SYNGRESS

Hacking with Kali

Practical Penetration Testing Techniques

James Broad
Andrew Bindner

Hacking with Kali

Hacking with Kali

Practical Penetration Testing Techniques

James Broad

Andrew Bindner

ELSEVIER

AMSTERDAM ● BOSTON ● HEIDELBERG ● LONDON
NEW YORK ● OXFORD ● PARIS ● SAN DIEGO
SAN FRANCISCO ● SINGAPORE ● SYDNEY ● TOKYO
Syngress is an imprint of Elsevier

SYNGRESS®

Publisher: Steve Elliot
Acquisitions Editor: Chris Katsaropoulos
Editorial Project Manager: Benjamin Rearick
Project Manager: Mohana Natarajan
Designer: Matthew Limbert

Syngress is an imprint of Elsevier

225 Wyman Street, Waltham, MA 02451, USA

First edition **2014**

Library of Congress Cataloging-in-Publication Data
Application Submitted

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-407749-2

Dedication

I would like to dedicate this book to my family, who have always stood by me. Lisa, Teresa, and Mary, my sisters, have always been there for me. My wife, Dee, and children Micheal and Tremara give me the reason to continue learning and growing. My extended family made of friends, new and old, makes life more exciting and are far too many to list, but include Amber and Adam, Vince and Annette, Darla, Travis and Kim, Steve and Sharon.

Thank you all!

If you aren't doing, you're dying. Life is doing.

Jeff Olson

CHAPTER 1

Introduction

INFORMATION IN THIS CHAPTER

- Book Overview and Key Learning Points
- Book Audience
- Diagrams, Figures, and Screen Captures
- Common Terms
- Kali Linux History

BOOK OVERVIEW AND KEY LEARNING POINTS

This book will walk the reader through the penetration testing lifecycle using the most advanced live disk available today, Kali Linux. After this brief introduction, the chapter details how to find, download, install, and customize Kali Linux. Next a brief introduction to basic Linux configurations and settings will ensure basic commands and settings are understood. The remainder of the book is devoted to the penetration testing lifecycle—Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting. While there are hundreds of different tools on the Kali Linux distribution, each chapter covering the penetration testing lifecycle will cover the tools most commonly used in that phase. The reporting phase will detail reports that can be used to present findings to management and leadership and a Rules of Engagement (ROE) template that can be used before beginning a penetration test.

BOOK AUDIENCE

Technical Professionals

Technical professionals in a wide range of specialties can gain benefit from learning how penetration testers work. By gaining this understanding these

Hacking with Kali. DOI: http://dx.doi.org/10.1016/B978-0-12-407749-2.00001-X

professionals will better know the basic concepts and techniques used by penetration testers, this knowledge can then be used to better secure their information systems. These specialties include, but are not limited to, server administrators, network administrators, Database Administrators, and Help Desk Professionals.

Those technical professionals that want to transition into becoming a professional penetration tester will gain a good deal of knowledge by reading this book. The underlying understanding that these technical experts have in the various specialties gives them a distinct advantage when becoming a penetration tester. Who better to test the secure configuration of a server than a penetration tester that has extensive knowledge in the administration of server technologies? This is true for other specialties as well.

This book will introduce these technical professionals to the world of penetration testing, and the most common tool used by penetration testers, the Linux Live Disk. By following the examples and instructions in the coming chapters, these professionals will be on the way to understanding or becoming a penetration tester.

Security Engineers

Those security engineers that are striving to better secure the systems they develop and maintain will gain a wealth of knowledge by understanding the penetration testing mindset and lifecycle. Armed with this knowledge, these engineers can "bake in" security features on the systems they are developing and supporting.

Students in Information Security and Information Assurance Programs

Understanding the world of penetration testing will give these students insight into one of the most rewarding, and frustrating, professions in the information technology field. By being introduced to penetration testing early in their careers, these students may decide a career in penetration testing is the right choice for them.

Who This Book Is Not for

This book will not give you the skills and experience to break into the National Security Agency (NSA) or a local bank branch, and I suggest no one attempts to do this. This book is not for someone that has been conducting professional penetration tests for a number of years and fully understands how each tool on the Backtrack/Kali Linux disk works. Anyone with intentions of breaking the law, as the intention of the book is to introduce more people to penetration testing as a way to better secure information systems.

DIAGRAMS, FIGURES, AND SCREEN CAPTURES

Diagrams figures and charts in this book are simplified to provide a solid understanding of the material presented. This is done to illustrate the basic technical concepts and techniques that will be explained in this text.

Screen captures are used throughout this book to illustrate commands and actions that will be occurring in the Kali Linux environment and are included to provide further clarification of the topic. Depending on the configuration and version of Kail Linux, these screen captures may differ slightly from what will be displayed locally. This should not impact learning the basics of penetration testing and should only be slight.

WELCOME

This chapter will serve as an introduction to the exciting and ever expanding world of the professional ethical penetration tester. Penetration testing, or more simply pentesting, is a technical process and methodology that allows technical experts to simulate the actions and techniques of a hacker or hackers attempting to exploit a network or an information system. This book will walk the reader through the steps that are normally taken as a penetration tester develops an understanding of a target, analyzes the target, and attempts to break in. The book wraps up with a chapter on writing the reports and other documents that will be used to present findings to organizational leadership on the activities of the penetration test team and the flaws discovered in the system. The last chapter also includes a basic ROE template that should be formalized and approved before any penetration testing starts. It is important to only conduct penetration tests on systems that have been authorized and to work within the requirements of the approved ROE.

PENETRATION TESTING LIFECYCLE

There are a number of different penetration testing lifecycle models in use today. By far the most common is the methodology and lifecycle defined and used by the EC-Council Certified Ethical Hacker (EC C|EH) program. This five-phase process takes the tester through Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks [1]. This book will follow the modified penetration testing lifecycle illustrated by Patrick Engebretson in his book "The Basics of Hacking and Penetration Testing" [2]. This process follows the basic phases used by the C|EH but will not cover the final phase, Covering Tracks. This was a conscious decision to remove this phase from this book as many of the techniques in that final phase are best explained in a more advanced book.

TERMS

There are a number of common terms that often come into debate when discussing penetration testing. Different professions, technical specialties, and even members of the same team have slightly different understandings of the terms used in this field. For this reason, the following terms and associated definitions will be used in this book.

Penetration Testing, Pentesting

Penetration testing is the methodology, process, and procedures used by testers within specific and approved guidelines to attempt to circumvent an information systems protections including defeating the integrated security features of that system. This type of testing is associated with assessing the technical, administrative, and operational settings and controls of a system. Normally penetration tests only assess the security of the information system as it is built. The target network system administrators and staff may or may not know that a penetration test is taking place.

Red Team, Red Teaming

Red Teams simulate a potential adversary in methodology and techniques. These teams are normally larger than a penetration testing team and have a much broader scope. Penetration testing itself is often a subcomponent of a Red Team Exercise, but these exercises test other functions of an organizations security apparatus. Red Teams often attack an organization through technical, social, and physical means, often using the same techniques used by Black Hat Hackers to test the organization or information systems protections against these hostile actors. In addition to Penetration Testing, the Red Team will perform Social Engineering attacks, including phishing and spear phishing and physical attacks including dumpster diving and lock picking to gain information and access. In most cases, with the exception a relatively small group, the target organizations staff will not know a Red Team Exercise is being conducted.

Ethical Hacking

An Ethical Hacker is a professional penetration tester that attacks systems on behalf of the system owner or organization owning the information system. For the purposes of this book, Ethical Hacking is synonymous with Penetration Testing.

White Hat

White Hat is a slang term for an Ethical Hacker or a computer security professional that specializes in methodologies that improve the security of information systems.

Black Hat

Black Hat is a term that identifies a person that uses technical techniques to bypass a systems security without permission to commit computer crimes. Penetration Testers and Red Team members often use the techniques used by Black Hats to simulate these individuals while conducting authorized exercises or tests. Black Hats conduct their activities without permission and illegally.

Grey Hat

Grey Hat refers to a technical expert that straddles the line between White Hat and Black Hat. These individuals often attempt to bypass the security features of an information system without permission, not for profit but rather to inform the system administrators of discovered weaknesses. Grey Hats normally do not have permission to test systems but are usually not after personal monetary gain.

Vulnerability Assessment, Vulnerability Analysis

A vulnerability analysis is used to evaluate the security settings of an information system. These types of assessments include the evaluation of security patches applied to and missing from the system. The Vulnerability Assessment Team, or VAT, can be external to the information system or part of the information systems supporting staff.

Security Controls Assessment

Security Controls Assessments evaluate the information systems compliance with specific legal or regulatory requirements. Examples of these requirements include, but are not limited to, the Federal Information Security Management Act (FISMA), the Payment Card Industry (PCI), and Health Insurance Portability and Accountability Act (HIPAA). Security Control Assessments are used as part of the Body of Evidence (BOE) used by organizations to authorize an information system for operation in a production environment. Some systems require penetration tests as part of the security control assessment.

Malicious User Testing, Mal User Testing

In Malicious User Testing, the assessor assumes the role of trusted insider acting maliciously, a malicious user, or more simply a maluser. In these tests, the assessor is issued the credentials of an authorized general or administrative user, normally as a test account. The assessor will use these credentials to attempt to bypass security restrictions including viewing documents and settings in a way the account was not authorized, changing settings that should

not be changed, and elevating his or her own permissions beyond the level the account should have. Mal user testing simulates the actions of a rogue trusted insider.

Social Engineering

Social Engineering involves attempting to trick system users or administrators into doing something in the interest if the social engineer, but beyond the engineer's access or rights. Social Engineering attacks are normally harmful to the information system or user. The Social Engineer uses people's inherent need to help others to compromise the information system. Common Social Engineering techniques include trying to get help desk analysts to reset user account passwords or have end users reveal their passwords enabling the Social Engineer to log in to accounts they are not authorized. Other Social Engineering techniques include phishing and spear phishing.

Phishing

In Phishing (pronounced like fishing), the social engineer attempts to get the targeted individual to disclose personal information like user names, account numbers, and passwords. This is often done by using authentic looking, but fake, emails from corporations, banks, and customer support staff. Other forms of phishing attempt to get users to click on phony hyperlinks that will allow malicious code to be installed on the targets computer without their knowledge. This malware will then be used to remove data from the computer or use the computer to attack others. Phishing normally is not targeted at specific users but may be everyone on a mailing list or with a specific email address extension, for example every user with an "@foo.com" extension.

Spear Phishing

Spear Phishing is a form of phishing in which the target users are specifically identified. For example, the attacker may research to find the email addresses of the Chief Executive Officer (CEO) of a company and other executives and only phish these people.

Dumpster Diving

In Dumpster Diving, the assessor filters through trash discarded by system users and administrators looking for information that will lead to further understanding of the target. This information could be system configurations and settings, network diagrams, software versions and hardware components, and even user names and passwords. The term refers to entering a large trash container, however "diving" small office garbage cans if given the opportunity can lead to lucrative information as well.

Live CD, Live Disk, or LiveOS

A live CD or live disk refers to an optical disk that contains an entire operating system. These disks are useful to many assessors and can be modified to contain specific software components, settings, and tools. While live disks are normally based on Linux distributions, several Microsoft Windows versions have been released over the years. Based on the information systems settings, live disks could be the only piece of equipment that the assessor or tester will need to bring to the assessment as the target systems computers can be booted to the live disk, turning one of the information systems assets against the system itself.

KALI HISTORY

Kali Linux is the most recent live disk security distribution released by Offensive Security. This current version has over 300 security and penetration testing tools included, categorized into helpful groups most often used by penetration testers and others assessing information systems. Unlike earlier distributions released by Offensive Security, kali Linux uses the Debian 7.0 distribution as its base. Kali Linux continues the lineage of its predecessor, Backtrack and is supported by the same team. According to Offensive Security, the name change signifies the companies complete rebuild of the Backtrack distribution. The vast improvements over earlier releases of the Backtrack distribution merited a change in name that indicates that this is not just a new version of Backtrack. Backtrack itself was an improvement over the two security tools it was derived from White Hat and SLAX (WHAX) and Auditor. In this line, Kali Linux is the latest incarnation of state of the industry security auditing and penetration assessment tools.

REFERENCES

[1] < http://www.eccouncil.org >.

[2] The basics of hacking and penetration testing: ethical hacking and penetration testing made easy (Syngress Basics Series).

CHAPTER 2

Download and Install Kali Linux

INFORMATION IN THIS CHAPTER

- This chapter will explain how to get one of the most powerful penetration testing toolkits available, Kali Linux

CHAPTER OVERVIEW AND KEY LEARNING POINTS

This chapter will explain the downloading and installing process Kali Linux on:

- Hard drives
- Thumb drives (USB memory sticks)
- SD cards

KALI LINUX

Installing operating systems, such as Microsoft's Windows, Apple's OSX, or open source platforms like Debian and Ubuntu, may be second nature to some, but a refresher on this process is always good. Those that have never installed an operating system before should not worry, the following sections in this chapter will provide all of the steps necessary to locate, download, and install Kali Linux.

