  2018 Videos
root@kali:~#
root@kali:~# cd Desktop/
root@kali:~/Desktop#
root@kali:~/Desktop# ls -l
total 0
lrwxrwxrwx 1 root root 36 Apr 26  2018 mount-shared-folders.sh -> /usr/local/sbin/mount-shared-folders
lrwxrwxrwx 1 root root 32 Apr 26  2018 restart-vm-tools.sh -> /usr/local/sbin/restart-vm-tools
root@kali:~/Desktop#

```

Currently in the root directory

Blue indicates folders

Furthermore, if we have a text file in our directory, we can use the `cat` command to view its content. Also, we can add additional lines of text to an existing file directly from the Terminal by using the `echo "text" >> filename.txt` syntax, as shown in the following screenshot. Looking closely, we can see that the `ls` command was used to show the files on the desktop, the `cat` command was used to print the content of the `Test.txt` file on the Terminal, and `echo` was used to add text:

```

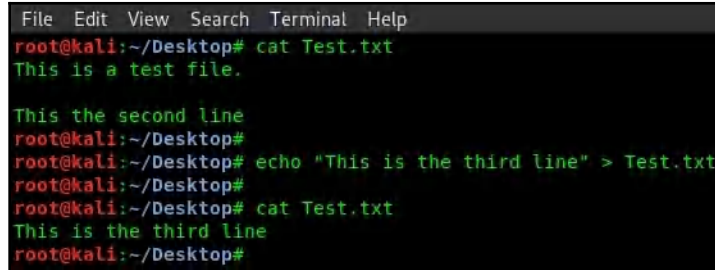
File Edit View Search Terminal Help
root@kali:~/Desktop# ls
mount-shared-folders.sh  restart-vm-tools.sh  Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is a test file.

root@kali:~/Desktop# echo "This the second line" >> Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is a test file.

This the second line
root@kali:~/Desktop#

```

Using the `>>` switch will add another line to the existing text file (in other words, insert a new line). However, using a single `>` will overwrite all the content with the new string, as we can see here:

A terminal window with a dark background and light green text. The menu bar at the top shows 'File Edit View Search Terminal Help'. The terminal shows the following commands and output:

```
root@kali:~/Desktop# cat Test.txt
This is a test file.

