Mastering Kali Linux for Advanced Penetration Testing

Robert W. Beggs

Chapter No. 1
"Starting with Kali Linux"
In this package, you will find:
A Biography of the author of the book
A preview chapter from the book, Chapter NO.1 "Starting with Kali Linux"
A synopsis of the book’s content
Information on where to buy this book

About the Author
Robert W. Beggs is the founder and CEO of Digital Defence, a company that specializes in preventing and responding to information security incidents. He has more than 15 years of experience in the technical leadership of security engagements, including penetration testing of wired and wireless networks, incident response, and data forensics.

Robert is a strong evangelist of security and is a cofounder of Toronto Area Security Klatch, the largest known vendor-independent security user group in North America. He is a member on the advisory board of the SecTor Security Conference as well as on several academic security programs. He is an enthusiastic security trainer and has taught graduates, undergraduates, and continuing education students courses in information security at several Canadian universities.

Robert holds an MBA in Science and Technology from Queen's University and is a Certified Information Systems Security Professional.

For More Information:
Firstly, and perhaps most importantly, I would like to thank the developers and supporters of Kali Linux. Together, they have produced one of the most significant tools for securing networks and data. I would like to thank the editors and reviewers at Packt Publishing for their support and seemingly unending patience during the writing of this book. I promise that the next one will go quicker!

I would also like to thank Brian Bourne and other members of the Toronto Area Security Klatch. They've given me an incredible opportunity to learn and share knowledge with the best-ever community of security geeks.

Throughout the writing of this book, my family has given me both incredible motivation and support. Thank you Sarah, Alex, and Annika.

And finally, a very special thank you to my mother and father—I can't remember when I first learned to read—with your encouragement, it was always just natural to have a book in my hands.

Thank you.

For More Information:
Mastering Kali Linux for Advanced Penetration Testing

This book is dedicated to the use of Kali Linux in performing penetration tests against networks. A penetration test simulates an attack against a network or a system by a malicious outsider or insider. Unlike a vulnerability assessment, penetration testing is designed to include the exploitation phase. Therefore, it proves that the exploit is present, and that it is accompanied by the very real risk of being compromised if not acted upon.

Most testers and attackers follow an informal, open source, or proprietary-defined testing methodology that guides the testing process. There are certain advantages of following a methodology:

- A methodology identifies parts of the testing process that can be automated (for example, a tester may always use a ping sweep to identify potential targets; therefore, this can be scripted), allowing the tester to focus on creative techniques to find and exploit vulnerabilities
- The results are repeatable, allowing them to be compared over time or to cross-validate one tester's results against another, or to determine how the security of the target has improved (or not!) over time
- A defined methodology is predictable in terms of time and personnel requirements, allowing costs to be controlled and minimized
- A methodology that has been preapproved by the client, protects the tester against liability in the event there is any damage to the network or data

Formal methodologies include the following well-known examples:

- **Kevin Orrey's penetration testing framework**: This methodology walks the tester through the sequenced steps of a penetration test, providing hyperlinks to tools and relevant commands. More information can be found at [www.vulnerabilityassessment.co.uk](http://www.vulnerabilityassessment.co.uk).

- **Information Systems Security Assessment Framework (ISSAF)**: This comprehensive guide aims to be the single source for testing a network. More information on this can be found at [www.oissg.org](http://www.oissg.org).

- **NIST SP 800-115, technical guide to information security testing and assessment**: Written in 2008, the four-step methodology is somewhat outdated. However, it does provide a good overview of the basic steps in penetration testing. You can get more information at [http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf](http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

For More Information:
• **Open Source Security Testing Methodology Manual (OSSTMM):** This is one of the older methodologies, and the latest version attempts to quantify identified risks. More details can be found at [www.osstmm.org](http://www.osstmm.org).

• **Open Web Application Security Project (OWASP):** This is focused on the 10 most common vulnerabilities in web-based applications. More information on this can be found at [www.owasp.org](http://www.owasp.org).

• **Penetration Testing Execution Standard (PTES):** Actively maintained, this methodology is complete and accurately reflects on the activities of a malicious person. You can get more information at [www.pentest-standard.org](http://www.pentest-standard.org).

