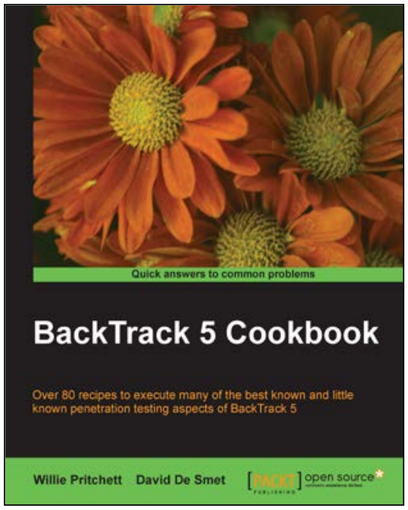
[PACKT] open source
PUBLISHING
community experience distilled

BackTrack 5 Cookbook

Willie Pritchett
David De Smet


Quick answers to common problems
BackTrack 5 Cookbook
Over 80 recipes to execute many of the best known and little known penetration testing aspects of BackTrack 5
Willie Pritchett
David De Smet
[PACKT] open source

Chapter No. 1
"Up and Running with BackTrack"

In this package, you will find:

A Biography of the authors of the book

A preview chapter from the book, Chapter NO.1 "Up and Running with BackTrack"

A synopsis of the book’s content

Information on where to buy this book

About the Authors

Willie Pritchett, MBA, 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 and data-driven application development and also in staffing services. He has worked with state and local government agencies, as well as helped 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 even the roughest days. A special thanks to all of my now colleagues, associates, and business partners who gave me a chance when I first got 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.

BackTrack 5 Cookbook

BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. BackTrack is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm.

BackTrack 5 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 BackTrack 5 and setting up a virtual environment in which 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 further learn about privilege escalation, radio network analysis, Voice over IP (VoIP), password cracking, and BackTrack forensics.

This book will serve as an excellent source of information for the security professional and novice equally. The book offers detailed descriptions and example recipes that allow you to quickly get up to speed on both BackTrack 5 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 BackTrack, shows you how to set up BackTrack in your testing environment and configure BackTrack to work within your network.

Chapter 2, Customizing BackTrack, looks at installing and configuring drivers for some of the popular video and wireless cards.

Chapter 3, Information Gathering, covers tools that can be used during the information gathering phase, including Maltego and Nmap.

Chapter 4, Vulnerability Identification, explains the usage of the Nessus and OpenVAS vulnerability scanners.

Chapter 5, Exploitation, covers the use of Metasploit through attacks on commonly used services.

Chapter 6, Privilege Escalation, explains the usage of tools such as Ettercap, SET, and Meterpreter.

Chapter 7, Wireless Network Analysis, shows how to use various tools to exploit the wireless network.

Chapter 8, Voice over IP (VoIP), covers various tools used to attack wireless phones and VoIP systems.

Chapter 9, Password Cracking, explains the use of tools to crack password hashes and user accounts.

Chapter 10, BackTrack Forensics, examines tools used to recover data and encryption.

1

Up and Running with BackTrack

In this chapter, we will cover:

- Installing BackTrack to a hard disk drive
- Installing BackTrack to a USB drive with persistent memory
- Installing BackTrack on VirtualBox
- Installing BackTrack using VMware Tools
- Fixing the splash screen
- Changing the root password
- Starting network services
- Setting up the wireless network

Introduction

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

For all the recipes in this and the following chapters, we will use BackTrack 5 R3 using GNOME 64-bit as the **Window Manager** (**WM**) flavor and architecture (`http://www.backtrack-linux.org/downloads/`). The use of KDE as the WM is not covered in this book, but still, you will be able to follow the recipes without much trouble.

Installing BackTrack 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 BackTrack at full speed without the DVD.

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

Getting ready

Before explaining the procedure, the following requirement needs to be met:

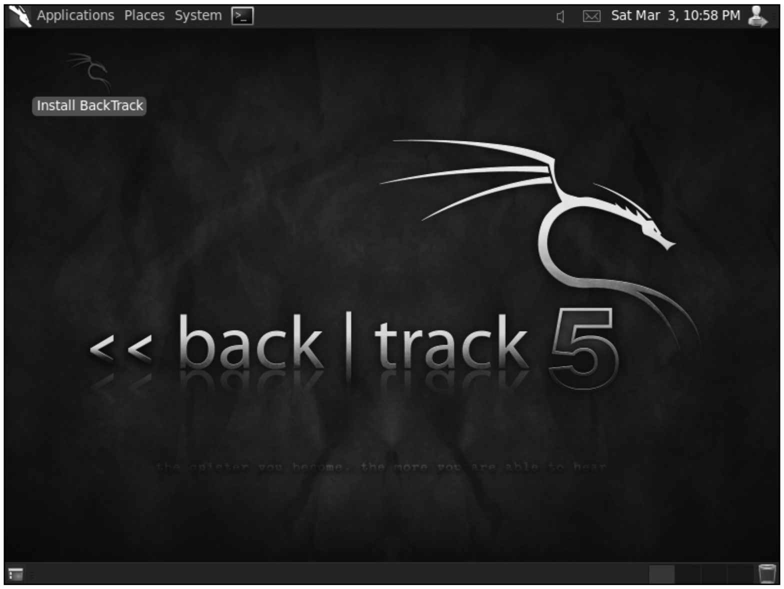
- A minimum of 25 GB of free disk space
- A BackTrack Live DVD

Let's begin the installation. Insert and boot the BackTrack Live DVD.

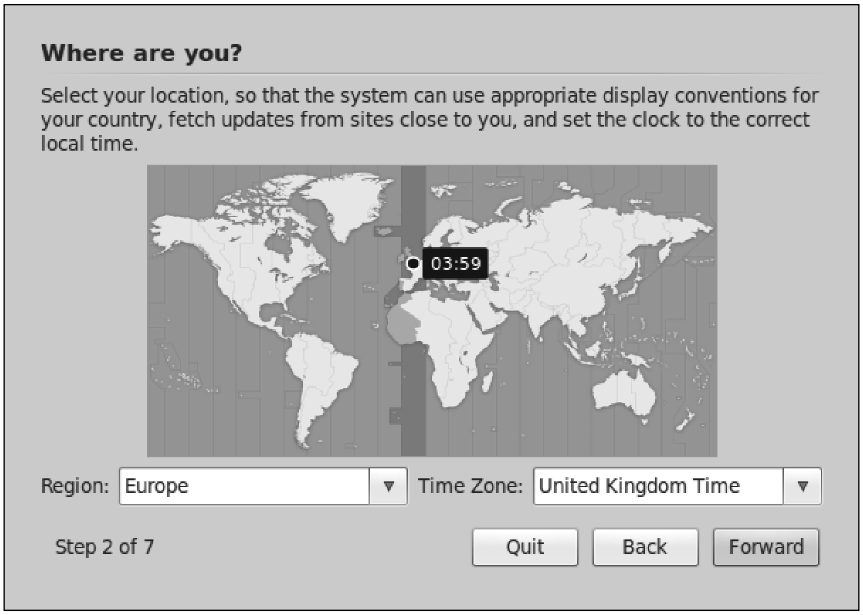
How to do it...