This the second line
root@kali:~/Desktop#
root@kali:~/Desktop# echo "This is the third line" > Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is the third line
root@kali:~/Desktop#
```

The `Test.txt` file now has the most recent string of text.



If you're interested in learning more about Linux, check out the *Linux Unhatched* and *Linux Essentials* courses at Cisco Networking Academy:
<https://www.netacad.com/courses/os-it>.

Always remember that the more you practice using a Linux operating system, the easier it is to perform tasks.

Next, we will demonstrate how to find your way around Kali Linux using various utilities.

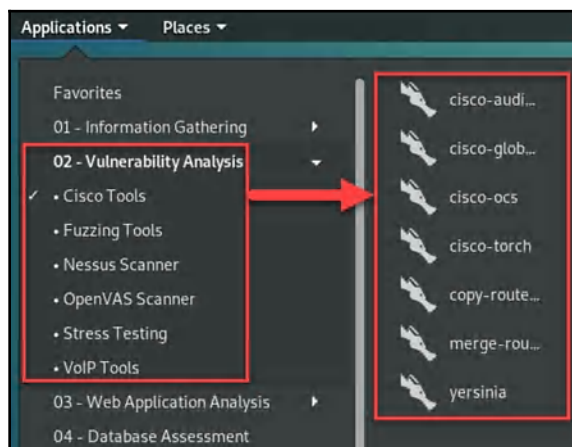
Navigating in Kali Linux

In this section, we will guide you through the basics of maneuvering the Kali Linux operating system. As we mentioned previously, Kali Linux is based on the Debian flavor of Linux. This means that all other Debian-based operating systems will have a similar user interface.

After Kali Linux has booted, you'll be presented with the login screen; the default username and password for logging into Kali Linux are `root/t00r`. Upon logging in, you'll be presented with a very nice, clean, and polished user interface. One of the very first things you'll notice in the top-left corner is the **Applications** drop-down menu. This is the menu where all of your penetration testing and forensics tools are kept. The **Applications** menu, as shown in the following screenshot, is organized into various categories, such as **Information Gathering**, **Vulnerability Analysis**, and **Web Application Analysis**:

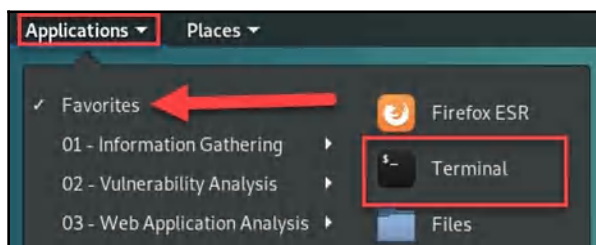


Additionally, hovering over a category will display the popular tools for this section. However, clicking on a category will expand further subcategories, and each subcategory contains even more tools. Let's click on **Applications** | **02 – Vulnerability Analysis** | **Cisco Tools**. You'll see an additional menu open to the right, displaying all the vulnerability tools related to Cisco devices, as shown in the following screenshot:

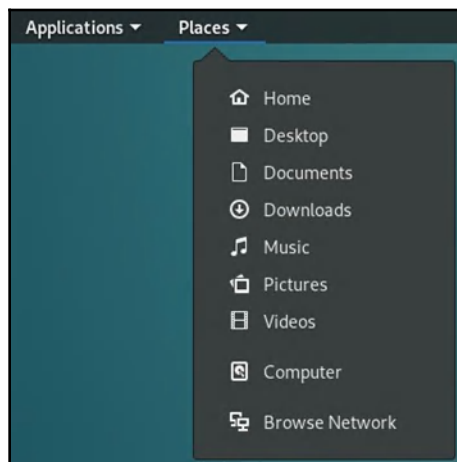


When you become a Linux user, you'll soon realize that one of the most powerful applications on the operating system is the Linux Terminal. The Terminal is equivalent to Command Prompt in the Windows operating system. A lot of tasks and tools are usually initialized via the Terminal window. You may be wondering: Kali Linux has a **graphical user interface (GUI)**, so don't all of its built-in tools have a GUI as well? The short answer is no.