• **Offensive (Web) Testing Framework (OWTF):** Introduced in 2012, this is a very promising direction in combining the OWASP approach with the more complete and rigorous PTES methodology. More details can be found at [https://github.com/7a/owtf](https://github.com/7a/owtf).

Unfortunately, the use of a structured methodology can introduce weaknesses into the testing process:

• Methodologies rarely consider why a penetration test is being undertaken, or which data is critical to the business and needs to be protected. In the absence of this vital first step, penetration tests lose focus.

• Many penetration testers are reluctant to follow a defined methodology, fearing that it will hinder their creativity in exploiting a network.

• Penetration testing fails to reflect the actual activities of a malicious attacker. Frequently, the client wants to see if you can gain administrative access on a particular system ("Can you root the box?"). However, the attacker may be focused on copying critical data in a manner that does not require root access, or cause a denial of service.

To address the limitations inherent in formal testing methodologies, they must be integrated in a framework that views the network from the perspective of an attacker, the "kill chain."

**The "Kill Chain" approach to penetration testing**

In 2009, Mike Cloppert of Lockheed Martin CERT introduced the concept that is now known as the "attacker kill chain." This includes the steps taken by an adversary when they are attacking a network. It does not always proceed in a linear flow as some steps may occur in parallel. Multiple attacks may be launched over time at the same target, and overlapping stages may occur at the same time.

---

For More Information:
In this book, we have modified the Cloppert's kill chain to more accurately reflect on how attackers apply these steps when exploiting networks and data services. The following diagram shows a typical kill chain of an attacker:

A typical kill chain of an attacker can be described as follows:

- **Reconnaissance phase** – The adage, "reconnaissance time is never wasted time", adopted by most military organizations acknowledges that it is better to learn as much as possible about an enemy before engaging them. For the same reason, attackers will conduct extensive reconnaissance of a target before attacking. In fact, it is estimated that at least 70 percent of the "work effort" of a penetration test or an attack is spent conducting reconnaissance! Generally, they will employ two types of reconnaissance:
  
  o **Passive reconnaissance** – This does not directly interact with the target in a hostile manner. For example, the attacker will review the publicly available website(s), assess online media (especially social media sites), and attempt to determine the "attack surface" of the target.

  One particular task will be to generate a list of past and current employee names. These names will form the basis of attempts to brute force, or guessing passwords. They will also be used in social engineering attacks. This type of reconnaissance is difficult, if not impossible, to distinguish from the behavior of regular users.

  o **Active reconnaissance** – This can be detected by the target but, it can be difficult to distinguish most online organizations' faces from the regular backgrounds.

  Activities occurring during active reconnaissance include physical visits to target premises, port scanning, and remote vulnerability scanning.

For More Information:

• **The delivery phase** – Delivery is the selection and development of the weapon that will be used to complete the exploit during the attack. The exact weapon chosen will depend on the attacker's intent as well as the route of delivery (for example, across the network, via wireless, or through a web-based service). The impact of the delivery phase will be examined in the second half of this book.

• **The exploit or compromise phase** – This is the point when a particular exploit is successfully applied, allowing attackers to reach their objective. The compromise may have occurred in a single phase (for example, a known operating system vulnerability was exploited using a buffer overflow), or it may have been a multiphase compromise (for example, an attacker physically accessed premises to steal a corporate phone book. The names were used to create lists for brute force attacks against a portal logon. In addition, e-mails were sent to all employees to click on an embedded link to download a crafted PDF file that compromised their computers.). Multiphase attacks are the norm when a malicious attacker targets a specific enterprise.

• **Post exploit: action on the objective** – This is frequently, and incorrectly, referred to as the "exfiltration phase" because there is a focus on perceiving attacks solely as a route to steal sensitive data (such as login information, personal information, and financial information); it is common for an attacker to have a different objective. For example, a business may wish to cause a denial of service in their competitor's network to drive customers to their own website. Therefore, this phase must focus on the many possible actions of an attacker. One of the most common exploit activity occurs when, the attackers attempt to improve their access privileges to the highest possible level (vertical escalation), and to compromise as many accounts as possible (horizontal escalation).