Let's begin the process of installing BackTrack to the hard drive:

1. When the desktop environment finishes loading, double-click on **Install BackTrack** to run the installation wizard:


Applications Places System
Sat Mar 3, 10:58 PM
Install BackTrack
<< back | track 5
the quieter you become, the more you are able to hear

2. Select your language and click on the **Forward** button.
3. Select your geographical location and click on **Forward**:



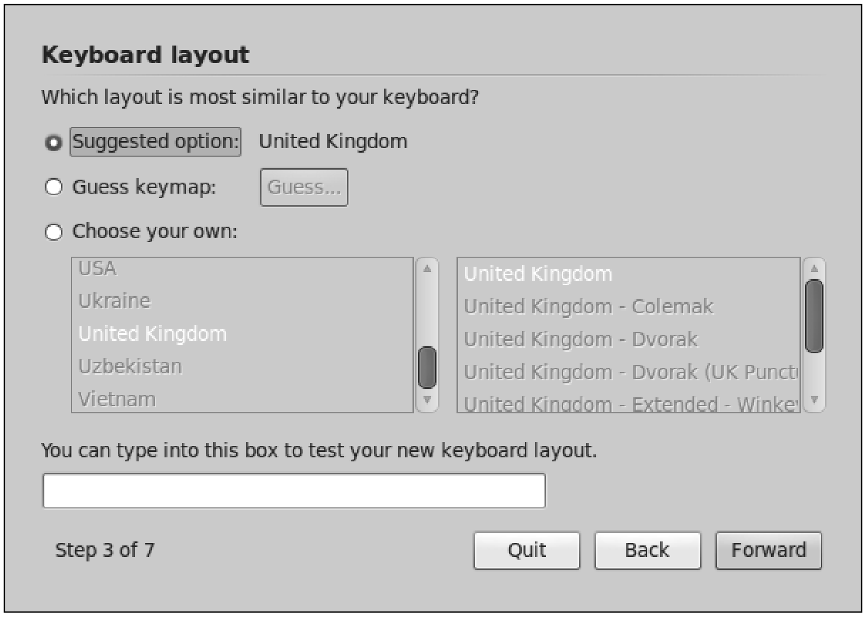
Where are you?

Select your location, so that the system can use appropriate display conventions for your country, fetch updates from sites close to you, and set the clock to the correct local time.

Region: Europe   Time Zone: United Kingdom Time

Step 2 of 7

4. Choose your keyboard layout and click on **Forward** to continue to the next step:



Keyboard layout

Which layout is most similar to your keyboard?

● Suggested option: United Kingdom

○ Guess keymap: Guess...

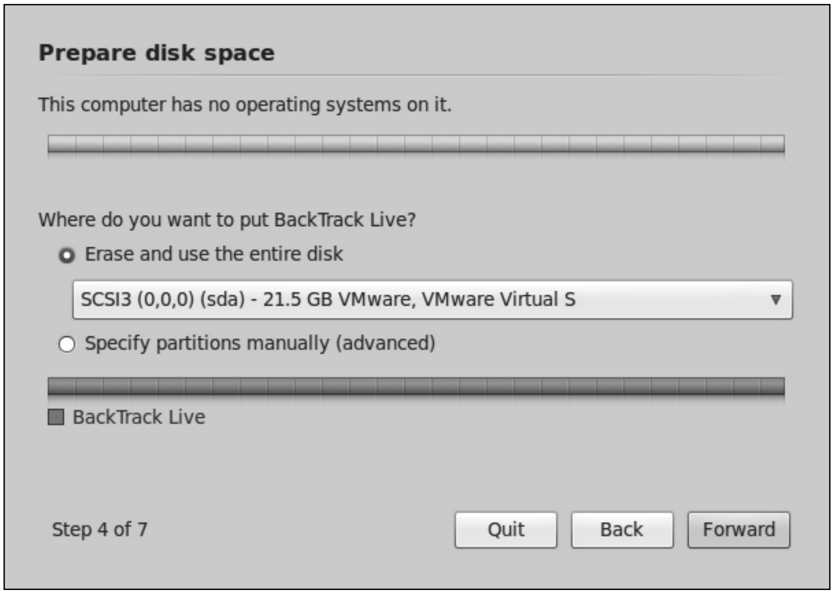
○ Choose your own:

USA	United Kingdom
Ukraine	United Kingdom - Colemak
United Kingdom	United Kingdom - Dvorak
Uzbekistan	United Kingdom - Dvorak (UK Puncti
Vietnam	United Kingdom - Extended - Winke'

You can type into this box to test your new keyboard layout.

Step 3 of 7

5. Leave the default option, which will erase and use the entire disk. Click on the **Forward** button one more time:



Prepare disk space

This computer has no operating systems on it.

Where do you want to put BackTrack Live?