Most of Kali Linux's powerful tools are only controlled by the **command-line interface (CLI)**; however, some have the option to use a GUI. The benefit of using a CLI is that the output for a tool is much more detailed on the Terminal in comparison to that for a GUI. We'll take a look at this concept later in the book. To open the Terminal, select **Applications** | **Favorites** | **Terminal**:

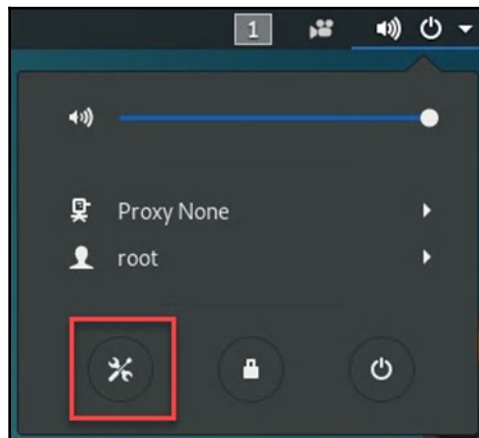


Kali Linux has all the regular features and functions that any other operating system has. This means that there are user directories such as Home, Desktop, Documents, Downloads, Music, and Pictures. To quickly access any of the locations with Kali, simply click on the **Places** drop-down menu:

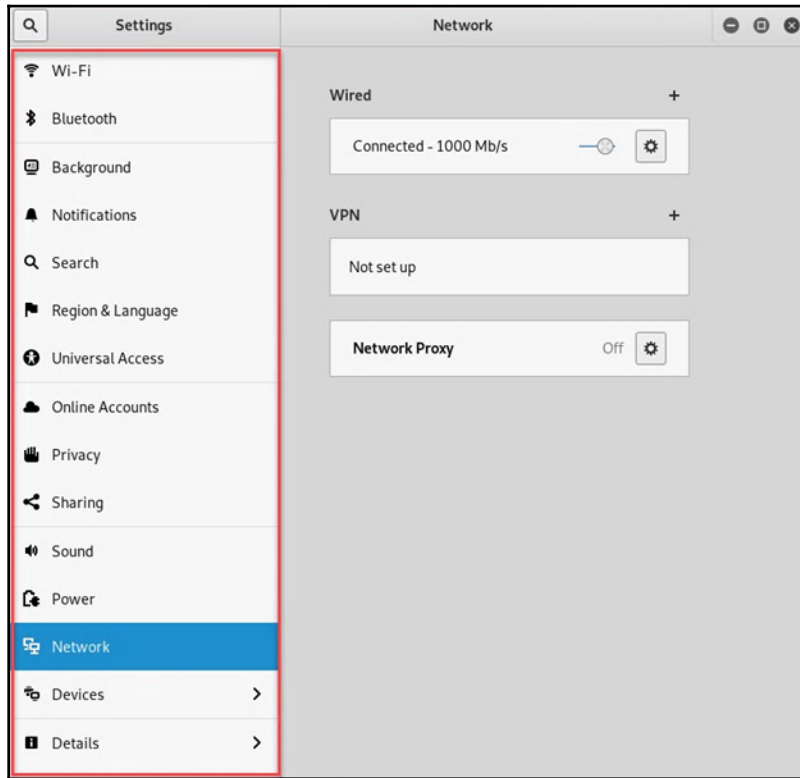


Now, regular Windows users won't feel as though their experience is complete until they have something that resembles Control Panel. To access the equivalent of Control Panel in Kali Linux, simply click the power button icon, which can be found in the top-right corner. This will create a drop-down menu where you will see a spanner and screwdriver icon, as shown in the following screenshot.

Clicking on this icon will open the **Settings** menu for the operating system:



In the left-hand side column, you will find the main categories. The right-hand side shows the expansion of each:



Please ensure that you record your default settings before making any configuration changes on Kali Linux. This is to ensure that if any issues arise after you've made a change, you can revert to the previous state. Additionally, create a snapshot of the virtual machine prior to making any major changes.

Now that you have a better understanding of where popular directories and settings are located, we can move on and learn about updating and installing programs on Kali Linux.

Updating sources and installing programs

At times, a tool may not be working as expected, or even crash unexpectedly on us during a penetration test or security audit. Developers often release updates for their applications. These updates are intended to fix bugs and add new features to the user experience.

To update the software packages on our Kali Linux operating system, we must first resynchronize the package index files with their sources. Let's get started:

1. Open the Terminal, and execute the `apt-get update` command:

```
root@kali:~# apt-get update
Get:1 http://kali.mirror.globo.tech/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.globo.tech/kali kali-rolling/main amd64 Packages [17.0 MB]
Get:3 http://kali.mirror.globo.tech/kali kali-rolling/non-free amd64 Packages [188 kB]
Get:4 http://kali.mirror.globo.tech/kali kali-rolling/contrib amd64 Packages [105 kB]
Fetched 17.4 MB in 16s (1,055 kB/s)
Reading package lists... Done
root@kali:~#
```



The indexes are located in the `/etc/apt/sources.list` file.

This process usually takes a minute or two to complete with a stable internet connection.

2. If you want to upgrade the current packages (applications) on your Kali Linux machine to their newest and latest versions, use the `apt-get upgrade` command:

```
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
```

When you perform an upgrade, ensure that all your tools and scripts are working perfectly before conducting a penetration test.



If you experience an error while upgrading packages on Kali Linux, use the `apt-get update --fix-missing` command to resolve any dependencies, and then execute the `apt-get upgrade` command once more.

3. At the end of the output, the interactive menu will ask you to select yes (y) or no (n) to continue with the upgrade process. Once you've selected yes, the operating system will download all the latest versions of each package and install them one by one. This process takes some time to complete.



Optionally, if you would like to upgrade your version of Kali Linux to the most current distribution, use the `apt-get dist-upgrade` command. At the time of writing, we are using Kali Linux 2019.2.

Additionally, executing the `apt autoremove` command will perform a cleanup operation on your Kali Linux operating system by removing any old or no longer needed package files:

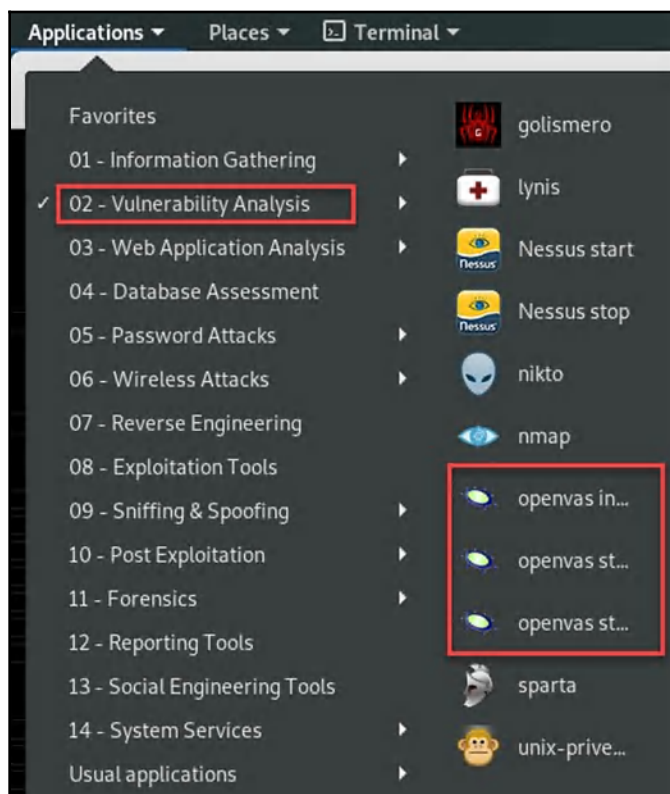
```
root@kali:~# apt autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
gdal-bin gdal-data geoip-database-extra libaec0 libappindicator1 libarmadillo8
libdbusmenu-gtk4 libepsilon1 libfcgi-bin libfcgi0ldbl libfile-copy-recursive-pe
libhdf4-0-alt libhdf5-100 libindicator7 libjs-openlayers libkmlbase1 libkmlconv
libminizip1 libnetcdf13 libogdi3.2 libpango-perl libpyside1.2 libqca2 libqca2-p
libqgis-networkanalysis2.18.17 libqgis-server2.18.17 libqgispython2.18.17 libqh
```

Now that we have a clear understanding of how to update and upgrade our operating system, let's take a look at how to install a new application (package) within Kali Linux 2019. A very well-known vulnerability scanner is the **Open Vulnerability Assessment System (OpenVAS)**. However, OpenVAS is not included in Kali Linux 2019 by default. In this exercise, we will install the OpenVAS application on our Kali machine. To get started, ensure that you have an internet connection on your Kali machine.

Use the `apt-get install openvas` command to search for the repository and download and install the package with all its dependencies:

```
root@kali:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

This process should take a few minutes to complete. Ensure that you execute the `apt-get update` command prior to installing any packages on Kali Linux. Once the package (application) has been installed, it will appear within the designated category in the **Applications** menu, as shown in the following screenshot:



Please be sure to check the release notes for your version of Kali Linux at <https://www.kali.org/category/releases/>.

Sometimes, updating your source file will assist in updating, upgrading, and retrieving packages on Kali Linux. The latest updates to the `sources.list` file can be found at <https://docs.kali.org/general-use/kali-linux-sources-list-repositories>.