Kali Linux is unique in many ways, but the most important distinctions of this distribution are the ability to not only run from a hard drive installation but also boot as a live disk and the number and type of specialized applications installed by default. A live disk is an operating system installed on a disk including Compact Disks (CDs), Digital Video Disk (DVD), or Blu-Ray Disk. As a penetration tester, the ability to boot a live disk is quite important.

Hacking with Kali. DOI: http://dx.doi.org/10.1016/B978-0-12-407749-2.00002-1

Those with access to local machines on the network can leverage live disks to use these machines even if the penetration tester does not have an account on the installed operating system. The system will boot to the live disk instead of the local hard drive; that is, if the machine is configured correctly the penetration tester will then have access to many of the resources on the local network, while at the same time not leaving evidence on the local machines hard drive. The software installed on Kali Linux is another reason it is uniquely outfitted for the penetration tester. By default Kali Linux has 400 penetration testing and security tools, packages and applications installed and has the ability to add more as they are needed.

SYSTEM INFORMATION

All operating systems have uniqueness's and slight deviations that will appear through their initial installation and setup; however, most Linux/Unix-based platforms are relatively similar in nature. When installing Kali Linux, as with other Linux operating systems, planning before installation is crucial. Below is a short list of things to consider when installing Kali Linux.

- Will the operating system be running on a desktop computer or laptop?
- What size hard drive is needed?
- Does the available hard drive have sufficient space available?
- How many hard drive partitions are needed?
- Is log management a concern?
- Is security a concern?

Selecting a Hardware Platform for Installation

Traditionally, the operating system is installed on the computer's hard drive, however, with operating systems such as Kali Linux, there is an ability to install the operating system to thumb drives (aka flash drives) and SD cards due to the recent, availability, and affordability of larger capacity devices. Regardless of the storage device is used to install the operating system, it is critical to determine whether to install to a standalone computer (such as a lab computer) or a laptop that will allow for a mobile solution?

If very specific hardware, such as high-powered graphics cards, will be used for cracking passwords, it is recommended that the installation of Kali Linux be installed on a desktop computer. If there is a need to carry the operating system from customer site to customer site, or there is a desire to test wireless devices, a laptop is recommended. The installation of the operating system is the same for laptop and desktop computers.

Hard Drive Selection

Not to over use the phrase, but "Size does matter." A general rule of thumb is the bigger the drive, the better. This book is recommending a drive with a minimum of 120GB of space; however, even this can become full very quickly, especially in the case of password cracking and forensics or pentesting projects that require a lot of control over, evidence, logs and report generation or collection. In the case of most commercial and government security assessments, the operating system is cleaned, erased, or completely removed to maintain an established baseline environment. This practice is widely accepted throughout the security community due to the need for a proper handling of customer confidential data and minimizing spillage of corporate information that could possibly harm the company's infrastructure or reputation.

Partitioning the Hard Drive

Partitioning is the act of separating out the file system to specific areas of the hard drive by setting special block sizes and sectors. Partitioning can prevent an operating system from becoming corrupted by log files that take over a system and under certain circumstances provide greater security. The operating system is, at the basic level, already broken into two different partitions. The first partition is the swap area, which is used for memory paging and storage. A second partition is designated for everything else and is formatted with a file structure such as the extended file system 3 (ext3) or extended file system 4 (ext4). In the case of laptops, especially those devices where the operating system will be reloaded time and time again, further partitioning is not necessary. For customized installations or computers that will have a more persistent operating system, there is a need to at least separate out the temporary (*tmp*) files.

Advanced partitioning of the hard drive and dual booting a computer are outside the scope of this book and will not be covered. The only exception is in Appendix A where customized distributions are introduced with a third-party application called, Tribal Chicken.

Security During Installation

Kali Linux is a very powerful operating system with a plethora of preinstalled tools that can possibly destroy computers, network infrastructure, and if used improperly or unethically, can lead to actions that will be perceived as criminal or law breaking. For this reason passwords are essential. While passwords are the most basic security practice, many administrators and security professionals often forget or ignore the use of passwords. Basic security practices such as proper use of passwords are essential to ensure that your installation

of Kali Linux is not used by others who might inadvertently or maliciously cause harm to a person, computer, or network.

DOWNLOADING KALI

Kali Linux is a distribution of Linux and is downloaded in an ISO (pronounced: *eye-so*) file. It will need to be downloaded from another computer and then burned to a disk prior to installation. At the time of writing this book, Kali Linux can be downloaded from http://www.kali.org/downloads/. Documentation for advanced operations, configurations, and special cases can also be found in Kali's official website, http://www.kali.org/official-documentation/. There is also a very large and active community where users can post questions and help others with difficulties. Registration at this site is recommended to gain access to the community boards that are managed by Offensive Security, the makers of Kali Linux. Offensive Security will also send out messages about updates and community information (Figure 2.1).

Be sure to select the right architecture (*i386 = 32-bit, amd64 = 64-bit*). The trusted contributed images of Kali Linux is outside the scope of this book; however, if you wish to get familiar with Kali or need a sandbox environment for greater control then the VMware download is perfect for those situations. Click on the appropriate download link to continue with your selection.

For Microsoft Windows7 users, double-click on the completed download and the Burn ISO Wizard will appear. Follow the prompts to complete the conversion of ISO image to a DVD that can be used for installation. Linux users will need to open the ISO in a suitable disk burning application such as K3b.

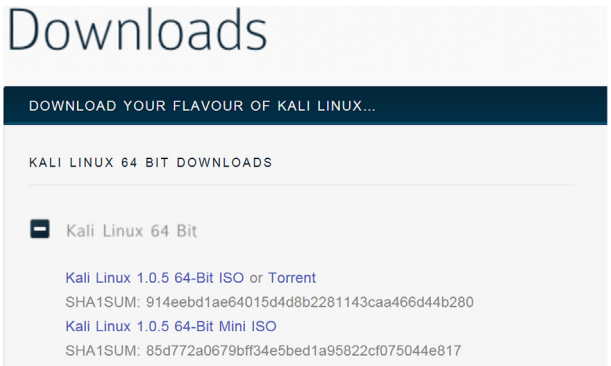

FIGURE 2.1
Downloading Kali Linux.

HARD DRIVE INSTALLATION

The following sections will provide a textual and graphical installation guide designed for simplicity. To correctly install Kali on the systems hard drive, or even boot to the live disk, it is critical that the Basic Input Output System (BIOS) be set to boot from optical disk. To begin the installation, place the CD in the computer's CD tray and boot the computer to the disk. Advanced users comfortable with virtualization technology such as VMware's Player or Oracle's Virtualbox will also find this guide straightforward and helpful as an aide to creating a virtualized version of Kali Linux.

Booting Kali for the First Time

A computer booted to the Kali Linux disk successfully will display a screen that looks similar to Figure 2.2. The version of Kali Linux being used for this guide is 1.0.5 64-Bit; versions downloaded at different times may look slightly different; however, the graphical installations are quite similar in nature. An updated guide for every new release of Kali Linux can be found at http://www.kali.org/, and it is highly recommended that this site is consulted for the latest documentation for your version prior to installation or if you have any questions along the way.

Kali Linux is distributed as a "Live CD" (aka *Live ISO*), which means that the operating system can be run straight from the disk in addition to being installed to a hard drive. Running Kali from the live disk allows the system to boot and all of the tools will execute; however, the operating system presented is ***nonpersistent***. Nonpersistent means that once the computer is shut down, any memory, saved settings, documents, and possibly very important work or research may be lost. Running Kali in a nonpersistent state takes great care, advanced handling, and decent understanding of the Linux commands and operating system. This method is great for learning the Linux

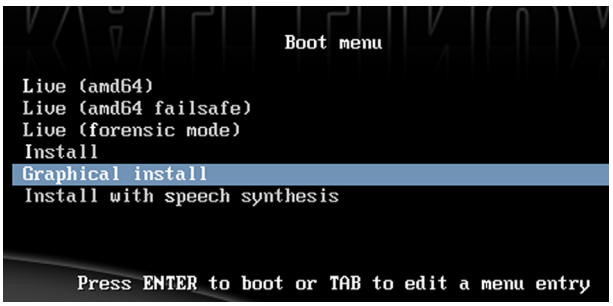

FIGURE 2.2
Live ISO Boot menu.

operating system without deleting the existing operating system already installed on the computer's hard drive.

Another installation, that is out of the scope of this book, is Installation with Speech Synthesis. This is newer feature to Kali and the Debian operating system. Installation can be controlled vocally if you have hardware that supports speech synthesis. This book will focus on the graphical installation for now; therefore, highlight **Graphical Install** and press the Enter key.

Installation—Setting the Defaults

The next few screens will allow the selection of the systems a default language, location, and keyboard language. Select the appropriate settings and click on continue to advance the installer. As the computer begins to prestage the installation of Kali Linux, various progress bars will be presented on the screen throughout the installation. Selecting the default settings is appropriate for most of the selection screens.

Installation—Initial Network Setup

Figure 2.3 details the initial setup and basic configuration of the primary network interface card. Choose a hostname by typing in the box and clicking on continue. Hostnames should be unique, as complications with networking can be a result of computers that were accidentally configured with the same hostname while located on the same network.

After selecting a hostname and clicking on the Continue button, the next screen will ask for the computer's ***fully qualified domain name***, FQDN. This is necessary for joining domain environments and not necessary for most lab

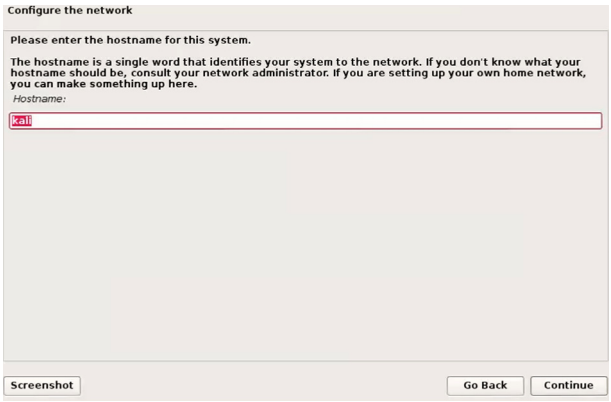

FIGURE 2.3
Setting a hostname.

environments. For this guide, the FQDN was left intentionally blank and can be bypassed by selecting the Continue button.

Passwords

The next prompt in the wizard will ask for a root-level password. The default password is: ***toor***; however, it is recommended that a new password is selected that contains at least one each of the following: uppercase, lowercase, number, and symbol. The password should have no traceability to the user and not be easily guessed. A password of 10 or more characters is suggested. For example if the user once played high school soccer, then *soccer22* would not be recommended. Passwords can be made from variations of common phrases to increase recall. Here are some examples of strong passwords:

- St0n(3)b@tt73 – *"Stone Battle"*
- P@p3r0kCur5# – *"Paper, Rock, Curse"*
- m!gh7yP@jjjama% h – *"Mighty Pajamas"*

When typing your password, it will show up as a series of dots or asterisk. This is normal and hides your password from being displayed in case someone may be viewing the computer screen. After entering in the same strong password twice, click on the Continue button to advance further into the installation (Figure 2.4).

Configuring the System Clock

Figure 2.5 shows the prompt for selecting a time zone. Click on the appropriate time zone and the click on the Continue button to advance on in the installation.

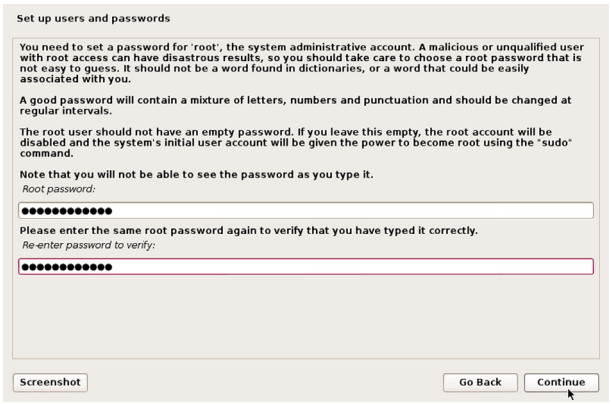

FIGURE 2.4
Setting a password.

Partitioning Disks

There are so many ways to configure partitions for setting up a Linux operating system that someone could devote an entire book to the subject. This guide will focus on the most basic installation, **Guided Partitioning**. Figures 2.6 through Figures 2.10 show the default settings to that are initially highlighted. There will be nothing to select until Figure 2.10. At this time, the installation may be sped up by clicking continue until partitioning is complete, however, it is wise to take a moment and review each step of the installation wizard.