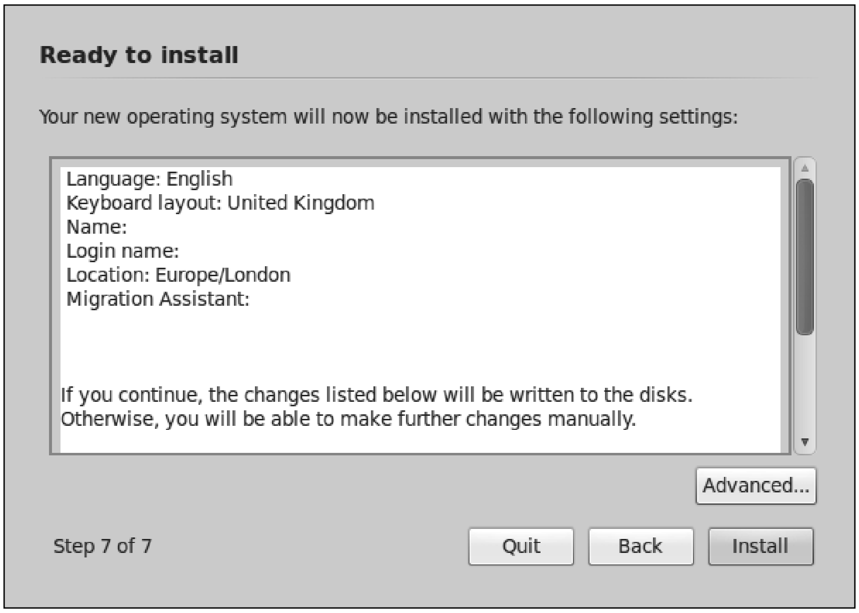
● Erase and use the entire disk

SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

○ Specify partitions manually (advanced)

▨ BackTrack Live

6. The installation summary will appear. Check whether the settings are correct and click on the **Install** button to begin:



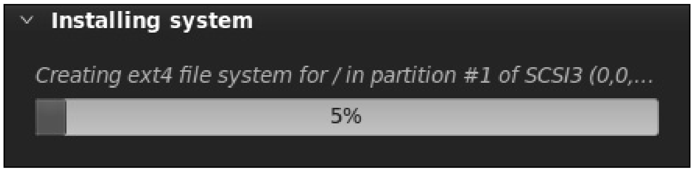
Ready to install

Your new operating system will now be installed with the following settings:

Language: English
Keyboard layout: United Kingdom
Name:
Login name:
Location: Europe/London
Migration Assistant:

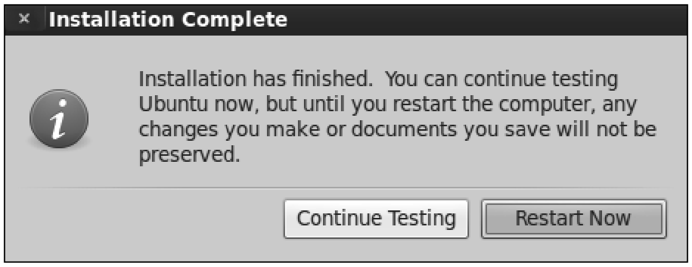
If you continue, the changes listed below will be written to the disks.
Otherwise, you will be able to make further changes manually.

7. The installer will start and in a few minutes will be completed:



Creating ext4 file system for / in partition #1 of SCSI3 (0,0,...

8. Finally, the installation will be complete and you'll be ready to start BackTrack without the install DVD. Click on **Restart Now** to reboot your computer. To log in, use the default username `root` and password `toor`.



Installation has finished. You can continue testing Ubuntu now, but until you restart the computer, any changes you make or documents you save will not be preserved.

Installing BackTrack to a USB drive with persistent memory

Having a BackTrack 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 BackTrack with us at all times.

Thanks to open source tools such as UNetbootin, we can create a bootable Live USB drive of a vast majority of Linux distributions, including BackTrack with persistent storage.

Getting ready

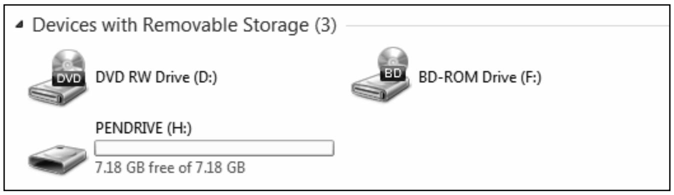
The following tools and preparation are needed in order to continue:

- A FAT32 formatted USB drive with a minimum capacity of 8 GB
- A BackTrack ISO image
- UNetbootin (`unetbootin.sourceforge.net/unetbootin-windows-latest.exe`)
- You can download BackTrack 5 from `http://www.backtrack-linux.org/downloads/`

How to do it...

Let's begin the process of installing BackTrack 5 to a USB drive:

1. Insert our previously formatted USB drive:



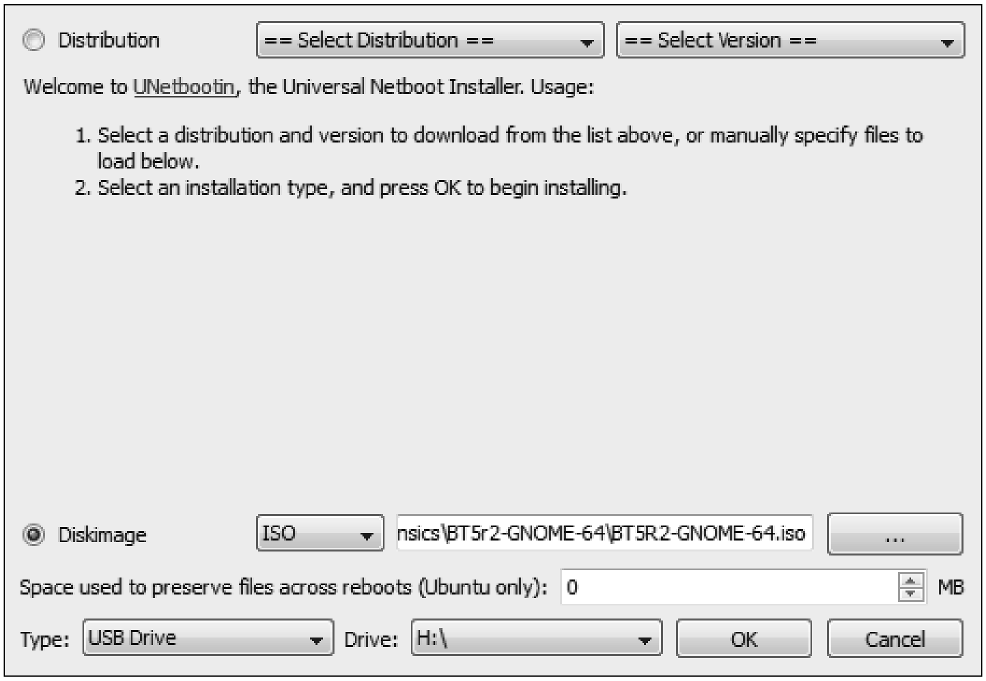
Devices with Removable Storage (3)

DVD RW Drive (D:)

BD-ROM Drive (F:)