• **Post exploit: persistence** – If there is value in compromising a network or system, then that value can likely be increased if there is persistent access. This allows attackers to maintain communications with a compromised system. From a defender's point of view, this is the part of the kill chain that is usually the easiest to detect.

Kill chains are metamodels of an attacker's behavior when they attempt to compromise a network or a particular data system. As a metamodel, it can incorporate any proprietary or commercial penetration testing methodology. Unlike the methodologies, however, it ensures a strategic-level focus on how an attacker approaches the network. This focus on the attacker's activities will guide the layout and content of this book.

For More Information:
What This Book Covers

This book is divided into two parts. In *Part 1, The Attacker's Kill Chain*, we will follow the steps of a kill chain, analyzing each phase in detail. In *Part 2, The Delivery Phase*, we will focus on the delivery phase and some of the available methodologies to understand how attacks take place, and how this knowledge can be used to secure a network.

*Chapter 1, Starting with Kali Linux*, introduces the reader to the fundamentals of Kali Linux, and its optimal configuration to support penetration testing.

*Chapter 2, Identifying the Target – Passive Reconnaissance*, provides a background on how to gather information about a target using publicly available sources, and the tools that can simplify the reconnaissance and information management.

*Chapter 3, Active Reconnaissance and Vulnerability Scanning*, introduces the reader to stealthy approaches that can be used to gain information about the target, especially the information that identifies vulnerabilities, which could be exploited.

*Chapter 4, Exploit*, demonstrates the methodologies that can be used to find and execute exploits that allow a system to be compromised by an attacker.

*Chapter 5, Post Exploit – Action on the Objective*, describes how attackers can escalate their privileges to achieve their objective for compromising the system, including theft of data, altering data, launching additional attacks, or creating a denial of service.

*Chapter 6, Post Exploit – Persistence*, provides a background on how to configure a compromised system so that the attacker can return at will and continue post-exploit activities.

*Chapter 7, Physical Attacks and Social Engineering*, demonstrates why being able to physically access a system or interact with the humans who manage it provides the most successful route to exploitation.

*Chapter 8, Exploiting Wireless Communications*, demonstrates how to take advantage of common wireless connections to access data networks and isolated systems.

*Chapter 9, Reconnaissance and Exploitation of Web-based Applications*, provides a brief overview of one of the most complex delivery phases to secure: web-based applications that are exposed to the public Internet.

*Chapter 10, Exploiting Remote Access Communications*, provides an increasingly important route into systems as more and more organizations adopt distributed and work-from-home models that rely on remote access communications that are themselves vulnerable to attack.

For More Information:
Starting with Kali Linux

Kali Linux (Kali) is the successor to the BackTrack penetration testing platform which is generally regarded as the de facto standard package of tools used to facilitate penetration testing to secure data and voice networks. This chapter provides an introduction to Kali, and focuses on customizing Kali to support some advanced aspects of penetration testing. By the end of this chapter, you will have learned:

- An overview of Kali
- Configuring network services and secure communications
- Updating Kali
- Customizing Kali
- Extending Kali’s functionality with third-party applications
- Effective management of penetration tests

Kali Linux

BackTrack (BT), (www.offensive-security.com) was released to provide an extensive variety of penetration testing and defensive tools that were perfect for auditors and network administrators interested in assessing and securing their networks. The same tools were used by both authorized and unauthorized (hackers) penetration testers.

The final version of BackTrack, BT 5r3, was released in August 2012. Based on the Ubuntu Linux platform, it was widely adopted and supported by the security community. Unfortunately, its file architecture made it difficult to manage the array of tools and their accompanying dependencies.

For More Information:
In BackTrack, all of the tools used for penetration testing were placed in the 
\texttt{/pentest} directory. Subfolders such as \texttt{/web} or \texttt{/database} helped to further define the location of tools. Finding and executing tools within this hierarchy could be counterintuitive. For example, is sqlninja, which identifies an SQL injection, a web vulnerability assessment tool, a web exploit tool, or a database exploit tool?

In March 2013, BackTrack was superseded by Kali Linux, which uses a new platform architecture based on the Debian GNU/Linux operating system.