Figure 2.6 shows different options for partitioning hard drives during the installation. LVM, or ***Logical Volume***Management, is not recommended for

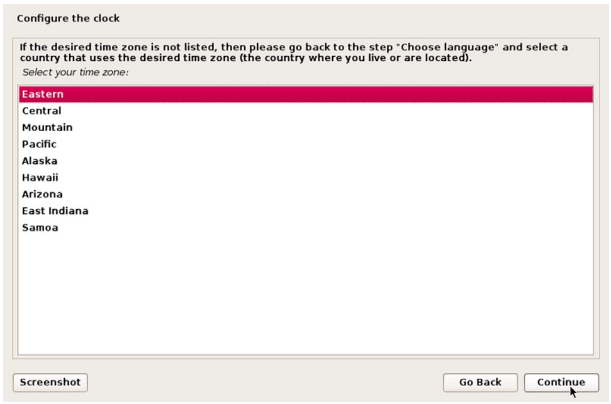

FIGURE 2.5
Configure the clock.

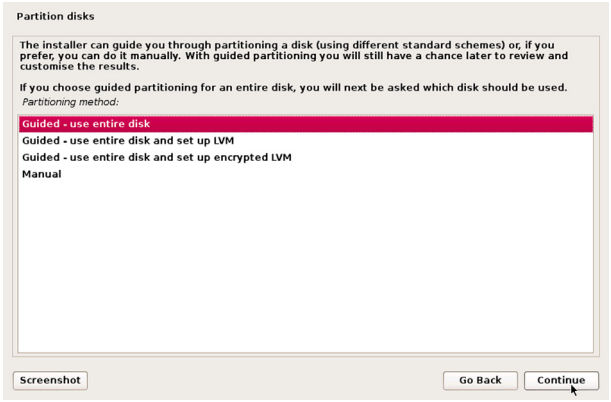

FIGURE 2.6
Partition disks—1.

laptop, thumb drive, or SD card installation. LVM is for multiple hard drives and is recommended only for advanced users. "Guided—user entire disk," should be selected. Click on the Continue button to advance through the installation process.

Figure 2.7 shows the hard drive that has been selected for installation. Depending on hardware and version of Kali Linux, the installation experience may differ slightly. The hard drive will be selected for and if acceptable click on the Continue button to advance through the installation process (Figure 2.8).

As this book is geared toward new users of the Kali Linux distribution: "All files in one partition (recommended for new users)" is the best option and should be selected. Click on the Continue button to advance through the installation process.

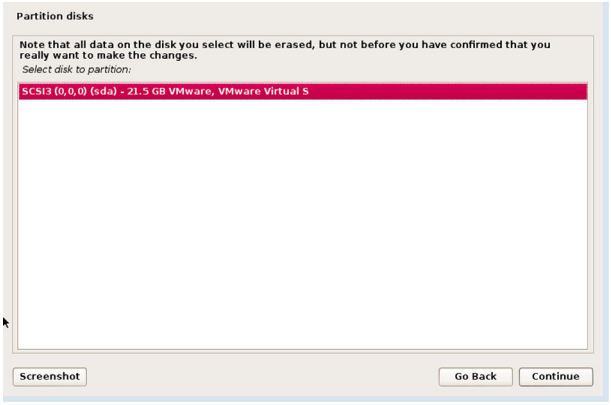

FIGURE 2.7
Partition disks—2.

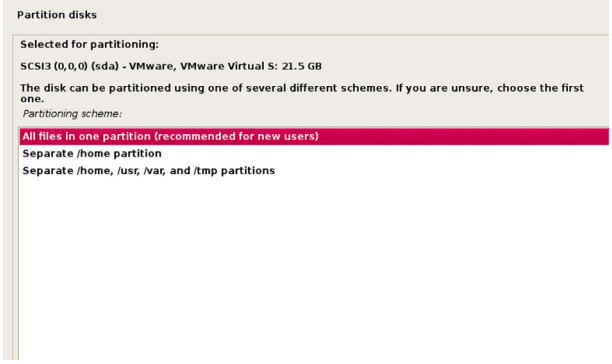

FIGURE 2.8
Partition disks—3.

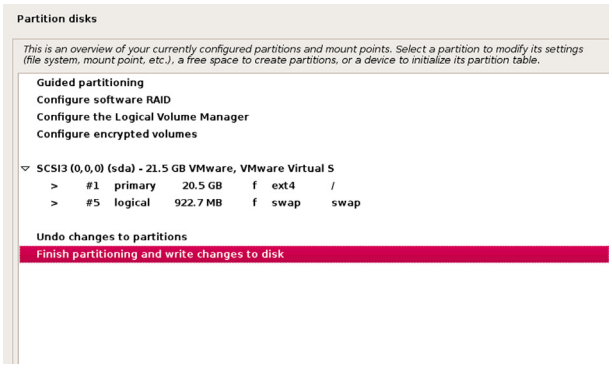

FIGURE 2.9
Partition disks—4.

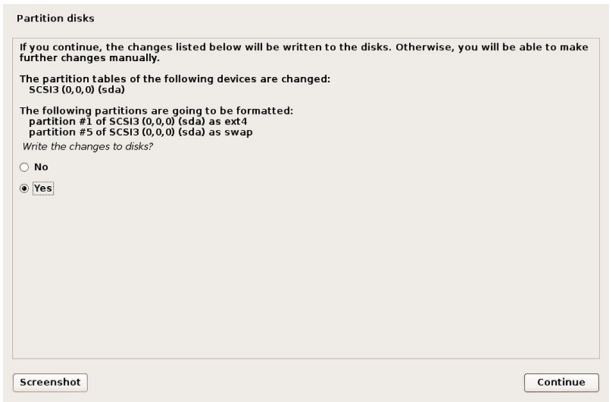

FIGURE 2.10
Partition disks—5.

At the next prompt in the wizard, the partition guide has been completed and is presented for your review. A primary partition containing all of the system, user, and scripting files will be created as one partition. A second partition is created for ***swap*** space. The swap area is virtual system memory that pages files back and forth between the computer's central processing unit (CPU) and random access memory (RAM). All Linux systems are recommended to have a swap area and the general practice is to set the swap area equal to or one and a half times the amount of physical RAM installed on the computer. As seen in Figure 2.9, "Finish partitioning and write changes to disk," will be selected for you. Click on the Continue button to advance through the installation process.

Figure 2.10 is a last chance review for partitioning before the hard drive configuration is committed. There are ways to change partition sizes in the future

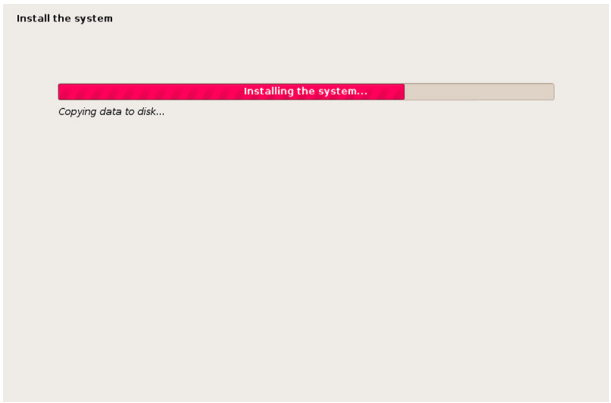

FIGURE 2.11
Installation is underway.

if necessary, but doing so could potentially cause massive damage to your operating system if not done correctly. This prompt in the wizard is a warning that you are about to write data to a specified hard drive with the previously defined partition tables. Select ***YES*** and click on the Continue button to advance through the installation process.

After clicking continue at the last prompt of the partitioning section of the wizard, the hard drive partition will begin. Figure 2.11 shows that the actual installation is being conducted at this time. Depending on the hardware you possess, this process can take just a few minutes or even an hour or more.

Configure the Package Manager

The package manager is a crucial part of the operating system's setup. The package manager refers to the update repository where Kali Linux will pull updates and security patches. It is recommended to use the network mirror that comes with the Kali Linux ISO as this will the most up to date sources for package management. Figure 2.12 shows that "**YES**" will be selected by default. Click on the Continue button to advance through the installation process.

If using a proxy, enter the configuration information where appropriate on the next prompt in the wizard or leave it blank as pictured in Figure 2.13. Click on the Continue button to advance through the installation process.

Installing the GRUB Loader

TheGrand Unified Bootloader **(GRUB)** is the main screen that will be displayed every time the computer is started. This allows the verification of certain settings at boot, make on the fly changes, and make setting

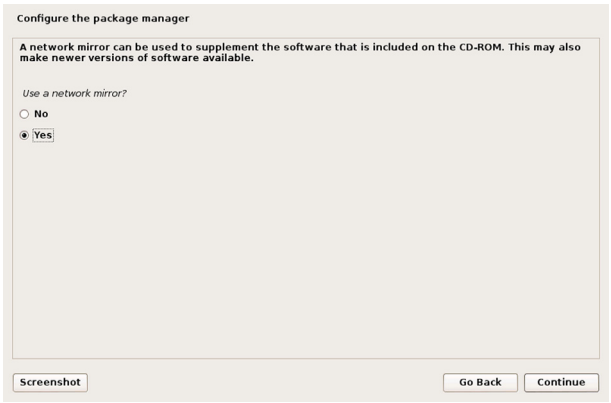

FIGURE 2.12
Configure the package manager.

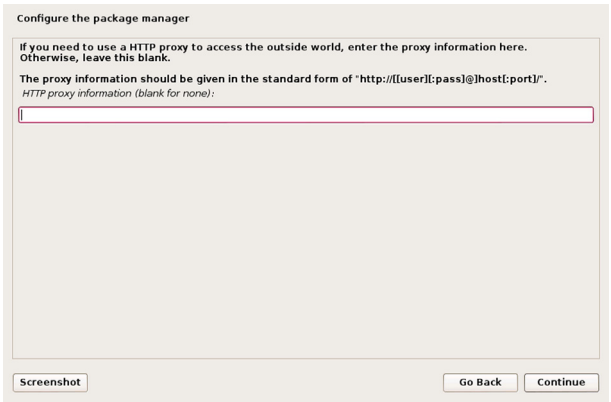

FIGURE 2.13
Configuring a proxy.

adjustments before the operating system loads. While GRUB is not necessary for some advanced users, it is highly recommended for most installation types. Figure 2.14 shows that "**YES**" to install the GRUB is selected for you. Click on the Continue button to advance through the installation process.

Completing the Installation

Now remove the disk from the computer and reboot you machine. When prompted do so and then click on the Continue button to finish the installation (Figure 2.15).

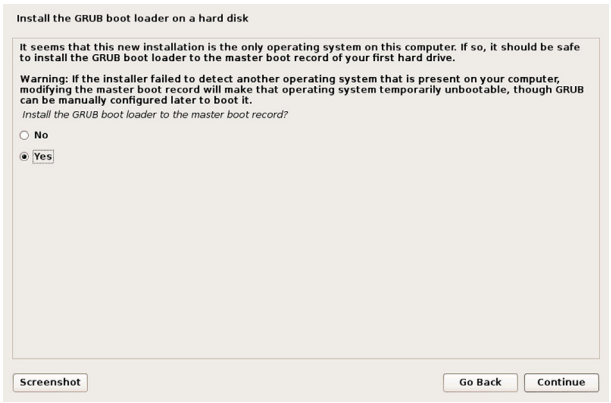

FIGURE 2.14
Install GRUB.

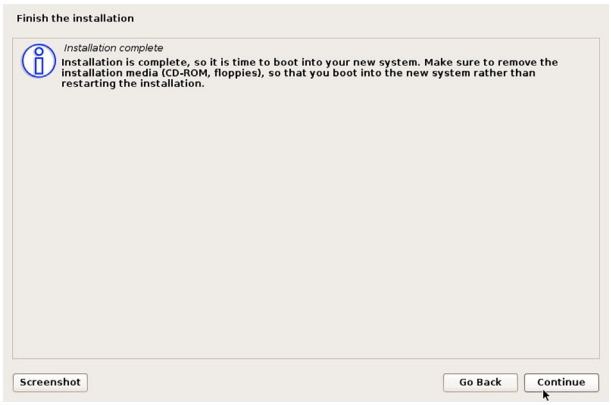

FIGURE 2.15
Installation complete.

After rebooting, the welcome screen will be presented. Log in as the root user with the predefined password set earlier in the installation process. Welcome to Kali Linux!

THUMB DRIVE INSTALLATION

USB memory devices, often referred to as thumb drives and many other names, are nothing more than a storage device that is attached via a USB interface to the computer. This book recommends using a USB device with at

least 8GB of space, preferably much more. New computers can boot to USB devices. If this option is selected make sure that the computer being used can support booting from a USB device.