PENDRIVE (H:)
7.18 GB free of 7.18 GB

2. Start **UNetbootin** as administrator.
3. Choose the **Diskimage** option and select the location of the BackTrack DVD ISO image:



○ Distribution == Select Distribution == == Select Version ==

Welcome to UNetbootin, the Universal Netboot Installer. Usage:

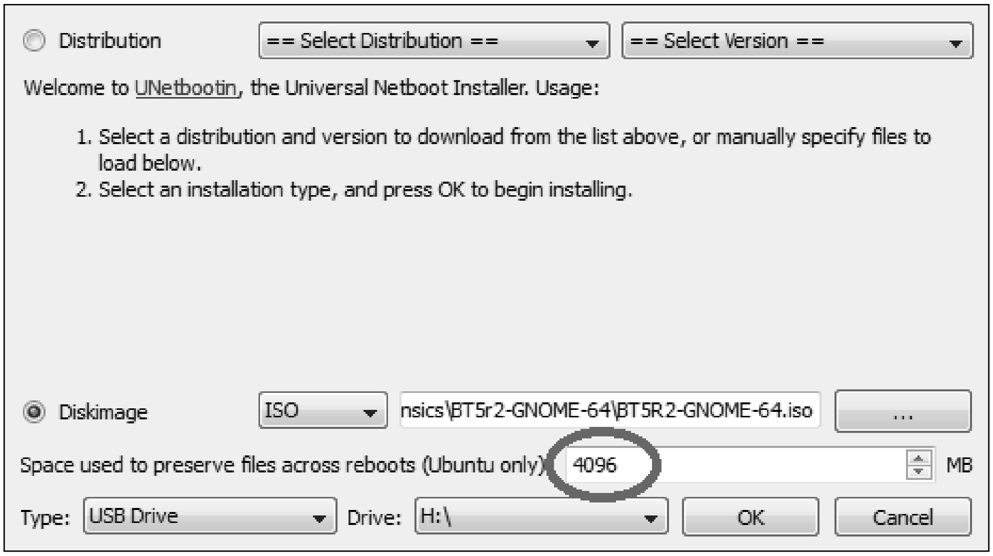
1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

● Diskimage ISO nsics\BT5r2-GNOME-64\BT5R2-GNOME-64.iso ...

Space used to preserve files across reboots (Ubuntu only): 0 MB

Type: USB Drive Drive: H:\ OK Cancel

4. Set the amount of space to be used for persistence. We're going to use `4096` MB for our 8 GB USB thumb drive:



○ Distribution == Select Distribution == == Select Version ==

Welcome to UNetbootin, the Universal Netboot Installer. Usage:

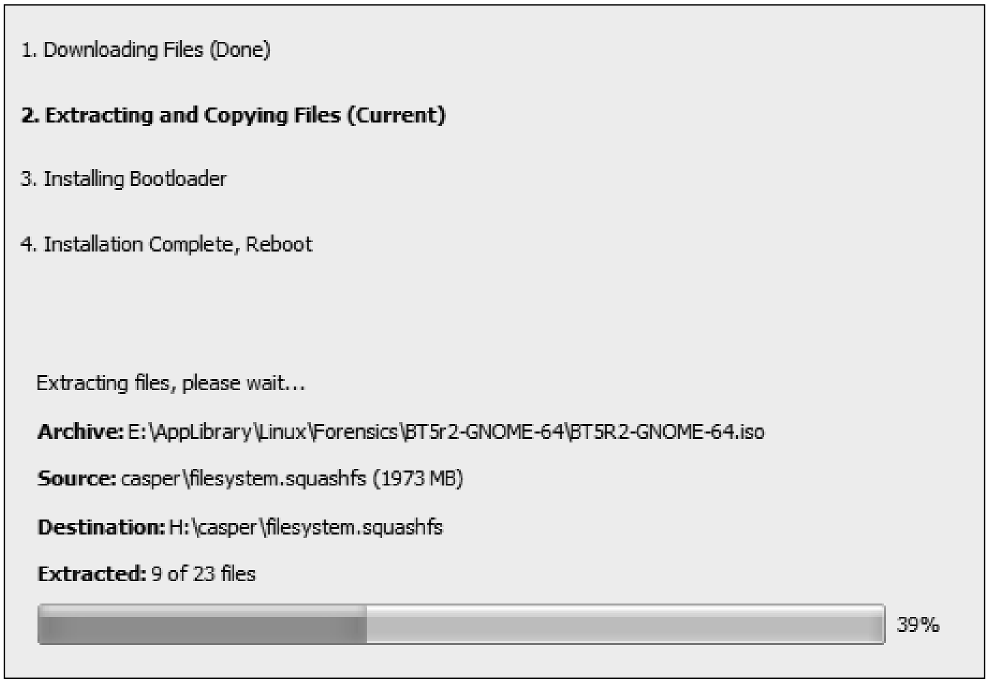
1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

● Diskimage ISO nsics\BT5r2-GNOME-64\BT5R2-GNOME-64.iso

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

Type: USB Drive Drive: H:\

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:



1. Downloading Files (Done)

2. Extracting and Copying Files (Current)

3. Installing Bootloader

4. Installation Complete, Reboot

Extracting files, please wait...

Archive: E:\AppLibrary\Linux\Forensics\BT5r2-GNOME-64\BT5R2-GNOME-64.iso

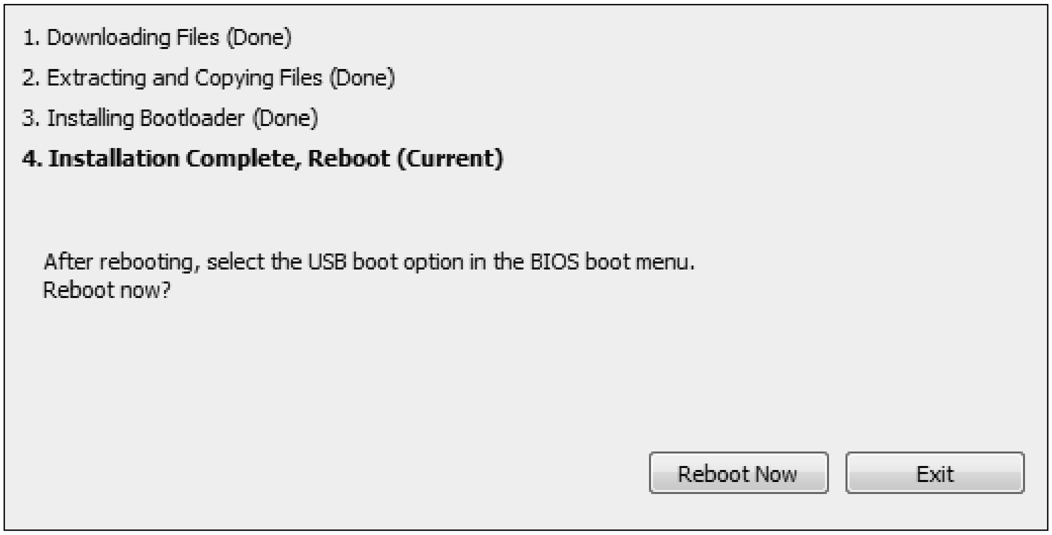
Source: casper\filesystem.squashfs (1973 MB)