Debian adheres to the \textbf{Filesystem Hierarchy Standard (FHS)}, which is a significant advantage over BackTrack. Instead of needing to navigate through the \texttt{/pentest} tree, you can call a tool from anywhere on the system because applications are included in the system path.

Other features of Kali include the following:

- Support for multiple desktop environments such as Gnome, KDE, LXDE, and XFCE, and provides multilingual support.
- Debian-compliant tools are synchronized with the Debian repositories at least four times daily, making it easier to update packages and apply security fixes.
- Support for ISO customizations, allowing users to build their own versions of Kali. The bootstrap function also performs enterprise-wide network installs that can be automated using pre-seed files.
- \textbf{ARME}L and \textbf{ARMHF} support allows Kali to be installed on devices such as Raspberry Pi, ODROID-U2/-X2, and the Samsung Chromebook.
- Over 300 penetration testing data forensics and defensive tools are included. They provide extensive wireless support with kernel patches to permit the packet injection required by some wireless attacks.
- Kali remains an open source project that is free. Most importantly, it is well supported by an active online community.

Throughout this book, we’ll be using a VMware \textbf{virtual machine (VM)} of 64-bit Kali (refer to \textit{Appendix, Installing Kali Linux} for instructions on installing Kali).

A VM is used because it makes it easy to rapidly execute certain applications in other operating systems, such as Microsoft Windows. In addition, a VM can be archived with the results from a penetration test, allowing the archive to be reviewed to determine if a particular vulnerability would have been detected with the toolset that was used for testing.
When Kali is launched, the user will be taken to the default desktop GUI with a menu bar at the top and a few simple icons. By selecting the menu item Applications, and then Kali Linux, the user will gain access to a menu system that contains the Top 10 Security Tools as well as a series of folders, organized in the general order that would be followed during a penetration test, as shown in the following screenshot:

The menu will be familiar to users of BT 5r3. However, there are some changes, which include simplified access to network services and communications.

For More Information:
Configuring network services and secure communications

The first step in being able to use Kali is to ensure that it has connectivity to either a wired or wireless network to support updates and customization.

You may need to obtain an IP address by DHCP (Dynamic Host Configuration Protocol), or assign one statically. First, confirm your IP address using the `ifconfig` command from a terminal window, as shown in the following screenshot:

![ifconfig output]

In this particular case, the VM has been assigned an IP address of 192.168.204.132. If an IP address was not obtained, an address can be assigned by DHCP using the command `dhclient eth0` (or other available interfaces, which will depend on the specific configuration of the system being used).

If a static IP address is used, additional information may be required. For example, you can assign a static IP of 192.168.204.128 as follows:

```
host IP address: 192.168.204.128
subnet mask: 255.255.255.0
default gateway: 192.168.204.1
DNS server: 192.168.204.10
```

For More Information:
Enter a terminal window and enter the following command:

```
root@kali:~# ifonconfig eth0 192.168.204.128/24
root@kali:~# route add default gw 192.168.204.1
root@kali:~# echo nameserver 192.168.204.10 > /etc/resolv.conf
```

Changes made to IP settings are nonpersistent, and will be lost when Kali is rebooted. To make the changes permanent, you will need to edit the `/etc/network/interfaces` file, as shown in the following screenshot:

By default, Kali does not start with the DHCP service enabled. Doing so announces the new IP address on the network, and this may alert administrators about the presence of the tester. For some test cases, this may not be an issue, and it may be advantageous to have certain services start automatically during boot up. This can be achieved by entering the following commands:

```
root@kali:~# update-rc.d networking defaults
root@kali:~# /etc/init.d/networking restart
```

Kali installs with network services that can be started or stopped as required, including DHCP, HTTP, SSH, TFTP, and the VNC server. These services are usually invoked from the command line, however, some are accessible from the Kali menu.

For More Information:
Adjusting network proxy settings

Users located behind an authenticated or unauthenticated proxy connection must modify `bash.bashrc` and `apt.conf`. Both files are located in the `/root/etc` directory.