The following sections break down the installation of Kali Linux on to USB using a Microsoft Windows computer or Linux platform. Be sure to check the documentation provided on the Official Kali Linux homepage for updates to this process.

When it comes to thumb drives being used as bootable devices, there are two key terms that are very important: persistence and nonpersistence. Persistence refers to the ability of your device to retain any written or modified files after the machine is powered off. Nonpersistence refers to the device losing all setting, customizations, and files if the machine reboots or is powered off. Specifically for this book, the thumb drive installation of Kali Linux from a Windows platform will be ***nonpersistent***, and the installation from a Linux platform will be ***persistent***.

Windows (Nonpersistent)

Required application—Win32 Disk Imager: http://sourceforge.net/projects/win32diskimager/

After downloading the Kali Linux ISO, put a thumb drive in the computer and allow it to automatically be detected by Windows, taking note of the drive letter assigned. Next open Win32 Disk Imager. Click on the folder icon to browse and select the Kali ISO file and then click the "OK" button. Select the correct drive letter from the device drop-down menu. Finally click the "Write" button.

When Win32 Disk Imager has completed burning the ISO, reboot the computer and select the thumb drive from the BIOS POST menu. Most manufacturers have different methodologies for booting to USB devices; be sure to check the computer manufacturer's documentation.

Linux (Persistent)

When building a persistent thumb drive, again, size does matter! The bigger the thumb drive, the better. Also, depending on the version of Linux in which you will be building this USB device, be sure that the application GParted is installed. Be sure to check your operating system's documentation if you are having difficulties installing GParted. One of the following methods may be necessary for your Linux installation if GParted is not installed:

- apt-get install gparted
- aptitude install gparted
- yum install gparted

After downloading the Kali Linux ISO, plug in thumb drive. Open a terminal window and verify the USB devices location the following command.

```
mount | grep -i udisks |awk '{print $1}'
```

Figure 2.16 shows that the output of the command as "/dev/sdb1." The USB device's output may be different based on the computers settings and configuration. In the next command, swap "sdb" to match the correct identification and remove any numbers at the end.

Use the "dd" command to transfer the Kali ISO image to the USB device.

```
dd if=kali_linux_image.iso of=/dev/sdb bs=512k
```

Now launch Gparted.

```
gparted /dev/sdb
```

The drive should already have one partition with the image of Kali that was just installed.

Add a new partition to the USB by selecting New, from the menu that appears after clicking on the Partition menu from the File Menu Bar. Slight deviations in output can be present from many different device manufacturers. On average, the steps are similar to the following.

- Click on the grey "unallocated" space.
- Click on "New" from the Partition drop-down menu.
- Use the sliders or manually specify drive size.
- Set the File System to ext4.

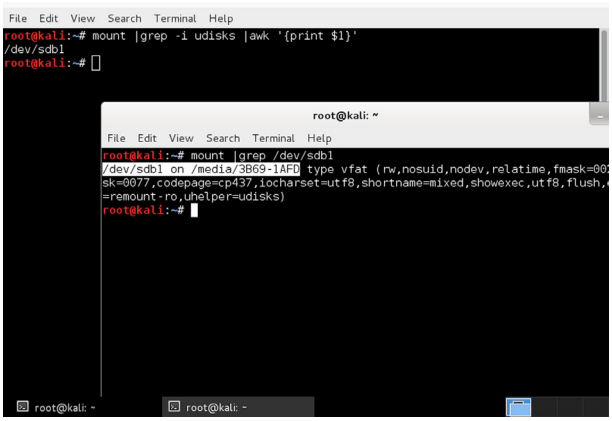

FIGURE 2.16
Mounted USB.

- Click Add.
- From the main window select, **Apply All Operations** from the **Edit** drop-down menu.
- Click **Okay** when prompted. *This may take a while.*

To add in persistent functionality use the following command.

```
mkdir /mnt/usb
mount /dev/sdb2 /mnt/usb
echo "/ union" >> /mnt/usb/persistence.conf
umount /mnt/usb
```

Creation of the LiveUSB is now be completed. Reboot the computer and boot from the thumb drive.

SD CARD INSTALLATION

Microcomputing devices such as the RaspberryPi and Google's Chrome Notebook are capable of running on SD cards. These small devices can be used for a plethora of purposed; someone is only limited by their own imagination. The greatest advantage of devices; such as the Raspberry Pi, is that they are cheap and a huge hit in the open source communities making resources readily available to tinkerers everywhere.

There is one drawback to the installing Kali Linux on ARM devices, the images are custom and have to be defined for each piece of hardware. Images for ARM devices can be located on Kali's official download pages, http://www.kali.org/downloads/. Be sure to check out the website to see if your hardware has a supported image available for download.

The following steps provide a short guide to installing Kali Linux to compatible ARM architecture-based devices.

1. Download the appropriate image from Kali's official website (http://www.kali.org/downloads/).
2. Insert a blank SD card. Verify the mounted location with the following command.
   ```
   mount | grep -i vfat
   ```
   (Assuming/dev/sdb for the next step.)
3. Transfer the Kali.img file to the SD card.
   ```
   dd if=kali.img of=/dev/sdb bs=512k
   ```
4. Unmount and sync any write operations before removing the device.
   ```
   umount /dev/sdb
   sync
   ```
5. Remove the SD card.

6. Insert the SD card containing the Kali Linux image into your ARM architecture computing device and boot to the SD card.

SUMMARY

In this chapter, the topics covered will give the user the ability to install Kali Linux to most computers, laptops, thumb drives, and microcomputing devices. Installing Kali Linux is much like riding a bicycle; do it once, and you won't really ever forget how to install Kali. Be sure to check with the documentation and community message boards on Kali's official website as new updates, versions, and technologies developed in the security community. Linking up and networking with other security professionals, hobbyists, and hackers alike can, and will, expand the mind, delve deeper into new projects, and assist in answer questions when able.

CHAPTER 3

Software, Patches, and Upgrades

INFORMATION IN THIS CHAPTER

- APT Package Handling Utility
- Debian Package Manager
- Tar-balls
- A Practical Guide to Installing Nessus

CHAPTER OVERVIEW AND KEY LEARNING POINTS

This chapter will explain the process necessary to maintain, upgrade, and install custom and third-party applications using APT package handling utility (apt-get) and the Debian package manager (dpkg).

APT PACKAGE HANDLING UTILITY

The APT package handling utility, simply known as "apt-get," is a lightweight and extremely powerful command-line tool for installing and removing software packages. Apt-get keeps track of everything installed along with the required dependencies. Dependencies are the additional software packages required for proper functionality of other software. For instance, Metasploit, the pentester's best friend, relies on a particular programming language called Ruby. Without Ruby installed, Metasploit could not even launch; therefore, Ruby is a dependency of Metasploit.

Apt-get not only keeps track of the dependencies for installed software but will keep track of versioning and interdependencies when updates are available. When software packages are no longer useful or depreciated apt-get will alert the user at the next update and prompt to remove old packages.

Hacking with Kali. DOI: http://dx.doi.org/10.1016/B978-0-12-407749-2.00003-3

Apt-get can be a very simple or highly involved tool. The administration of packages is crucial to making sure Kali Linux functions properly and that software packages are up to date. While, the average user of Kali Linux does not need to know the in-depth workings of apt-get, there are some basics that every user should know.

Installing Applications or Packages

Installing additional software is the most basic function of the apt-get command and is simple and straightforward. The syntax below will provide an example of the necessary usage of the install subcommand:

```
apt-get install {package_name}
```

Try installing "gimp;" an image editing software package:

```
apt-get install gimp
```

Update

From time to time the sources, or repositories, need to be checked for updates to various applications and packages installed on Kali Linux. It is recommended that updates are checked before installing any new packages, and is essential before performing an upgrade to the operating system or software applications or packages. The syntax for performing updates follows:

```
apt-get update
```

Upgrade

No system is ever perfect, in fact every major operating system is in a constant state of improvement, enhancement, and patch management to offer new features or correct bugs. The upgrade function will pull down and install all new packaged versions of ***already installed*** software packages. The beauty of all Linux-based operating systems is that they're open source, meaning that anyone in the world can submit new code to the distribution managers of the operating system to help improve the functionality of the system if they spot a bug or a need for improvement. This also allows for patches to be updated faster compared to the corporate giants like Microsoft. As stated earlier, it is vital to perform an update before running an upgrade. To upgrade Kali use the following command:

```
apt-get upgrade
```

Distribution Upgrade

The distribution upgrade function works very similarly to the upgrade function, however, this function also seeks out sources for special marked packages and their dependencies as well as new packages the distribution managers have designated to be included with the newest baseline. For example, when invoking the distribution upgrade function, the entire version

of Kali will be raised from version 1.0 to version 1.***n***, or 2.***n***, and so on. Use the following syntax to upgrade Kali:

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

Remove

Apt-get can be used to reduce the footprint of a system, or when removing rid of a specific program. It is also recommended all packages not in use, those not serving a purpose, or not necessary for your operating system be uninstalled. For example, if the Leafpad application isn't needed on the system, then remove it. If the application needs to be installed later, it can be, however, it is best to leave out what is unnecessary. The following syntax can be used to remove an application or package:

```
apt-get remove {package_name}
```

Try removing "leafpad" and then reinstalling the application:

```
apt-get remove leafpad
apt get install leafpad
```

Auto Remove

Over time the operating system's application packages are replaced with new and improved versions. The auto remove function will remove old packages that are no longer needed for the proper functionality of the system. It is recommended that the auto remove function be run after an upgrade or distribution upgrade. Use the following syntax to run auto remove:

```
apt-get autoremove
```

Purge

What is the difference between remove and purge? The remove function will not destroy any configuration files, and leaves those items on your hard drive in case the files are needed later. This is useful, especially with applications such as MySQL, Samba Server, or Apache. The configuration files are crucial for the operability of your applications. However, sometimes, it is necessary to remove all of the application files, even configuration files for that application, from the system in order to re-install applications to a blank state and start over, or clear all traces of possibly sensitive information. Purging an application from the system will completely erase the application package and all related configuration files in one fell swoop. Be careful not to get too complacent when using the purge function; it is dangerous when used incorrectly or on the wrong application as all associated files will be removed from the system. Purge can be used with the following syntax:

```
apt-get purge {package_name}
```

Clean

Packages are downloaded to the system from their source, unpackaged, and then installed. The packages will reside on the system until further notice. These packages are no longer necessary after installation of the application. Over time, these packages can eat up disk space and need to be cleaned away. The following syntax can be used to initiate the clean function:

```
apt-get clean
```

Autoclean

Autocleaning also cleans the system in a similar fashion as the clean function; however, it should be run after upgrade and distribution upgrades to the system, as the autoclean function will remove old packages that have been replaced with new ones. For instance, suppose application Y version 1 was installed on the system and after an upgrade to the system, application Y v1 is replaced with application Y v2. The autoclean function will only clean away version 1, whereas, the clean function will remove the application packages for both versions. The following syntax will start the autoclean function:

```
apt-get autoclean
```

Putting It All Together

Administration of packages is about working smarter, not harder. Below are the following commands that a user can be used to make sure that all of the possible patches, packages, and updates are up to date and ready to go:

1. `apt-get update && apt-get upgrade && apt-get dist-upgrade`
2. `apt-get autoremove && apt-get autoclean`

The "&&" entry on the command line allows for multiple commands to run sequentially.

DEBIAN PACKAGE MANAGER

The major flavors (*or distributions*) of Linux have individual application packaging systems. Kali Linux was built on top of the Debian 7.0 base operating system, and may need third-party applications, such as Tenable's Nessus. Nessus is a vulnerability scanning application that can be installed from prepackaged files suitable for the Debian Package Manager. The use of Nessus will be covered in the chapter on scanning. When downloading these types of applications, look for the ".deb" file extension at the end of the file name.

There is no benefit of using the Debian Package Manager over APT. The apt-get program was written specifically for the management of Debian packages. Third-party company's applications that must be purchased from a vendor

are not available publicly and apt-get's sources will be unable to locate the packages for download and installation. Kali Linux is not capable of processing RPM (Red Hat Packages) without extra software installed, and the practice of using RPMs on a Debian-based system is not recommended.