Destination: H:\casper\filesystem.squashfs

Extracted: 9 of 23 files

39%

7. The installation is complete and we're ready to reboot the computer and boot from the newly created BackTrack 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?

If you're concerned about the information stored in the USB drive, you can increase the security by creating an encrypted USB drive. See the *Backtrack 5 – Bootable USB Thumb Drive with "Full" Disk Encryption* article for details at `http://www.infosecramblings.com/backtrack/backtrack-5-bootable-usb-thumb-drive-with-full-disk-encryption/`.

Installing BackTrack on VirtualBox

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

Getting ready

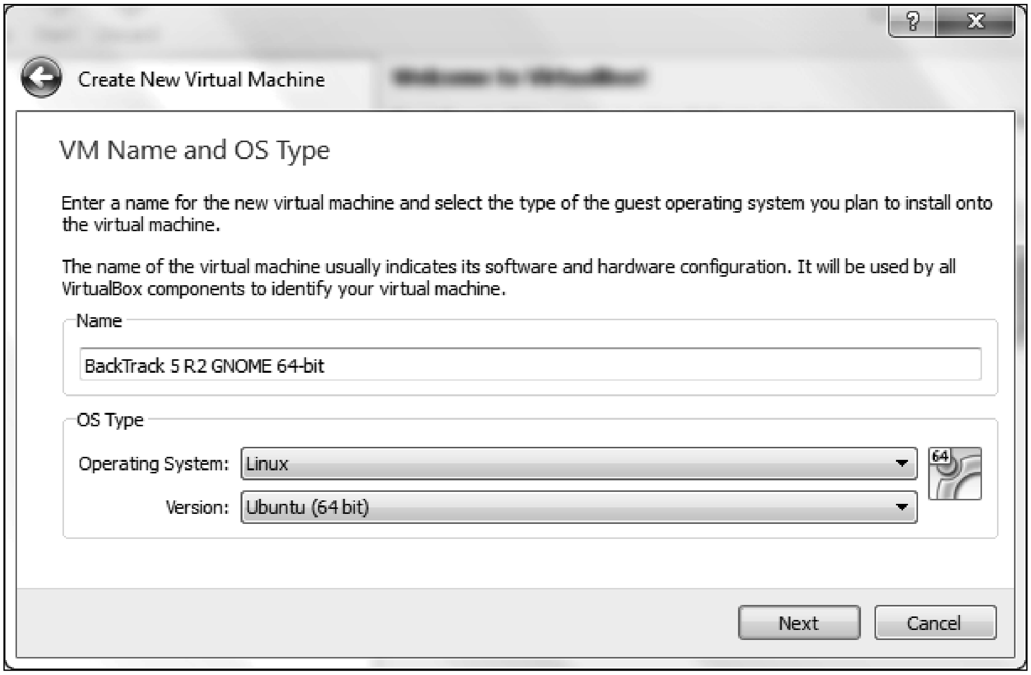
The required prerequisites are listed as follows:

- Latest version of VirtualBox (`https://www.virtualbox.org/wiki/Downloads`).
- A copy of the BackTrack ISO image. You can download a copy from `http://www.backtrack-linux.org/downloads/`.

How to do it...

Let's begin the process of installing BackTrack on Virtualbox:

1. Launch VirtualBox and click on **New** to start the Virtual Machine Wizard.
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 case, we selected an operating system of **Linux** and **Ubuntu (64 bit)** for the version. Click on the **Next** button to continue:



Create New Virtual Machine

VM Name and OS Type

Enter a name for the new virtual machine and select the type of the guest operating system you plan to install onto the virtual machine.

The name of the virtual machine usually indicates its software and hardware configuration. It will be used by all VirtualBox components to identify your virtual machine.

Name

BackTrack 5 R2 GNOME 64-bit

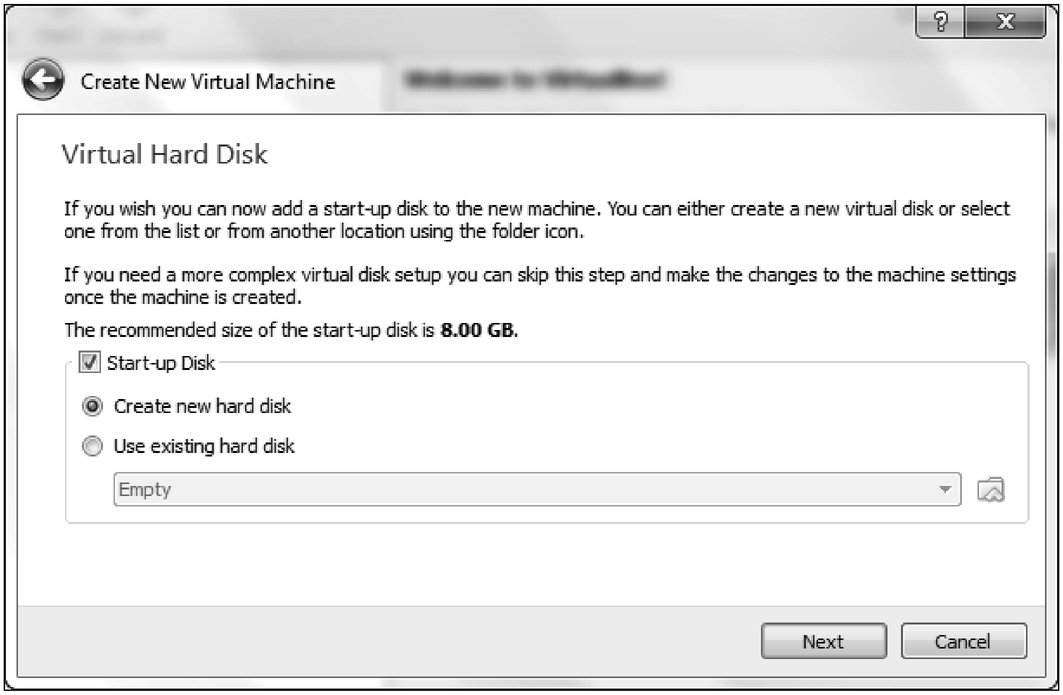
OS Type

Operating System: 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:



Virtual Hard Disk

If you wish you can now add a start-up disk to the new machine. You can either create a new virtual disk or select one from the list or from another location using the folder icon.