1. Edit the `bash.bashrc` file, as shown in the following screenshot, use a text editor to add the following lines to the bottom of the `bash.bashrc` file:

   ```bash
   export ftp_proxy="ftp://user:password@proxyIP:port"
   export http_proxy="http://user:password@proxyIP:port"
   export https_proxy="https://user:password@proxyIP:port"
   export socks_proxy="https://user:password@proxyIP:port"
   ```

2. Replace `proxyIP` and `port` with your proxy IP address and port number respectively, and replace the username and password with your authentication username and password. If there's no need to authenticate, write only the part following the `@` symbol.

3. In the same directory, create the `apt.conf` file and enter the following command lines, as shown in the following screenshot:

For More Information:

4. Save and close the file. Log out and then log in to activate the new settings.

**Securing communications with Secure Shell**

To minimize detection by a target network during testing, Kali does not enable any externally-listening network services. Some services, such as Secure Shell (SSH), are already installed. However, they must be enabled prior to use.

Kali comes preconfigured with default SSH keys. Before starting the SSH service, it’s a good idea to disable the default keys and generate a unique keyset for use.

Move the default SSH keys to a backup folder, and then generate a new SSH keyset using the following command:

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

The process of moving the original keys and generating the new keyset is shown in the following screenshot.

For More Information:
To verify that the newly generated keys are unique, calculate their `md5sum` hash values, and compare with the original keys as shown in the following screenshot.

To start the SSH service using the menu, select Applications | Kali Linux | System Services | SSHD | SSHD Start.

To start SSH from the command line, use the command line shown in the following screenshot:

```
root@kali:~# /etc/init.d/ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
```

To verify that SSH is running, perform a `netstat` query, as shown in the following screenshot:

```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name    tcp  0  0  0.0.0.0:22       0.0.0.0:*              LISTEN
19783/sshd
```

The SSH daemon is listening on port 22 in the previous example. To stop SSH, use the following command:

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

For More Information:
Chapter 1

Updating Kali Linux
Kali must be patched regularly to ensure that the base operating system and applications are up-to-date and that security patches have been applied.

The Debian package management system
Debian's package management system relies on discrete bundled applications called packages. Packages can be installed or removed by the user to customize the environment, and support tasks such as penetration testing. They can also extend the functionality of Kali, supporting tasks, such as communications (Skype, instant messaging, and secure e-mails) or documentation (OpenOffice and Microsoft Office running under Wine).

Packages are stored in repositories and are downloaded to the system user to ensure the integrity of the package.

Packages and repositories
By default, Kali uses only the official Kali repositories. It is possible that an incomplete installation process may not add the repositories to the correct sources.list file, or that you may wish to extend the available repositories when new applications are added.

Updating the sources.list file can be done from the command line (echo deb http://http.kali.org/kali kali main contrib non-free >> /etc/apt/sources.list), or by using a text editor.

The default package repositories that should be present in /etc/apt/sources.list are listed as follows; if not present, edit the sources.list file to include them:

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

Not every Kali tool is presently maintained in the official tool repositories. If you choose to update a tool manually, it is possible that you will overwrite existing packaged files and break dependencies. Therefore, some tools that have not been officially moved to Debian repositories, such as the aircrack-ng, dnsrecon, sqlmap, beef-xss, and Social Engineering Toolkit (se-toolkit), are maintained in the Bleeding Edge repository. This repository may also be added to sources.list using the following command line:

```
## Bleeding Edge repository
   deb http://repo.kali.org/kali kali kali-bleeding-edge main
```

For More Information:
**Dpkg**

Dpkg is Debian's package management system. This command-line application is used to install, remove, and query packages. In general, `dpkg` performs actions on individual packages.

`dpkg` is particularly useful in compiling a list of installed applications in Kali using the command `dpkg -l > list.txt`. If you want to know if a specific tool is installed, use `dpkg -l | grep <tool name>`.