Install

After downloading a .deb package, the dpkg command will need to be used in order to install the package. Most .deb packages are straightforward and contain all of the necessary dependencies appropriate for the application to function successfully. In rare cases, mostly dealing with licensed software, vendors may require additional steps before installation and will generally have instructions for proper installation on the system. Be sure to check the vendor's documentation before starting the installation:

```
dpkg -i {package_name.deb} /{target_directory}
```

Remove

Removing a package (-r) or purging a package (-P) works in the very same way that APT does and follows the same pattern for handling packages:

```
dpkg -r {package_name.deb}
```

Purging a package with the Debian package manager works similarly to the remove function and can be initiated with the following command:

```
dpkg -p {package_name.deb}
```

Checking for Installed Package

One super power that APT doesn't have over the Debian Package Manager is the wonderful ability to interpret the current status of installed or removed software. When using the *list* function within dpkg, the output will show a two- or three-character code at the beginning of the line indicating the package's current state of installation. When run against the Leafpad application package, the following picture shows that the package is removed, but the configuration files are still available (Figure 3.1).

After the command ***dpkg -P leafpad*** is run, the package's configuration files are also removed. Figure 3.2 shows the corresponding output of the Leafpad application package when it has been completely purged from the system.

To look for the status of installed or removed software, use the syntax below:

```
dpkg -l {package_name}
```

More detailed information about the package installed can also be displayed on the screen with the following command:

```
dpkg -p {package_name}
```

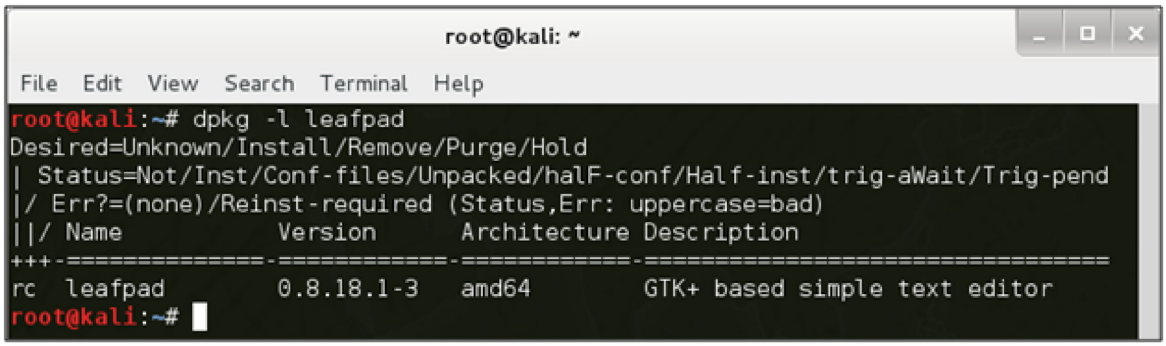

FIGURE 3.1
Leafpad removed.

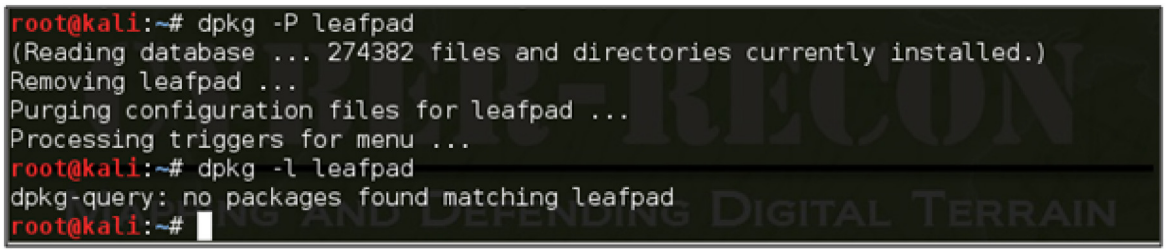

FIGURE 3.2
Leafpad purged.

Pay close attention to the use of upper and lowercase. Lowercase "p" prints the information to the screen. The upper case "P" will purge the package from the system without prompting, "Are you sure?"

TARBALLS

Tar, originating in the yesteryears of Unix systems, was named for its function, which was initially for writing multiple files to Tape Archives (TAR). Not everyone needs the ability to transfer multiple files to tape but commonly need the inherent functionality of the tar application which is to generate a container file that will house multiple files. This allows for easier transporting of files. Furthermore, these files can be compressed with gunzip (*gzip*) decreasing their overall size. Some packages from third-party or open-source projects can be downloaded in tarball format and are easily identified by the .tar file extension or .tar.gz for compressed tarballs.

During a penetration test, a massive amount of scanning documents, screen captures, customized scripts, and client documentation are captured. Using the Tarball system allows for easier collection, management, and disbursement of all documents. It is also highly recommended that all records from penetration tests be kept in a safe location for at least 5 years, or the date determined by the state's statute of limitations where the work was performed. Customers may also have stipulations on retention requirements that should be spelled out in the penetration tests rules of engagement (ROE). The ROE will be covered in the chapter on reporting. If a company or contractor is very active with penetration testing, the amount of documentation can pile up quickly and soon be out of control. Tarball, especially when compressed, provides a system of containment that keeps records apart and allows for easier backup and overall management.

Creation of a Tarball

Creating a tarball file can be very straightforward or very complex. Remember, the original function of the tar command was meant to send files to TAR. For advanced usage of the tarball system, check out the manual pages for tarball (*man tarball*). For this book only the basic creation of tarball files will be included; however, this information is useful and can transition to just about any Linux-based platform. The steps below provide a walk through that a user can follow to create a sample tarball. The steps are as follows:

Create a directory for your files. In this case the tar-demo1 directory is being created with the mkdir command:

```
mkdir tar-demo1
```

Next create a number of files in this directory that can be used to illustrate the tar command. In this case the right carrot (>) will be used to create a file with the content "Hello world". This file will be named file 1, and a number of files can be created in the same manner using the same syntax but changing the final number. Creating the files in this way will also move your files into the directory specified, in this case tar-demo1:

```
echo "Hello World" > tar-demo1/file1
echo "Hello World" > tar-demo1/file 2
```

Change into the directory that you wish to create a tarball in. In this case it is the tar-demo1 directory:

```
cd tar-demo1
```

Generate a new tarball with the files contained within the current directory. In this example the asterisk (*) is used to signify everything in this directory should be added to the tar file:

```
tar -cf tarball-demo.tar *
```

The tar -tf command is used to list the contents of the tarball:

```
tar -tf tarball-demo.tar
```

Extracting Files from a Tarball

The process of extracting files from a tarball is as easy as one, two, and three; however, the location of the information is put that is the key. The files extracted from a tarball are placed in the working directory. If a tarball is extracted from the root directory, that's where the files are going to end up. It is recommended that good habits form as soon as possible; therefore, all users of tarballs should use the "-C" switch when extracting files. The "-C" switch allows the user to specify the location of where the files need to go.

Make a directory for the files to be extracted into. In this case the directory created is named tar-demo2:

```
mkdir /root/tar-demo2
```

Extract the files into the specific directory:

```
tar -xf /root/tar-demo1/tarball-demo.tar -C /root/tar-demo2/
```

Make sure that all of the files are extracted to the directory that was specified in the earlier step:

```
ls /root/tarball-demo2/
```

Compressing a Tarball

Tarballs can be compressed during creation with multiple different types of algorithms. One standard in use is gunzip, also known as gzip. This is done with the following commands.

Create a directory for your files. In this case the tar-demo3 directory is created:

```
mkdir tar-demo3
```

Now move your files into the directory. As earlier the echo command will be used to create the files for this demonstration:

```
echo "Hello World" > tar-demo3/file1
```

Change into the directory that you wish to create a tarball in. Again in this example the tar-demo3 directory is being used:

```
cd tar-demo3
```

Generate a new tarball with the files contained within the current directory. This is done using the -czf switches with the tar command. The switches on the tar command ensure the tarball is created correctly. The c switch creates a new archive and the z ensures the files are compressed (or zipped) and the f switch signifies the name following the switches (tarball-demo.tar.gz) will be used as the name for the new file. Again the asterisk (*) lets tar know that everything in this directory should be included in the new tar file:

```
tar -czf tarball-demo.tar.gz *
```

Listing the contents of the tarball is done with the t and f switches. The t switch indicates the file contents should be displayed (or typed to the screen) and again the f switch indicates the file name will follow the switches:

```
tar -tf tarball-demo.tar
```

Extraction of files from a compressed tarball works exactly the same way as extraction from a noncompressed tarball. The only change is the x switch is used to indicate that tar should extract the contents of the tarball. While it is not required, it is standard practice to name the file with the .gz extension to indicate to others that the tarball is compressed. Notice that the file in this example has two periods (.tar.gz) this is totally acceptable in Linux environments and is standard with compressed tar files:

```
tar -xf {tarball_file.tar.gz} -C {directory_for_files}
```

A PRACTICAL GUIDE TO INSTALLING NESSUS

Tenable, a highly respected name in the security community, has produced an amazing application for vulnerability scanning called Nessus. There are two versions of the application that offer differing levels of functionality and support these are the Nessus Professional and Home versions. The professional version offers a lot more plug-ins for compliancy checking, SCADA, and configuration checking and is incredibly powerful for team usage. For this book, the installation of the Nessus Vulnerability Scanner with the home feed will be used. Nessus is discussed further in the chapter on scanning but installing Nessus now will help to cement the knowledge from this chapter.

Update and Clean the System Prior to Installing Nessus

In a terminal windows type the following commands:

```
apt-get update && apt-get upgrade && apt-get dist-upgrade
apt-get autoremove && apt-get autoclean
```

Install and Configure Nessus

Download Nessus 5.0 or higher from http://www.nessus.org/download. Select the Debian package for either 32- or 64-bit operating system as appropriate. Read the subscription agreement and if acceptable agree to the statement by clicking the Agree button. Nessus cannot be installed if the agreement is not accepted. Note the location where the file is being downloaded to as it will be needed to complete the installation.

From a terminal window enter the following:

```
dpkg -i ~/{Download_Location}/Nessus-{version}.deb
```

A more comprehensive setup guide can be found in Appendix A while setting up a pentesting environment framework with Tribal Chicken.

CONCLUSION

This chapter covered the foundational skills necessary for package management on the Kali Linux system. APT is a powerful command-line tool that automates the management of packages, update, and patches. The Debian Package Manager (dpkg) is the underlying system that APT was built on top of for package management. With the basic understanding and general familiarization of these tools, anyone can keep a system up to date and install new applications.

For advanced use of the tools described in this chapter, refer to the manual pages either from within a terminal window or online through their respective official websites. These tools have the ability to generate an environment perfect for any individual or destroy an entire system without a single prompt or thought of remorse. It is recommended that until a user is comfortable with the use of these tools, that hands-on practice should be exercised in a separate system or a virtual environment.

CHAPTER 4

Configuring Kali Linux

INFORMATION IN THIS CHAPTER

- Using the default Kali Linux settings can be beneficial for learning but it is often necessary to modify basic settings to maximize the use of this platform

CHAPTER OVERVIEW AND KEY LEARNING POINTS

This chapter will explain

- the basics of networking
- using the graphical user interface to configure network interfaces
- using the command line to configure network interfaces
- using the graphical user interface to configure wireless cards
- using the command line to configure wireless cards
- starting, stopping, and restarting the Apache server
- installing a FTP server
- starting, stopping, and restarting the SSH server
- mounting external media
- updating Kali
- upgrading Kali
- adding the Debian repository

ABOUT THIS CHAPTER

Networking is the way that computers and other modern electronic devices communicate with each other. This can be seen as paths or roads between devices with rules and requirements (protocols), traffic laws (rule sets and

Hacking with Kali. DOI: http://dx.doi.org/10.1016/B978-0-12-407749-2.00004-5

configurations), maintenance crews (network services), law enforcement (network security), closed and private roads (firewall ports and protocol restrictions—also part of security). In the following sections, the basics of networking will be described as will the steps that will need to be taken to properly configure networking in Kali.

Networking is a complex topic, and this chapter barely scratches the surface of networking. The explanation presented here only serves to frame and explain the components required to successfully configure the network components of Kali Linux. To get a more detailed understanding of networking check out *Networking Explained*, 2nd ed., by Michael Gallo and William Hancock. This explanation will provide the reader with the basic understanding of the most basic network components.

THE BASICS OF NETWORKING

Networking can be thought of as a series of electronic roads between computers. These roads can be physical, most commonly copper category 5 or 6 (CAT 5 or CAT 6) cables or fiber optic cables. Wireless networking uses special radio transmitters and receivers to conduct the same basic tasks as physical networks. A wired network interface card (NIC) is illustrated in Figure 4.1, and a wireless module is illustrated in Figure 4.2.