If you need a more complex virtual disk setup you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the start-up disk is **8.00 GB**.

☑ Start-up Disk

● Create new hard disk

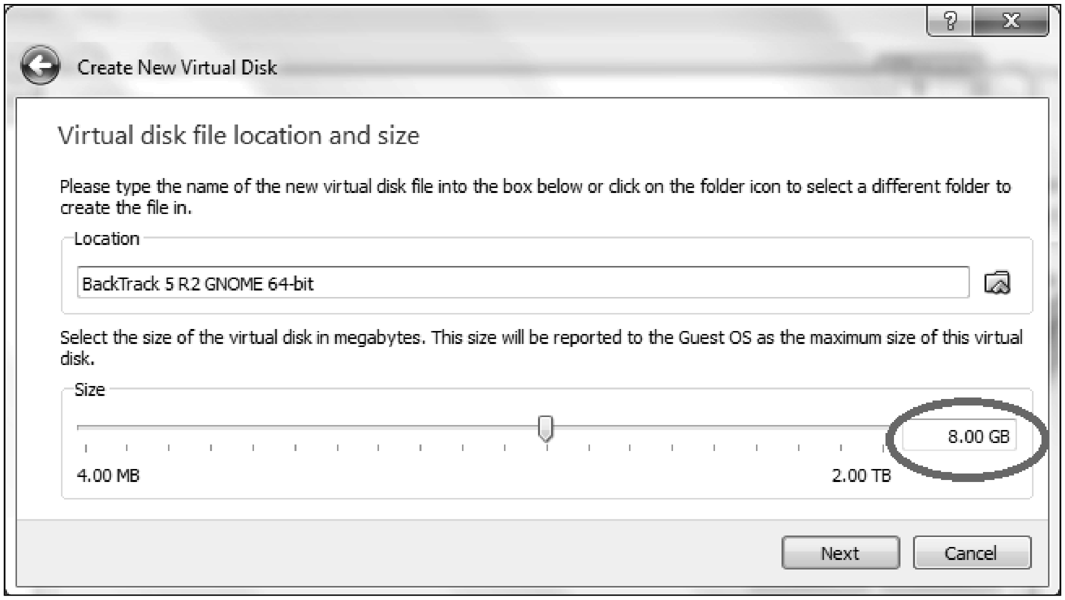
○ Use existing hard disk

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:



Virtual disk file location and size

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

Location

BackTrack 5 R2 GNOME 64-bit

Select the size of the virtual disk in megabytes. This size will be reported to the Guest OS as the maximum size of this virtual disk.

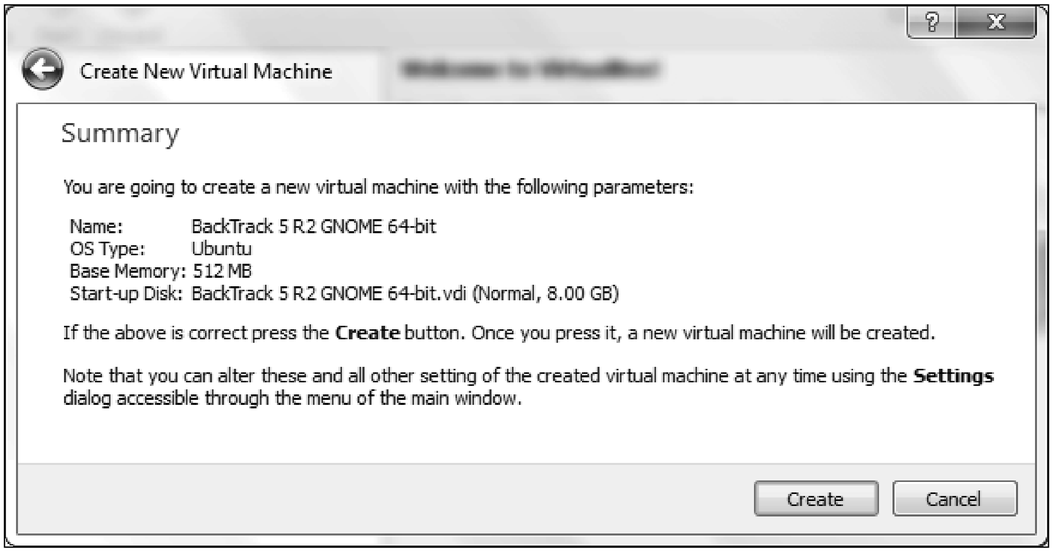
Size

8.00 GB

4.00 MB

2.00 TB

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:



Summary

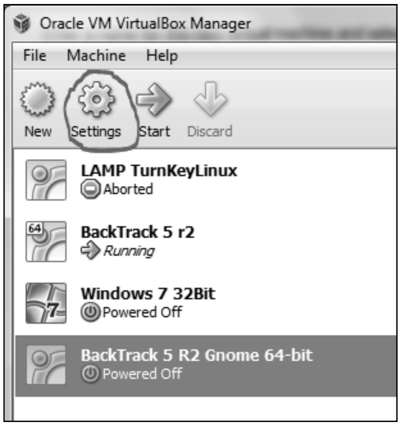
You are going to create a new virtual machine with the following parameters:

```
Name:          BackTrack 5 R2 GNOME 64-bit
OS Type:       Ubuntu
Base Memory:   512 MB
Start-up Disk: BackTrack 5 R2 GNOME 64-bit.vdi (Normal, 8.00 GB)
```

If the above is correct press the **Create** button. Once you press it, a new virtual machine will be created.

Note that you can alter these and all other setting of the created virtual machine at any time using the **Settings** dialog accessible through the menu of the main window.