The following screenshot shows an excerpt of the returned data when `dpkg -l` is invoked, providing a list of all applications installed on the Kali distribution; this is particularly useful in identifying applications that may only be accessible directly from the command line.

```
root@kali:~# dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
Status=Not/Conf-Files/Unpacked/half-conf/half-inst/trig-aWait/Trig-pend
/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
++===================================
11 acckcheck 0.2.1-1kalil3 amd64  Password dictionary attack tool for
11 accountsservice 0.6.21-8 amd64  query and manipulate user account in
11 ace-volp 1.10.1kalil4 amd64  A simple VoIP corporate directory en
11 acl 2.2.51-8 amd64  Access control list utilities
11 adduser 3.113+mmu3 all  add and remove users and groups
11 afflib-tools 3.7.1-0kalil3 amd64  support for Advanced Forensics forms
11 aircrack-ng 1.2-svn2256+ amd64  An 882.11 WEP and WPA-PSK key crack1
```

**Using Advanced Packaging Tools**

Advanced Packaging Tools (APT), extend the functionalities of `dpkg` by searching repositories and installing or upgrading packages along with all the required dependencies. The APT can also be used to upgrade a complete distribution.

The most common `apt` commands are as follows:

- **`apt-get update`**: This is used to resynchronize the local package index files with their source as defined in `/etc/apt/sources.list`. The `update` command should always be used first, before performing an `upgrade` or `dist-upgrade`.

- **`apt-get upgrade`**: This is used to install the newest versions of all packages installed on the system using `/etc/apt/sources.list`. Packages that are installed on Kali with new versions available are upgraded. The upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

For More Information:

• **`apt-get dist-upgrade`:** This upgrades all packages currently installed on the system and their dependencies. It also removes obsolete packages from the system.

The `apt-get` command can also be used to show a full description of a package and identify its dependencies (`apt-cache show <package name>`) or remove a package (`apt-get remove <package name>`).

Run the `apt-get update` command and the `upgrade` command at start-up to ensure your session is using the most up-to-date tools. The easiest way to do this is to create an `update.sh` script that includes the following command line:

```
apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
```

Some applications are not upgraded by the `apt-get` command. For example, the local copy of the `exploit-db` archive must be manually upgraded. Create a script named `update.sh` and add the following commands to it, to automate the update process:

```
cd /usr/share/exploitdb
wget http://www.exploit-db.com/archive.tar.bz2
tar -xvjf archive.tar.bz2
rm archive.tar.bz2
```

### Configuring and customizing Kali Linux

Kali is a framework that is used to complete a penetration test. However, the tester should never feel tied to the tools that have been installed by default, or by the look and feel of the Kali desktop. By customizing BackTrack, a tester can increase the security of client data that is being collected, and make it easier to do a penetration test.

Common customizations made to Kali include:

- Resetting the root password
- Adding a non-root user
- Speeding up Kali operations
- Sharing folders with MS Windows
- Creating encrypted folders

For More Information:

Resetting the root password

To change a user password, use the following command:

```
passwd root
```

You will then be prompted to enter a new password, as shown in the following screenshot:

```
root@kali:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
pwd: password updated successfully
root@kali:~#
```

Adding a non-root user

Many of the applications provided in Kali must run with root-level privileges in order to function. Root-level privileges do possess a certain amount of risk, for example, miskeying a command or using the wrong command can cause applications to fail or even damage the system being tested. In some cases, it is preferable to test with user-level privileges. In fact, some applications force the use of lower-privilege accounts.

To create a non-root user, you can simply use the command `adduser` from the terminal and follow the instructions that appear, as shown in the following screenshot:

```
root@kali:~# adduser noroot
Adding user 'noroot' ...
Adding new group 'noroot' (1001) ...
Adding new user 'noroot' (1001) with group 'noroot' ...
Creating home directory `/home/noroot' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
pwd: password updated successfully
Changing the user information for noroot
Enter the new value, or press ENTER for the default
 Full Name []: rwbegs
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@kali:~#
```

Speeding up Kali operations

Several tools can be used to optimize and speed up Kali operations:

- When using a virtual machine, install the VM’s software drive package: Guest Additions (VirtualBox) or VMware Tools (VMware).

For More Information:

• When creating a virtual machine, select a fixed disk size instead of one that is dynamically allocated. It is faster to add files to a fixed disk, and there is less file fragmentation.

• The preload application (apt-get install preload) identifies a user's most commonly used programs and preloads binaries and dependencies into memory to provide faster access. It works automatically after the first restart following installation.