In the next section, we will take a deep dive into learning about three of the most essential tools in the Kali Linux operating system.

The find, locate, and which commands

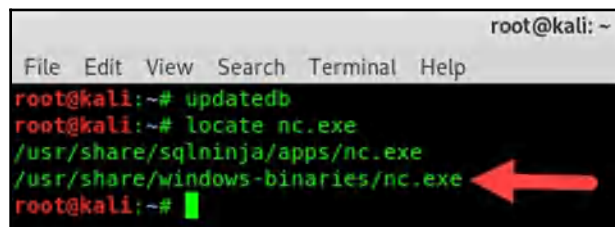
Within the Kali Linux operating system, there are many methods by which a user can locate files and directories. In this section, I will introduce you to the `find`, `locate`, and `which` utilities. Each of these utilities performs similar tasks, but returns the requested information a bit differently from each other.

Before we use any of these commands, we must first execute the `updatedb` command to build a local database for each file within our current filesystem on Kali Linux. This process usually takes a few seconds to complete.

In the following section, we will take a deeper look into each of the Linux utilities and how they are used.

The locate command

Once the database is completely built, we can use the `locate` utility to query the database for local files. In this example, we are attempting to locate the directory of the Netcat Windows executable file by using the `locate nc.exe` command:

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

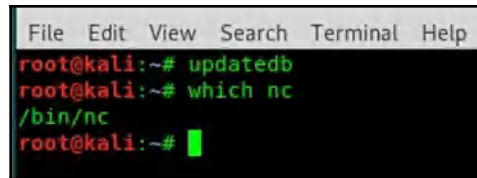
```
root@kali:~# updatedb
root@kali:~# locate nc.exe
/usr/share/sqlninja/apps/nc.exe
/usr/share/windows-binaries/nc.exe
```

A red arrow points to the second line of output, `/usr/share/windows-binaries/nc.exe`.

As we can see, the `locate` utility was able to retrieve the location of the `nc.exe` file within the filesystem for us.

The which command

Next, we are going to use the `which` utility to help us search for directories. Unlike the previous example, we do not need to specify the file extension; the `which` utility is used to locate the file path of an executable file. Simply put, the `which` utility will provide you with the file path only:

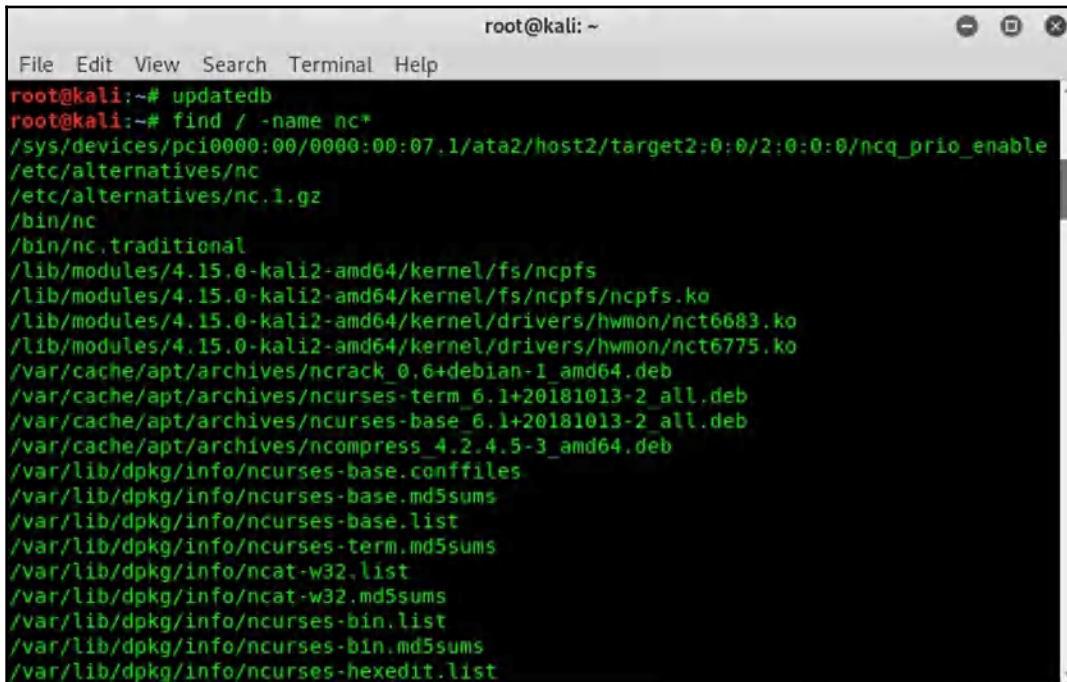


```
File Edit View Search Terminal Help
root@kali:~# updatedb
root@kali:~# which nc
/bin/nc
root@kali:~#
```