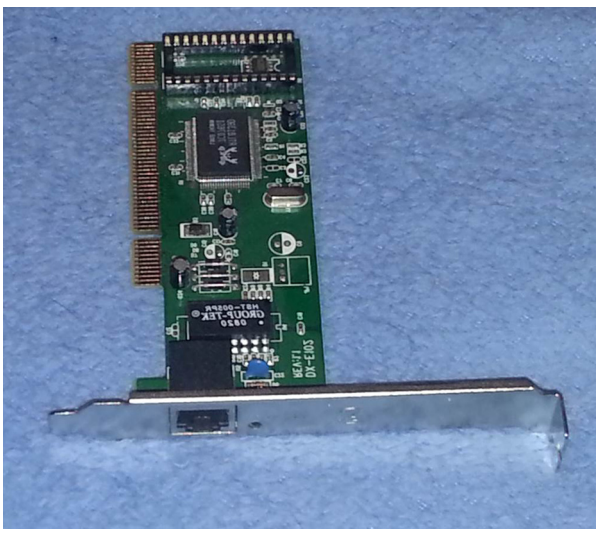

FIGURE 4.1
Network Interface Card.

FIGURE 4.2
Wireless network expansion card.

Regardless of the medium, physical or wireless networking has the same basic components. First there are two or more devices that will be communicating, for example Adams's computer will be communicating with Bill's computer. To do this they will need the correct communications equipment operating on the correct medium. For this example, Adam will be connecting to the same physical CAT5-based network that Bill is connected to; however, if the settings are correct Bill could be using a wireless network card and Adam could be using a wired network card as long as the protocols and settings for both are correct. For this to work correctly both Adam and Bill would need to be connecting to the same network segment using a device like a wireless router that would be connecting the different physical media types, wired and wireless.

There are a number of components that make up a modern network and fully explaining networking is far beyond the scope of this book; however, the small network segment that will be explained will be sufficient to describe how to configure a network card. This small network is only two computers that are being used by Adam and Bill, a wired router connected to a cable modem and the cables that connect everything together (all CAT5 in this example). The router has an inside Internet protocol (IP) address of 192.168.1.1, which is quite common for small office home office (SOHO) and home networks default configuration. This small router connects to the Internet through its external connection, using an IP address assigned by the Internet Service Provider that will enable Adam and Bill to surf the web once they correctly configure their network cards. In this example, the router also provides dynamic host configuration protocol (DHCP), basic firewall functions, and domain name service (DNS), each of these will be discussed in more detail later. This network is illustrated in Figure 4.3 and will be the base network used in all of the following chapters.

Private Addressing

The internal interface (or network card) for the router has an IP address of 192.168.1.1, this is what is called a private address as it can't be used on the Internet. It is fine for the internal network represented by the gray box in Figure 4.3 as are all of the addresses issued by DHCP, for example the IP address issued to Adam and Bill's computers. Table 4.1 lists the common private IP addresses that can be used for internal or private networks, but can't be used on the Internet.

To access the Internet, the router does a bit of magic called network address translation (NAT) that converts the IP addresses used by Adam and Bill to addresses that can be used on the Internet. This is normally the address that is issued to the router by the cable Internet provider and will be assigned to the external interface (another network card). If a user was to try and use these addresses on the Internet, without a NATing router, the communication would fail as Internet routers and other devices reject these private IP addresses.

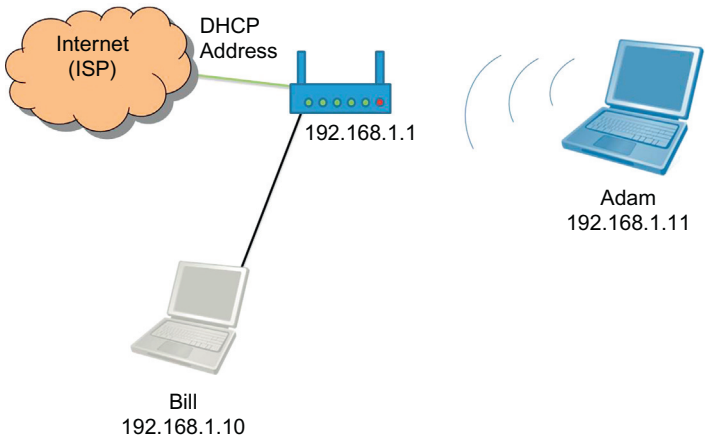

FIGURE 4.3
Example small network segment.

Table 4.1 Private IP Addresses

IP Address Range	Number of Possible Addresses
10.0.0.0 to 10.255.255.255	16,777,216
172.16.0.0 to 172.31.255.255	1,048,576
192.168.0.0 to 192.168.255.255	65,536

Default Gateway

The router separates these two networks, internal and external, and provides some basic security functions, like a rudimentary firewall. Additionally, the router provides a way out of the private network to the public network, normally the Internet. For this reason, the routers internal interface IP address is the way out of Adam and Bill's network. This address, called the default gateway, will be used later when configuring the network cards for the user's two computers. A good way to visualize the default gateway is to view it as the single road out of a small town. Anyone wanting to leave the town would need to know where this road is. On a network computers (through the network card) need to know where the way out of the local network is, this is the default gateway.

Name Server

Computers talk to each other in numbers, while people are much better at communicating with words and phrases. For communication to function correctly, networks normally make use of name server or domain name service (DNS). This book will cover DNS in greater detail later, so only a high-level overview of DNS will be discussed in this chapter. Basically, the name server translates human friendly names (like www.syngress.com) to an IP address that computers and networking components are better at working with. The DNS, synonymous with name server, provides translation between human friendly and computer friendly addresses. For example, when a computer wants to communicate with another computer, a web server for example, it must first translate the human readable address to a computer friendly address that can be used to route the message. The person would type www.syngress.com in their favorite browser, and the computer would forward this address for resolution to a DNS machine. The DNS would reply with the machine hosting the web pages IP address (`69.163.177.2`). The user's computer would then use this IP address to communicate with the Syngress web server and the user could interact with the Syngress web page. Without this service, humans would be required to memorize every website's unique IP Address. This would mean people would have to remember 69.163.177.2 not syngressc.com. Manual configuration of a network card requires the identification of a DNS or name server.

DHCP

For pure network magic nothing beats DHCP. With a computer set up for automatic configuration of DHCP, all the user needs to do is connect to a working network cable and go to work. This is done when the computer initiates communication across the network looking for a DHCP server, by sending out a broadcast request looking for a DHCP server. The server

responds to the client and assigns networking configurations to the requesting computer. This includes an IP address for the computer (well really just the network card but that is a little in the weeds for this explanation), the default gateway, name server—or name servers, and the default subnet mask. In most cases, this is a great way to configure your network card but if you are conducting a penetration test, using DHCP to configure your network card announces to everyone that you are entering the network, normally not a good thing.

Basic Subnetting

Subnetting is a topic that can confuse a lot of people, so for the sake of this book subnetting will only be explained as the way to configure networks in the best way to save IP addresses. This is done by applying a mask that will filter out some of the computer's IP address allowing the networks addressing to be uncovered. Back to the Syngress example, the IP address is 69.163.177.2 and if we were on a small network that had less than 255 users we could use a class C subnet mask of 255.255.255.0. When applying the mask, parts of the address are canceled out and others remain allowing the computers on the network to know the network they are on. Again a basic example of a subnet mask uses only the numbers 255 and 0 numbering octets; therefore, to identify the network, any part of the address matched up with a 255 is not changed at all, so the first three octets of the IP address (69, 163, 177) will all be matched with 255 allowing the original numbers to be passed through. Any number matched with 0 is totally canceled out, so the last octet of the address, or 2, would be canceled out resulting in a 0. So by applying the subnet mask of 255.255.255.0 to the address 69.163.177.2, we find that the network address is 69.163.177.0. In most small networks, a subnet mask of 255.255.255.0 will work well, larger networks will require a different subnet mask that may have been calculated to provide services to a specific number of network hosts.

Kali Linux Default Settings

As explained earlier, most penetration test engineers, white hat hackers, will not want their network card to announce their presence on the network as soon as the computer connects. This is just what Kali Linux will do when it is powered up and connect to a network. Care must be taken when conducting a penetration test to avoid this unneeded extra communication by disabling the network card before plugging in to the network. With custom installs including installing to a hard drive, thumb drive, or SD card, this automatic network configuration can be changed. Another way to change this is by building a custom live disk that will be configured for manual

network configuration. These methods will all be discussed in Chapter 5 on customizing Kali Linux.

USING THE GRAPHICAL USER INTERFACE TO CONFIGURE NETWORK INTERFACES

Configuring the network cards, also called network adapters, in Linux was once a process that could only be completed through the command line. This has changed in recent years, and Kali Linux is no different in fact Kali Linux has a robust graphical user interface (GUI) that allows many of the common settings to be configured through the use of simple dialog boxes. The network configurations dialog box is easily accessible by selecting Applications in the top right of the user interface (Figure 4.4) and then selecting System Tools, Preferences, and Network connections.

By clicking network connections, the network connections dialog box will be displayed, the wired tab is selected by default (Figure 4.5). Alternatively, right clicking on the two computers on the top right of the screen, as in Figure 4.6, and selecting edit connections will result in accessing the same dialog box. In most cases, computers will have only one network card that will need to be

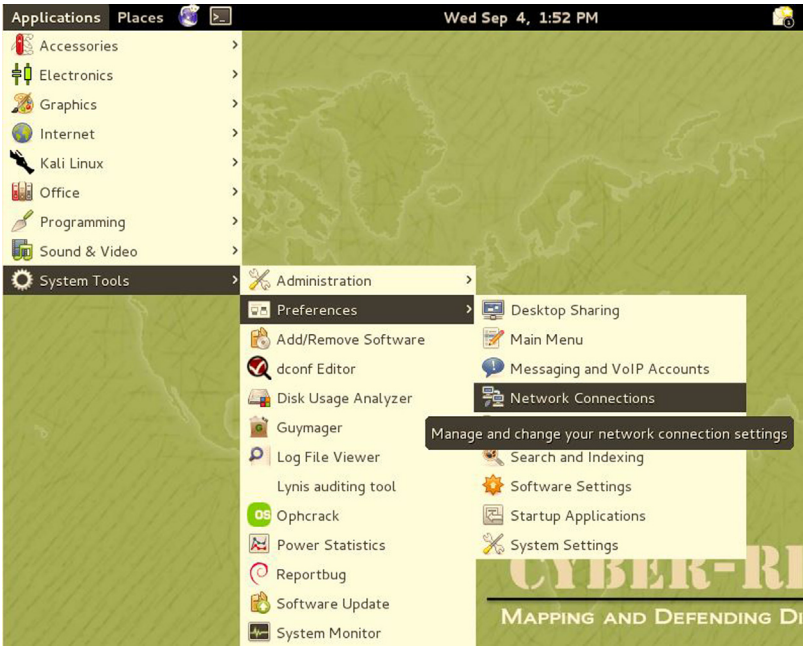

FIGURE 4.4
Graphical network configuration.

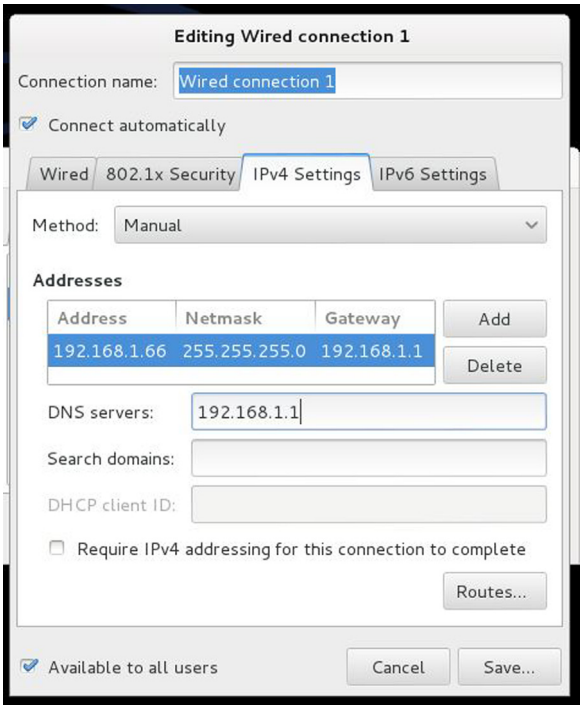

FIGURE 4.5
Graphical wired network configuration.

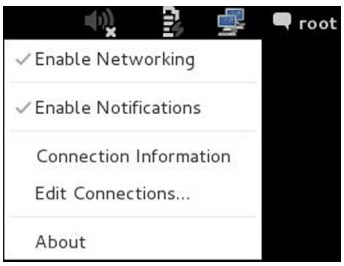

FIGURE 4.6
Alternate graphical wired network configuration.

configured, in cases where multiple NICs are installed, ensure you are configuring the correct card. This example will configure Wired connection 1, a name that can be changed if you like to something more meaningful, the only physical network card in the computer. The configuration dialog box is displayed after selecting the connection to be modified and clicking the Edit button. This will bring up the Editing box for the connection, with the Wired tab selected by default. This tab displays the devices media access control (MAC) address, an

address that is designed to remain the same for the life of the device, see the note on MAC addresses for more information on MAC addresses. The devices identifier is also displayed in parenthesis after the MAC address. In this case, the device identifier is eth0, where eth is short for Ethernet and 0 is the first card in the computer. The numbering sequence for network cards starts at 0 and not 1 so the second card in the computer would be eth1.tab.