• BleachBit (apt-get install bleachbit) frees disk space and improves privacy by freeing the cache, deleting cookies, clearing Internet history, shredding temporary files, deleting logs, and discarding other unnecessary files. Advanced features include shredding files to prevent recovery and wiping free disk space to hide traces of files that have not been fully deleted.

• By default, Kali does not show all applications that are present in the start-up menu. Each application that is installed during the boot-up process slows the system data, and may impact memory use and system performance. Install Boot Up Manager (BUM) to disable unnecessary services and applications that are enabled during the boot up (apt-get install bum), as shown in the following screenshot:

For More Information:
Starting with Kali Linux

• Add `gnome-do (apt-get install gnome-do)` to launch applications directly from the keyboard. To configure `gnome-do`, select it from the Applications | Accessories menu. Once launched, select the Preferences menu, activate the Quiet Launch function, and select a launch command (for example, `Ctrl + Shift`). Clear any existing commands, and then enter the command line to be executed when the launch keys are selected.

Rather than launching directly from the keyboard, it is possible to write specific scripts that launch complex operations.

Sharing folders with Microsoft Windows

The Kali toolset has the flexibility to share results with applications residing on different operating systems, especially Microsoft Windows. The most effective way to share data is to create a folder that is accessible from the host operating system as well as the Kali Linux VM guest.

When data is placed in a shared folder from either the host or the VM, it is immediately available via the shared folder to all systems that access that shared folder.

To create a shared folder, perform the following steps:

1. Create a folder on the host operating system. In this example, it will be called `Kali_Share`.
2. Right-click on the folder and select the Sharing tab. From this menu, select Share.
3. Ensure that the file is shared with Everyone, and that Permission Level for this share is set to Read / Write.
4. If you have not already done so, install the appropriate tools onto BackTrack. For example, when using VMware, install the VMware tools (refer to Appendix, Installing Kali Linux).
5. When the installation is complete, go to the VMware menu and select Virtual Machine Setting. Find the menu that enables Shared Folders and select Always Enabled. Create a path to the shared folder that is present on the host operating system, as shown in the following screenshot:

For More Information:
Although VirtualBox uses different menu titles, the process is the same.

6. Open the file browser on the Kali desktop. The shared folder will be visible in the mnt folder (it might be placed in a sub-folder, \hgfs\).

7. Drag the folder onto the Kali desktop to create a link to the real folder.

8. Everything placed in the folder will be accessible in the folder of the same name on the host operating system, and vice versa.

The shared folder, which will contain sensitive data from a penetration test, must be encrypted to protect the client's network and reduce the tester's liability should the data ever be lost or stolen.

For More Information:
Creating an encrypted folder with TrueCrypt

During a penetration test, you will have access to sensitive client information, including exploitable vulnerabilities and copies of successfully breached data. It is the tester’s legal and moral responsibility to ensure that this information in his care is secured at all times. The best means of meeting this responsibility is to ensure that all client information is encrypted during storage and transmission.

To install TrueCrypt on BackTrack, complete the following steps:

1. In the Applications menu, select Accessories | TrueCrypt.
2. To create an encrypted folder, open the application. You will be presented with the main menu, as shown in the following screenshot:

For More Information:
3. On the main menu, select the Create Volume button. This will launch the TrueCrypt Volume Creation Wizard, as shown in the following screenshot:

4. Select Create an encrypted file container, and then click on Next.

5. The next screen will prompt for Volume Type, select Standard TrueCrypt volume, and click on Next.

6. On the Volume Location screen, select Select File. You will be asked to Specify a New TrueCrypt Volume by providing a Name, and indicating that it will save in the folder specified, as shown in the following screenshot:

For More Information:
7. Chose a filename. Do not choose a filename related to the client being tested, or which indicates that sensitive material is present in the directory. Use a number or code word to represent the client, and a generic title for results. Save the file on the desktop, then click on Next.