The preceding screenshot shows where the `which nc` command was used to retrieve the Netcat path within Kali Linux.

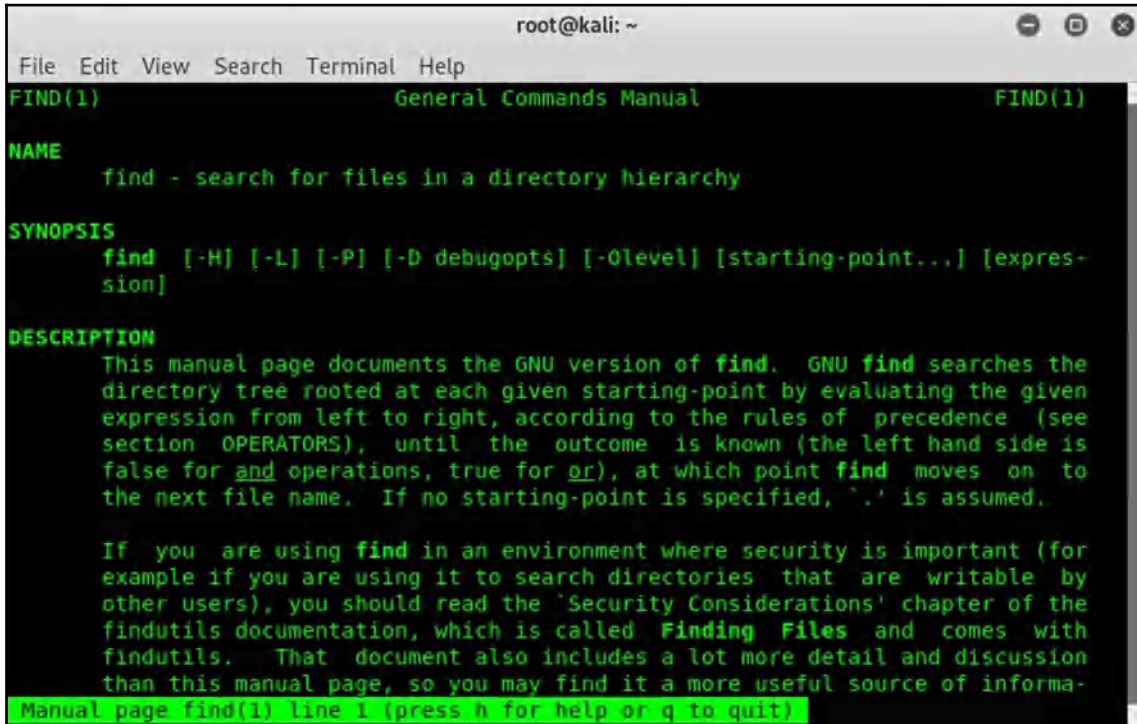
The find command

The `find` utility is a bit more aggressive than `locate` and `which`. The `find` utility will return all the results that contain the keyword or string we have specified. In our example, we've used the `find` command to provide us with a listing of all files (including their directories) that begin with `nc`:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# updatedb
root@kali:~# find / -name nc*
/sys/devices/pci0000:00/0000:00:07.1/ata2/host2/target2:0:0/2:0:0:0/ncq_prio_enable
/etc/alternatives/nc
/etc/alternatives/nc.1.gz
/bin/nc
/bin/nc.traditional
/lib/modules/4.15.0-kali2-amd64/kernel/fs/ncpfs
/lib/modules/4.15.0-kali2-amd64/kernel/fs/ncpfs/ncpfs.ko
/lib/modules/4.15.0-kali2-amd64/kernel/drivers/hwmon/nct6683.ko
/lib/modules/4.15.0-kali2-amd64/kernel/drivers/hwmon/nct6775.ko
/var/cache/apt/archives/ncrack_0.6+debian-1_amd64.deb
/var/cache/apt/archives/ncurses-term_6.1+20181013-2_all.deb
/var/cache/apt/archives/ncurses-base_6.1+20181013-2_all.deb
/var/cache/apt/archives/ncompress_4.2.4.5-3_amd64.deb
/var/lib/dpkg/info/ncurses-base.conffiles
/var/lib/dpkg/info/ncurses-base.md5sums
/var/lib/dpkg/info/ncurses-base.list
/var/lib/dpkg/info/ncurses-term.md5sums
/var/lib/dpkg/info/ncat-w32.list
/var/lib/dpkg/info/ncat-w32.md5sums
/var/lib/dpkg/info/ncurses-bin.list
/var/lib/dpkg/info/ncurses-bin.md5sums
/var/lib/dpkg/info/ncurses-hexedit.list
```

The `man` command can help us understand how a tool or utility works. The `man` command is used to provide us with the manual page for a tool. We can view the `man` page of the `find` utility using the `man find` command:



```
root@kali: ~  
File Edit View Search Terminal Help  
FIND(1)                                General Commands Manual                                FIND(1)  
  
NAME  
    find - search for files in a directory hierarchy  
  
SYNOPSIS  
    find [-H] [-L] [-P] [-D debugopts] [-O level] [starting-point...] [expression]  
  
DESCRIPTION  