Wired Ethernet configurations can be made by selecting the 802.1x Security tab, the IPv4 Settings, or the IPv6 Settings tab. This book will focus on configuring the IP version 4 (IPv4) settings so that tab will be selected. Once selected the configurations for the computers IP address (192.168.1.66), Subnet Mask or Netmask (255.255.255.0), Gateway (192.168.1.1), and DNS servers (192.168.1.1). Multiple DNS servers can be used by separating each with a comma. The configuration can be saved and made active by selecting the Save button.

USING THE COMMAND LINE TO CONFIGURE NETWORK INTERFACES

It is important to understand how to configure, or reconfigure, the network adapter from the command prompt, this is useful when not using the graphical interface for Linux or if you are connected to a system remotely through a terminal window. There are a number of cases in penetration testing where the command line will be the only option for making configuration changes. These changes will need to be made as a user with elevated permissions using the root account is a good way to make these changes on a live distribution and making them using the SDO command is another option for installations of Kali Linux. Once permissions have been elevated, the network card can be configured.

Checking the status of the computers network cards and the status of each card is done with the following command.

```
ifconfig -a
```

This will display the current configuration of all network cards on the computer. In Figure 4.7, two network addresses are displayed, eth0 the first Ethernet card and lo the loopback or internal interface. The settings for this adapter were set using the graphical interface. Changing these is simple using the command prompt.

Starting and Stopping the Interface

The interface can be started using the up option or stopped using the down option of the ifconfig command when specifying the interface to be stopped or started. The following command would stop the first Ethernet adapter.

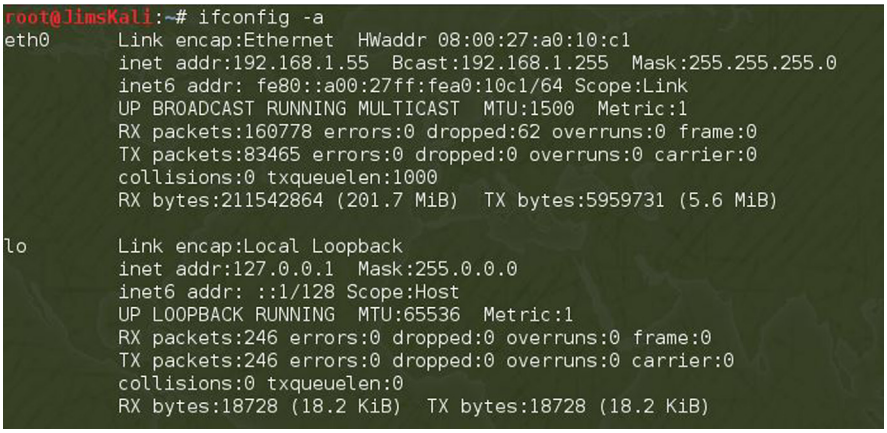

FIGURE 4.7
Viewing network configuration status through the command line.

```
ifconfig eth0 down
```

The following command would start the first Ethernet adapter.

```
ifconfig eth0 up
```

The IP address of this adapter can be changed from 192.168.1.66, its current configuration, to 192.168.1.22 by using the following command.

```
ifconfig eth0 192.168.1.22
```

The command line can be used to change the network mask as well by using the following command. This will set the IP address to 192.168.1.22 and set the subnet mask to 255.255.0.0.

```
ifconfig eth0 192.168.1.22 netmask 255.255.255.0
```

Full configuration of the network card at the command line does require a bit more work than using the graphical user interface as the configuration settings are not all stored in the same location. The default gateway is added or changed, in this case to 192.168.1.2, with the following command.

```
route add default gw 192.168.1.2
```

The name server (or DNS) settings are changed by modifying the resolv.conf file in the /etc directory. This can be changed by editing the file with your favorite editor or simply using the following command at the command prompt.

```
echo nameserver 4.4.4.4 > /etc/resolv.conf
```

The above command will remove the existing nameserver and replace it with 4.4.4.4. To add additional nameservers, the following command will append

new nameserver addresses adding to those already listed in resolv.conf. When the computer performs a name lookup, it will check the first three nameservers in the order they are listed.

```
echo nameserver 8.8.8.8 >> /etc/resolv.conf
```

DHCP from the Command Prompt

One of the easiest ways to configure a network card is to use DHCP services to configure the card. This way the DHCP server will supply all of the configuration settings required for the card. This is convenient for most end users but is not optimal when conducting penetration tests as the system being configured is logged in the DHCP server's database. Use the following commands to disable automatic DHCP configuration when conducting penetration tests. This example uses the nano editor, however other text editors can be used.

```
nano /etc/networking/interfaces
#add the following lines##
auto eth0
iface eth0 inet static
address {IP_Address}
netmask {netmask}
gateway {Gateway_IP_Address}
```

Save the text file and exit to complete the modification. It may be necessary to take down and bring back up the Ethernet interfaces to enable this configuration.

To configure the first network card simply enter the following command at the command prompt.

```
dhclient eth0
```

This will automatically configure the network card using the settings provided by the DHCP server.

USING THE GUI TO CONFIGURE WIRELESS CARDS

Configuring the wireless network card can be accomplished using the GUI described previously during the graphical configuration of the Ethernet interface. In this case, instead of selecting the tab for Wired select the Wireless tab in the Network Connections dialog box.

From this tab select the Add button, which will display a dialog box titled "Editing Wireless connection 1" (assuming this is the first wireless adapter). This dialog has four tabs that are sued to enable configuration of the wireless

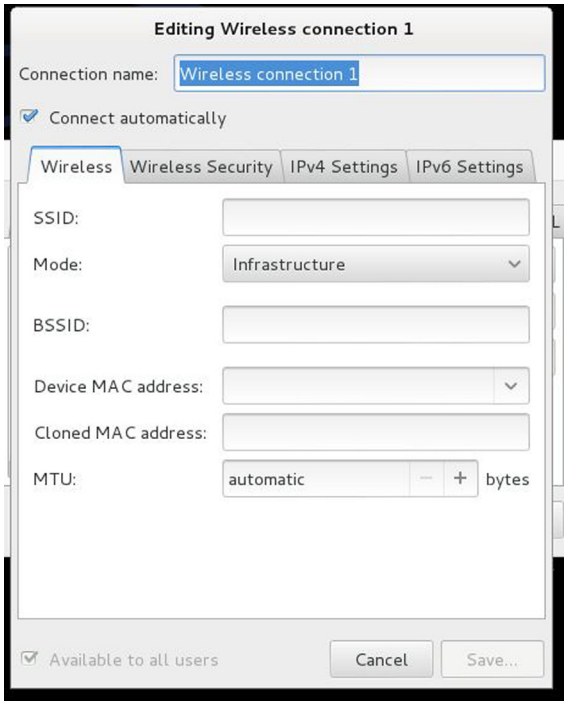

FIGURE 4.8
Graphical wireless network configuration.

card as illustrated in Figure 4.8. This dialog box contains a number of settings that are used to configure the systems wireless card.

Connection Name

The connection name setting defaults to "Wireless connection" followed by the number of the adapter being configured, in this case Wireless connection 1. This name can be changed to something that is more meaningful such as client1 wireless connection.

Connect Automatically Checkbox

When the "Connect automatically" checkbox is selected, the system will automatically try to connect to the wireless network when the computer is started without user intervention. Like DHCP described earlier, this may be convenient for most Linux users but is often not the best option for the penetration tester as it may announce to the testers presence on the network. If the checkbox is deselected, the tester will manually enable the wireless adapter.

Wireless Tab

Service Set Identifier

The service set identifier (SSID) is the network name used to logically identify the wireless network. Each network will have a single SSID that identifies the network, and this name will be used by clients to connect to the network. In networks with central access points, the SSID is set on the access point and all clients must use that SSID to connect to the network. In networks with multiple access points, the SSID must be the same on each to enable communication.

Mode

The wireless card can be configured in two modes either *ad hoc* or infrastructure. *Ad hoc* networks are often informal wireless connections between computers without a central access point performing network management functions. In these connections, each wireless connection must be configured to match each other computers wireless settings to establish the connection. In infrastructure mode, central access points manage the clients connecting to the network and to other computers in the service set. All clients must be configured to match the settings defined in the access point. The main difference between these two options is there is no central administration in *ad hoc* networking while access points centrally manage connections in infrastructure mode.

Basic Service Set Identification

The basic service set identifier (BSSID) is used in infrastructure mode to identify the media access control (MAC) address of the access point. Unlike the SSID, each access point will have a unique BSSID as each should have a unique MAC address.

Device MAC Address

The field for the device MAC address is used to lock this configuration to a physical wireless adapter. This is convenient when a computer has more than one wireless adapter. The drop down for this field will be populated with the MAC addresses of wireless adapters active. Simply select the correct MAC address for the adapter you are configuring.

Cloned MAC Address

Many times the penetration tester will not want to use the actual MAC address of the adapter that is being used on the computer. This may be done to bypass simple security procedures such as MAC address filtering where only systems with specific MAC addresses are allowed to connect to the network. This can also be done to masquerade your wireless adapter to appear to be from another manufacturer to match those wireless cards being used on the wireless network. Input the MAC address that should be cloned and used for this adapter.

Maximum Transmission Unit

The maximum transmission unit (MTU) is a networking setting that is used to determine how large the networking packets can be to communicate with the computer. In most cases, the MTU can be set to automatic and will work fine. In cases where applications require a specific MTU, refer to that applications' documentation to determine the MTU and set it in this area.

Wireless Security Tab

Security Drop Down

The Security drop-down area is used to select the method of securing the wireless network. For *ad hoc* networks, the network users determine the correct security settings, ensuring that each client's security settings match each other computer in the network. In infrastructure mode, each client must be configured to match the security setting of the access point.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an older security method that uses basic encryption technology to provide security equivalent to wired systems. WEP uses either a 10 or 26 hexadecimal key to secure the communication. The WEP encryption standard has security flaws that will allow penetration testers to easily break most WEP encryption keys. Dynamic WEP uses port security measures spelled out in IEEE 802.1x to provide additional security measures to the wireless network.

Lightweight Extensible Authentication Protocol

Lightweight Extensible Authentication Protocol (LEAP) was developed by Cisco Systems to provide enhanced security over the less secure WEP method. LEAP is similar to Dynamic WEP.

WiFi Protected Access

WiFi Protected Access (WPA) is an access technology that enhances security of wireless networks using temporal key integrity protocol (TKIP) and integrity checks. Networks employing WPA are much more resilient to attacks than WEP-protected wireless networks. The initial WPA standard was enhanced with the release of WPA2 by using a stronger security method for encryption. In WPA-personal mode, each computer is configured using a key generated by a password or pass phrase. WPA enterprise requires a central Remote Authentication Dial in User Service (RADIUS) server and 802.1x port security measures. While WPA enterprise is complicated to set up, it provides additional security measures.

Passwords and Keys

If WEP or WPA personal were selected as the security method from the drop down, type the security key in the password/key field. Check the Show password/key checkbox to verify the key being used has been typed correctly. In cases when the password should not be displayed, leave the checkbox unchecked. Some systems use a method of rotating passwords or keys. If this is the case, enter the password or key for each index by selecting the correct index and then entering the correct key or password for that index.

The network may have either open system or shared key authentication. In shared key authentication, the access point sends a challenge text message to the computer attempting to connect. The connecting computer then encrypts the text with the WEP key and returns the encrypted text to the access point. The access point then allows the connection if the encryption key used by the connecting computer produces the correct encryption string. Open system authentication on the other hand allows computers to connect without this challenge and response sequence, relying on the computer using the correct SSID. In both cases, the communication channel is completed when the WEP key is used to secure the channel. While shared key authentication may seem more secure, it is in fact less secure as the challenge text and encrypted text response are sent in clear text allowing anyone monitoring the wireless channel to capture the challenge and response. As the WEP key is used to encrypt the challenge, capturing the challenge and response can allow the WEP key to be determined.

LEAP security uses user name and password. These should be typed into the appropriate fields when LEAP is selected.

Dynamic WEP and WPA enterprise require a number of settings, certificates, and configurations to manage. These settings will not be covered in this text; however, if you are joining a network that uses these methods for security, simply enter the correct details and provide the correct certificates.

IPv4 Settings Tab

Once the information in Wireless and Wireless Security tabs has been completed, the IPv4 configuration can be completed. The process for configuring these settings is identical to the process used to configure the physical Ethernet connection described earlier.