10. With the new virtual machine created, we're ready to install BackTrack.
11. On the VirtualBox main window, highlight **BackTrack 5 R2 Gnome 64-bit** and then click on the **Settings** button:



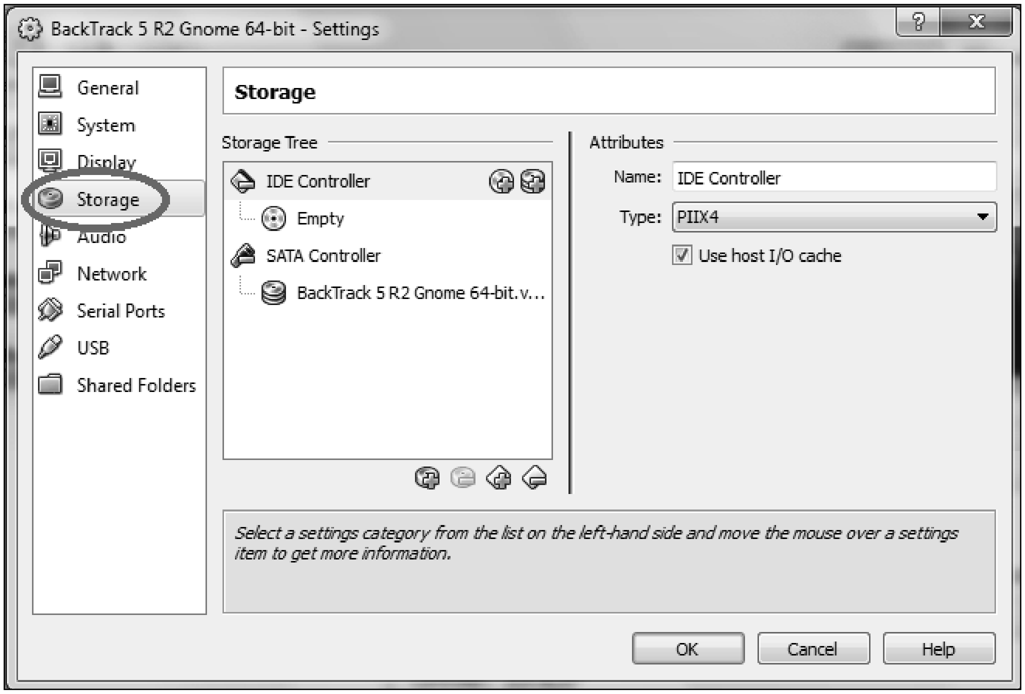
LAMP TurnKeyLinux
Aborted

BackTrack 5 r2
Running

Windows 7 32Bit
Powered Off

BackTrack 5 R2 Gnome 64-bit
Powered Off

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:

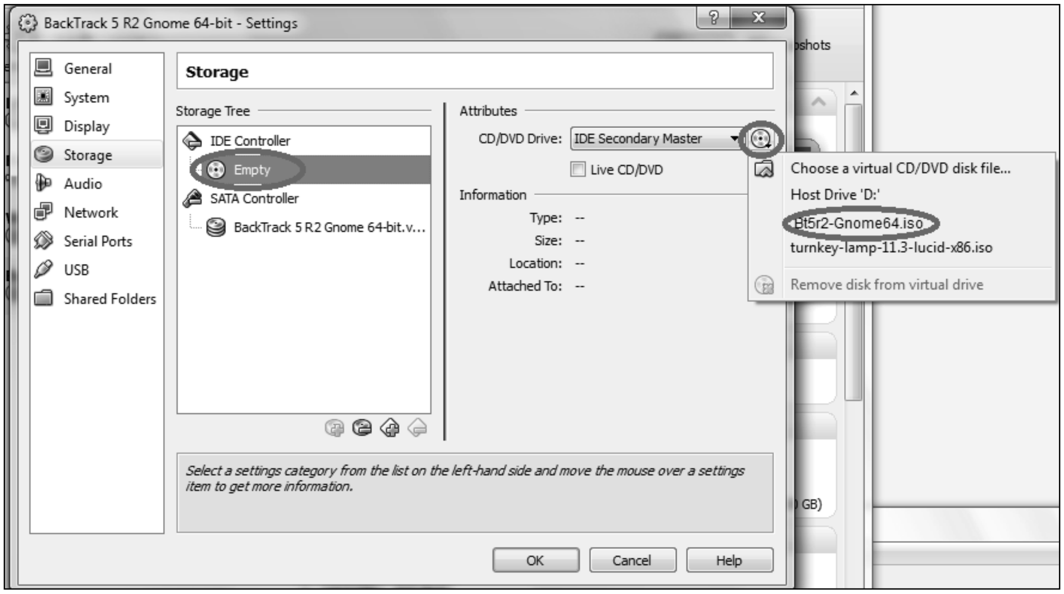


IDE Controller
Empty
SATA Controller
BackTrack 5 R2 Gnome 64-bit.v...

Name: IDE Controller
Type: PIIX4
☑ Use host I/O cache

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

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 BackTrack ISO file from the list. If the BackTrack 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

Information

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. Now that you are back on the main window, click on the **Start** button and then click inside the newly created window to proceed with the installation. The installation steps are covered in the *Installing BackTrack 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 BackTrack using VMware Tools

In this recipe, we will demonstrate how to install BackTrack 5 as a virtual machine using VMware Tools.

Getting ready

The following requirement needs to be fulfilled:

- A previously installed BackTrack VMware virtual machine
- An Internet connection

How to do it...

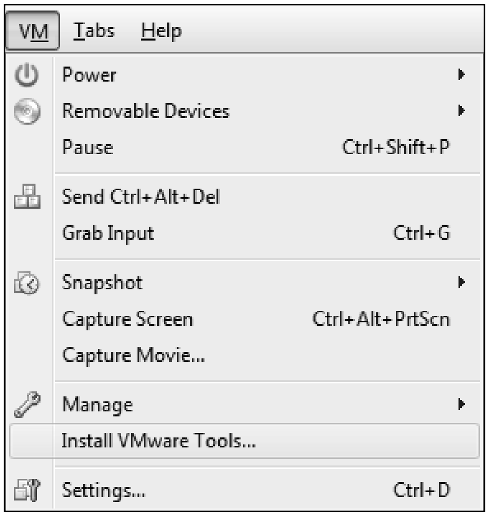
Let's begin the process of installing BackTrack 5 on VMware:

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, click on **VM** | **Install VMware Tools...**:



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

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

   > Replace the file name 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

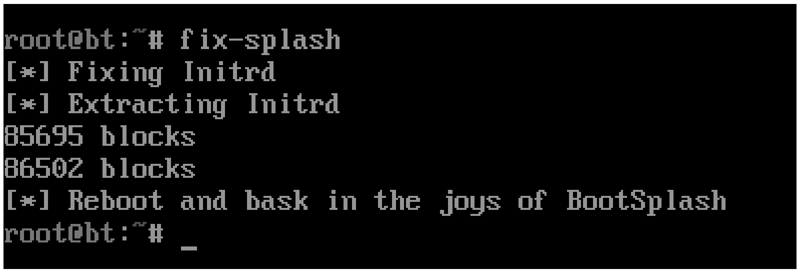
The first time we boot into our newly installed BackTrack system, we would notice that the splash screen disappeared. In order to manually fix it, we need to extract the Initrd, modify it, and then compress it again. Thankfully, there's an automated bash script created by Mati Aharoni (also known as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

The following screenshot shows the execution of the command:



```
root@bt:~# fix-splash
[*] Fixing Initrd
[*] Extracting Initrd
85695 blocks
86502 blocks
[*] Reboot and bask in the joys of BootSplash
root@bt:~# _
```

Changing the root password

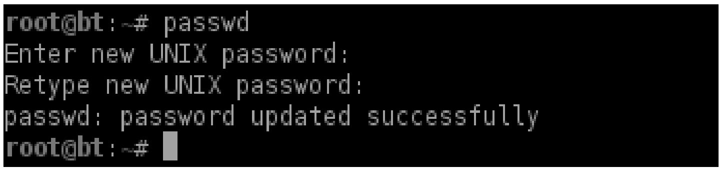
For security reasons, it's recommended as a good practice to always change the default root password. This would not prevent a malicious user obtaining access to our system, but surely will make things harder.

How to do it...

To change the default root password, just issue the following command:

```
passwd
```

Enter you new password and press *Enter*. You will also be asked to retype your password:



```
root@bt:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@bt:~# █
```

Starting network services

BackTrack 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

A connection to the network with a valid IP address is needed in order to continue.

How to do it...

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

1. Start the Apache web server:

   ```
   service apache2 start
   ```

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

2. To start the 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
   ```

   Here, `<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
   ```

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

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

> You can also start/stop services from the BackTrack Start menu by selecting **Backtrack | Services** from the **Start** menu.

Setting up the wireless network

In this final recipe of the chapter, we will cover the steps used to connect to our wireless network with security enabled, by using Wicd Network Manager and supplying our encryption details. The advantages of setting up our wireless network is that it enables us to use BackTrack 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.

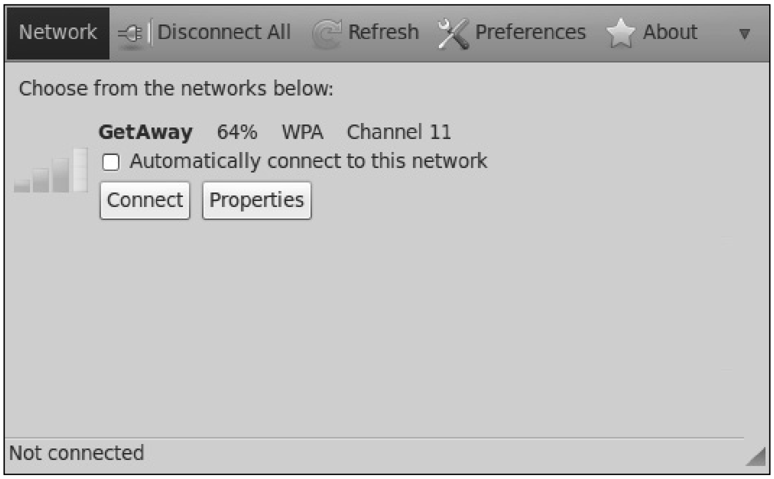
How to do it...

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:



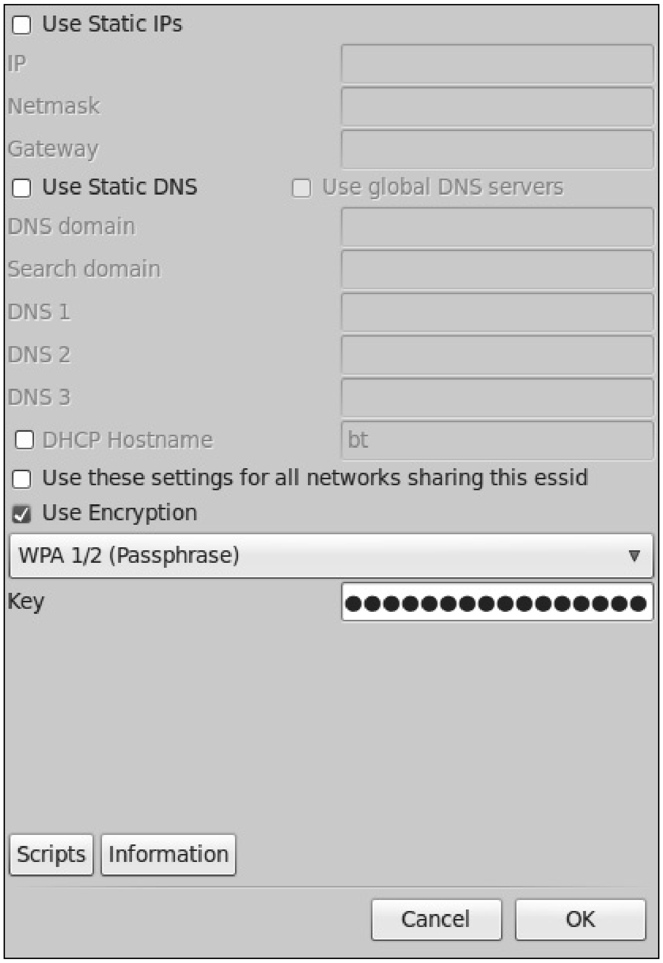
Choose from the networks below:

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 step began by starting the network manager and connecting to our router.

Where to buy this book

You can buy BackTrack 5 Cookbook from the Packt Publishing website: `http://www.packtpub.com/backtrack-5-penetration-testing-cookbook/book`.

Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

[PACKT] PUBLISHING open source community experience distilled

www.PacktPub.com