    This manual page documents the GNU version of find. GNU find searches the directory tree rooted at each given starting-point by evaluating the given expression from left to right, according to the rules of precedence (see section OPERATORS), until the outcome is known (the left hand side is false for and operations, true for or), at which point find moves on to the next file name. If no starting-point is specified, . is assumed.  
  
    If you are using find in an environment where security is important (for example if you are using it to search directories that are writable by other users), you should read the 'Security Considerations' chapter of the findutils documentation, which is called Finding Files and comes with findutils. That document also includes a lot more detail and discussion than this manual page, so you may find it a more useful source of information.  
Manual page find(1) line 1 (press h for help or q to quit)
```

The `man` command can be very useful when you want to learn about new and existing tools on Linux.

In the next section, we will discuss how to manage services in Kali Linux and take a look at a few practical examples.

Managing Kali Linux services

The Kali Linux operating system can function as a server for various types of services, such as **Secure Shell (SSH)**, **Hypertext Transfer Protocol (HTTP)**, and many more. In this section, I will demonstrate how to enable and disable various services. Once a service is running on a system, an associated network port is opened. For example, if HTTP is enabled on a machine, the default logical port is 80; for SSH, the port is 22.



Further information on services and port number assignments can be found on the **Internet Assigned Numbers Authority (IANA)** website at <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>.

To enable a service in Kali Linux, we can use the `service <service-name> command` syntax. In our example, we are going to enable the Apache web server, and, using the `netstat -antp | grep <service-name>` command we can verify that the associated service is running and that the network port is open, as shown in the following screenshot:

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the following commands and output:

```
root@kali:~# service apache2 start
root@kali:~# netstat -antp | grep apache
tcp6      0      0 :::80                :::*                   LISTEN      2467/apache2
root@kali:~#
```

The last column contains the service name; in our exercise, we can see `apache2` listed. This indicates that the web services are running—specifically, that the Apache2 web service is active on Kali Linux.



To enable SSH, we can use the `service ssh start` command.

Additionally, since it's a web server, we can open our web browser and enter the loopback IP address, `127.0.0.1`, to verify that the default Apache web page is loading on our screen:

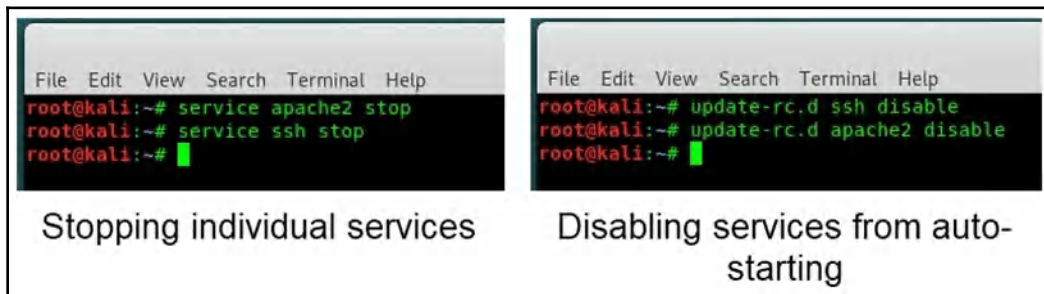


However, if our Kali Linux machine is powered off or restarted, the services that we previously enabled will revert back to their default start up settings. What if we want to ensure that certain services always start during the boot process of Kali Linux? This can be done by using the `update-rc.d <service-name> enable` command in the Terminal window:

```
File Edit View Search Terminal Help
root@kali:~# update-rc.d ssh enable
root@kali:~# update-rc.d apache2 enable
root@kali:~#
```


In our example, we have enabled the SSH service, which will allow us to remotely access our Kali Linux machine over a network securely. The HTTP server will allow us to access the web server pages.

Last but not least, we can disable individual services and disable services from automatically starting during the boot process, as shown in the following screenshot:



In the voice of Uncle from the Jackie Chan Adventures, "*One more thing!*", I recommend changing the default password for the root account on Kali Linux. To change the password, open the Terminal window and execute the `passwd` command. The interactive prompt will ask you to enter your new password and verify it.



Please note that when entering passwords on a Terminal interface on a Linux-based operating system, the characters you enter do not appear on the screen/Terminal.

In this section, you have learned the skills essential for using the Kali Linux operating system. These skills include navigating the filesystem, updating and installing software packages, and enabling and disabling services.

Summary

During the course of this chapter, we discussed the benefits of using the Kali Linux operating system as the preferred penetration testing distribution. We covered the basics of maneuvering and finding our way around the operating system, just as you would with any other operating system. Then, we took a look at updating our source file and upgrading our existing packages, and we demonstrated how to install a new application and remove outdated packages. Lastly, we covered how to use the `find`, `locate`, and `which` utilities to quickly find files and directories within the Kali Linux operating system.

Learning the essentials of Kali Linux will prove to be fruitful in your journey ahead. The skills taught in this chapter will help you understand the simple things when using Kali Linux, some of which are often overlooked. It would be pointless to know how to gather information on a target but not know how to find or locate files and directories within the Kali Linux operating system, so learning the basics will take you a long way.

In the next chapter, we will be covering **passive information gathering**, which is the beginning of the reconnaissance phase in penetration testing.

Questions

1. What was the predecessor of Kali Linux?
2. How do you update repositories on Kali Linux?
3. How do you upgrade current packages on Linux?
4. Which command installs a new application from the official online repository?
5. How can you quickly find a file within the filesystem?

Further reading

- **Kali Linux 2019.2 release information:** <https://www.kali.org/news/kali-linux-2019-2-release/>
- **Official Kali Linux documentation:** <https://www.kali.org/kali-linux-documentation/>