Save

Once all of the required information has been provided, save the settings by clicking the Save button. After the settings have been saved, the computer

will attempt to connect to the network. This is visualized by a graphic in the upper right corner of the screen. Any errors will be displayed in a dialog box.

WEB SERVER

Kali Linux contains an easy-to-configure Apache web server. Having an easily configurable web server is an excellent benefit to the penetration tester. For example, using this service, websites can be created that mimic existing pages on the Internet. These sites can then be used to serve malicious code to users on the target network using social engineering techniques like phishing including collocating servers hosting backdoors, handling callbacks, and providing commands to other malicious software. There are a number of other uses the HTTP service can be used in a penetration test.

Using the GUI to Start, Stop, or Restart the Apache Server

Using the GUI is the easiest way to start, stop, or restart/reset the web service, to do this select Applications from the bar at the top of the Kali screen. From the drop down that is presented select Kali Linux, an action that will cause a submenu to be displayed. From this menu, select System Services, which will in turn display another menu, select the HTTP option on the fly-out menu. This will display the options to start, stop, and restart the Apache service.

Once a selection is made from the menu, a command shell will start and the status of the server will be displayed. Default installations of Kali Linux will cause an error to be displayed when the Apache server is started or restarted. The error you may see is, "Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName." This error will not cause any problems at this point as the web server will be available on the network based on the systems IP address. To correct this error, edit the apache2.conf file in /etc/apache2/ by adding the server name to be used after ServerName at the end of this file and then save the file, as follows.

```
ServerName localhost
```

When the Apache server has been started or restarted, the default web page can be reached by typing the computers IP address in a web browser. The Kali Linux distribution includes the IceWeasle web browser that can be accessed by clicking on the IceWeasle icon on the top bar (a blue globe wrapped by a white weasel).

Starting, Stopping, and Restarting Apache at the Command Prompt

The Apache HTTP server can be easily started, stopped, and restarted using the command /etc/init.d/apache2 followed by the action requested (stop, start, or restart). Using the command line results in the same actions as does the GUI.

```
/etc/init.d/apache2 start
/etc/init.d/apache2 stop
/etc/init.d/apache2 restart
```

The Default Web Page

Once the Apache service is up and running the default (It works!) web page may need to be changed, to do this create the web content that should be displayed on the web page and save it as index.html in the /var/www/ directory. Alternatively, the existing index.html file at this location can be modified and new pages can be added.

FTP SERVER

The File Transfer Protocol (FTP) is used to move files between computers. It is important to note that FTP does not encrypt files or the communication channel between computers so any file traversing the network (or Internet) between the computers can be seen by anyone monitoring the network.

Kali Linux does not include a FTP server so one can be added to facilitate transferring files between systems. There are a number of FTP services that can be added, one of these is the Pure-FTPd (http://www.pureftpd.org/project/pure-ftpd); however, any supported FTP daemon should be acceptable. Use the apt-get command to download and install the Pure-FTPd service using the following command (Figure 4.9).

```
apt-get install pure-ftpd-common pure-ftpd
```

This will install and set up the FTP service. Some minor configuration is necessary to ensure proper operation of the Pure-FTP Server.

```
cd /etc/pure-ftpd/conf
echo no > Bind
echo no > PAMAuthentication
echo no > UnixAuthentication
ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/50pure
```

Next groups and users for the FTP service must be created. First create a new system group.

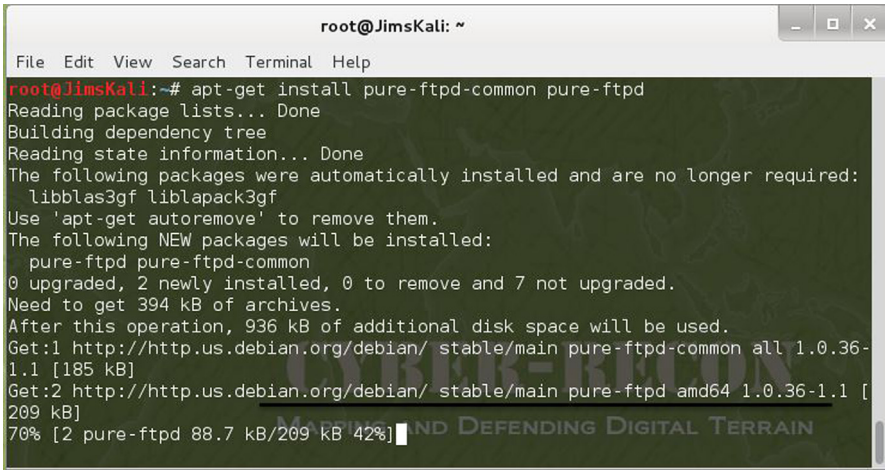

FIGURE 4.9
apt-get install of Pure-FTPd.

```
groupadd ftpgroup
```

Next add for the newly created group. This command will give the user no permission to the home directory or shell access.

```
useradd –g ftpgroup -d /dev/null –s /bin/false ftpuser
```

Create a directory for ftp files.

```
mkdir -p /home/pubftp
```

Add user folders to the ftp directory. In this case, the user sam that is going to be created needs a directory.

```
mkdir /home/pubftp/sam
```

Now add a user and password for the FTP service. In this case, the user sam is created.

```
pure-pw useradd sam –u ftpuser –g ftpgroup –d /home/pubftp/sam
```

A prompt will require a password be created.

Use the following command to update the Pure-FTPd database.

```
pure-pw mkdb
```

Finally start the FTP service with the following command.

```
service pure-ftpd start
```

After starting Pure-FTPd, it's a good idea to test it using the following command.

```
ftp {IP_Address}
```

When prompted enter user name sam and password. If authentication was successful, the FTP server is functioning correctly. If this was not successful, reboot the computer and try to ftp to the server again.

The guide from http://samiux.blogspot.com/2011/08/howto-pure-ftpd-and-atftpd-on-backtrack.html was used to complete the necessary steps to make Pure-FTPd functional.

SSH SERVER

Secure Shell (SSH) is a more secure method of accessing the contents of the Kali Linux file system from remote locations. SSH provides a secure, encrypted communications channel between the communicating computers. This is helpful for penetration testers as it allows file transfers to occur without being inspected by network security tools like intrusion detection system (IDS) and intrusion prevention system (IPS).

Generate SSH Keys

To securely use SSH, encryption keys must be generated to facilitate secure and encrypted communication. To generate these keys, type the following command at the command prompt.

Move the original SSH keys from their default directory; however, do not delete them.

```
mkdir -p /etc/ssh/original_keys
mv /etc/ssh/ssh_host_* /etc/ssh/original_keys
cd /etc/ssh
```

Generate new SSH keys.

```
dpkg-reconfigure openssh-server
```

Start/restart the SSH Daemon.

```
service ssh (start | restart)
```

Managing the SSH Service from the Kali GUI

The SSH server is built into the main file structure of the Kali GUI and is accessed in the same manner that the Apache server is started or stopped. To access the SSH menu, select Applications from the bar at the top of the Kali screen. From the drop down that is presented select Kali Linux, an action that will cause a submenu to be displayed. From this menu select System Services, which will in turn display another menu, select the SSH option on

the fly-out menu. This will display the options to start, stop, and restart the SSH service.

Managing the SSH Server from the Command Line

The SSH server can be started. Stopped and restarted from the command prompt as well. To do this the action being performed, start, stop, or restart, is added after the command /etc/init.d/ssh, as illustrated in the following commands.

```
/etc/init.d/ssh start
/etc/init.d/ssh stop
/etc/init.d/ssh restart
```

Accessing the Remote System

Once the SSH service is started on the Kali system, the computer can be accessed remotely from Linux systems by entering the following command at the command prompt (with a user name of sam and a remote system IP address of 192.168.1.66).

```
ssh sam@192.168.1.66
```

Accessing SSH from a Windows client will require the use of a SSH client. Many of these are available in the Internet, for example putty is a commonly used tool that is available from http://putty.org. Simply install the client and provide the IP address or name of the Kali Linux computer as well as log-in credentials and connect to the remote Kali computer.

CONFIGURE AND ACCESS EXTERNAL MEDIA

Accessing external media like hard drives or thumb drives is much easier in Kali Linux than in earlier versions of Backtrack. Generally media connected to the system using a universal serial bus (USB) connector will be detected and made available by the operating system. However if this does not happen automatically, manually mounting the drive may be necessary.

Manually Mounting a Drive

The first thing that must be done when manually mounting a drive to Kali Linux is to connect the physical drive to the computer. Next open a command prompt and create a mount point. To create the mount point permissions for the account being used will need to be elevated, this can be done with the sudo command if the root account is not being used. The following command will create a mount point called newdrive in the media directory.

```
mkdir /media/newdrive
```

Determine the drive and partition you are connecting using the fdisk command with details on the drive you are attaching. The first hard drive will normally be hda, and the first partition on this drive will be hda1. This sequence continues with additional drives connected to the computer with the second being hdb and the third being hdc. Most of the time, the primary internal drive will be labeled hda so the first external drive will be labeled hdb. To mount the first partition of hdb to the newdrive directory created in the last step use the following command.

```
mount /dev/hdb1 /media/newdrive
```

Once this is complete, the contents of the drive will be available by navigating to the newdrive directory.

```
cd /media/newdrive
```

UPDATING KALI

Like other operating systems, Kali has the built-in ability to update both the operating system and the applications, or packages, installed. As updates to packages become available, they will be posted to the Kali repository. This repository can then be checked to ensure the operating system and applications are up to date. Updates are normally smaller fixes that address software bugs, or errors, or are used to add new hardware capabilities. Updating Kali can be done with the apt-get command line utility.

```
apt-get update
```

UPGRADING KALI

Like updating, upgrading Kali can also be done at the command line with the apt-get utility. Upgrades are normally major revisions to applications or the operating system itself. Upgrades offer new functionality and are much larger that updates normally requiring more time and space on the systems drive.

```
apt-get upgrade
```

An example of the upgrade process is illustrated in Figure 4.10.

ADDING A REPOSITORY SOURCE

By default Kali checks only the software stored in its own repository for updates and upgrades. This is normally a good thing as some updates or

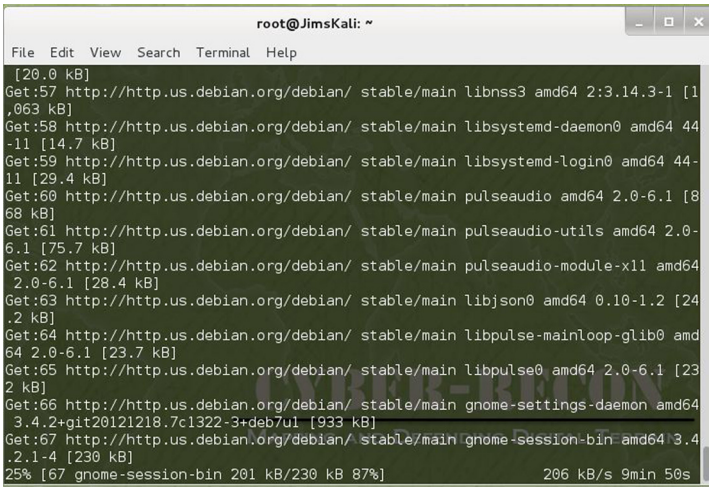

FIGURE 4.10
Upgrade process.

upgrades could break the functionality of Kali. For this reason, updates and upgrades are tested by the Kali developers at Offensive Security before they are added to the official Kali repository. While this is normally a good thing, there are some software applications that are not available when using the default Kali distribution points, and additional repositories may need to be added, in this example the Debian repositories will be added. Using nano, or a different text editor, open /etc/apt/sources.list.

```
nano /etc/apt/sources.list
```

Once open add the following comment and two lines to the bottom of the file.

```
#debian 7 main (this is just a comment)
debhttp://http.us.debian.org/debianstable main contrib non-free
deb-srchttp://http.us.debian.org/debianstable main contrib non-free
```

Now save the file, in nano this is done by pressing the control and "O" key to save the file, save as the same file name by hitting the enter key, finally use control and "X" key to exit. This will add the main Debian repository to the list of repositories that Kali will use to check for updates or upgrades and will also be used to search for applications or packages to install. To finalize this change, use the update command to update Kali with the new repository.

```
Apt-get update
```

SUMMARY

Kali is a powerful tool with an impressive number of tools installed by default. Using many of these features may be foreign to some users, so this chapter covered many of the basics of effectively using this and many other Linux distributions. From configuring network interfaces to adding a FTP server to adding a new repository and upgrading the operating system and applications, this chapter covered many of the basic tasks that must be accomplished to effectively use this toolset. Maintaining Kali is as important as any other operating system and should be done regularly to ensure its tools, applications and the operating system itself is up to date.