8. The next screen will provide you with Encryption Options. Select Encryption Algorithm from the drop-down menu. There are several choices, but for regular purposes, AES (the default 256-bit key) will suffice. You will also select a Hash Algorithm from the drop-down menu (the default, RIPEMD-160, should be sufficient). After your choices are complete, click on the Next button, as shown in the following screenshot:

![Encryption Options](image)

9. You will now be prompted for Volume Size. You should have a minimum size of approximately 500 MB, but this may vary depending on the testing regime. Click on Next.

For More Information:
10. The **Volume Password** should be selected according to the rules provided for strong passwords. Select and confirm the password, then click on **Next**, as shown in the following screenshot:

![Volume Password screenshot](image)

11. The next screen allows you to select **Format Options**. For **Filesystem Options** select **FAT** from the drop-down menu. Click on **Next**.

12. The next screen, **Volume Format**, creates a random key for the encrypted filesystem. The key is based on mouse movements, and you will be prompted to move the mouse over the window for a long period to ensure the randomness (cryptographic strength) of the encryption keys. When done, click on **Format** to create the TrueCrypt volume.

13. The final volume has been created. It will appear as an icon on the desktop. The volume is encrypted, and it can be copied to an external storage device or moved to the host system and remain encrypted.

For More Information:  
To use the encrypted volume, you must first choose a **Slot** to manage the encrypted folder in the main **TrueCrypt** menu. When this is done, use the **Select File** button to select the name of the encrypted file. In this case, we'll use a previously made file called `pentest` located on the desktop, as shown in the following screenshot:

Click on the **Mount** button. At this point, you will be prompted for the password, as shown in the following screenshot:

When the correct password is entered, you will see the **Slot 1** details change to reflect the encrypted folder's properties, and a new icon called `truecrypt1` will be displayed on the desktop, will be displayed on the desktop, as shown in the following screenshot:

---

**For More Information:**

If you double-click on the `truecrypt1` icon, you will be taken to a **File Browser** view.

At this point, it will act as a regular directory, and you can use the folder to store all of the test-related information. When you work with the contents of the folder, and wish to ensure that all data is encrypted, select **Dismount** on the main menu. The folder will revert to an encrypted state.

**Managing third-party applications**

Although Kali comes preloaded with several hundred applications, it is likely that you will need to install additional applications to effectively test specific environments (such as industrial systems), add new cutting edge tools, or ensure that your favorite tools are installed. Kali makes it easy to locate, install, and manage these tools.

**Installing third-party applications**

There are multiple ways to install third party applications: using the `apt-get` command, accessing a GitHub repository, and directly installing the application.

All tools should be installed from the Kali Linux repository using the `apt-get install` command. The `install` command can be executed from the command line in a terminal window, or the user may select a graphical package management tool.
Recommended third-party applications include:

- **apt-file**: This is a command-line tool to search within packages of the APT packaging system. It allows you to list contents of a package without installing or fetching it.
- **gnome-tweak-tool**: This allows users to change themes and rapidly configure desktop options.
- **instanbul**: This is a desktop screen recorder that allows you to make a movie of desktop activities.
- **openoffice**: This is an open-source office productivity suite that assists in documentation.
- **scrub**: This is a secure deletion (anti-forensic) tool that securely deletes data to comply with stringent government standards using various overwrite patterns.
- **shutter**: This is a screenshot tool that captures images of a desktop, open window, or a selection.
- **teamviewer**: This supports remote access and remote administration. It also allows testers to place a pre-configured computer (a dropbox) on the target network and control testing from a remote location.
- **terminator**: This is a replacement for the Linux terminal window that allows horizontal scrolling—no more wrapped text!

Tools that are not present in a Debian repository and are accessible using `apt-get install` can still be installed on Kali. However, the user must accept that manual installs are not coordinated with repositories, and they may break dependencies causing applications to fail.

Some tools use the GitHub online repository for software development projects. Many developers favor this open repository due to the flexibility of the Git revision system as well as the social-media aspects of the software sites. One tool that we will be using is `recon-ng`, a web reconnaissance framework.

To clone the current version of `recon-ng` from the GitHub repository, use the following command line:

```
cd /opt; git clone https://LaNMaSteR53@bitbucket.org/LaNMaStEr53/recon-ng.git
```

```
cd opt/recon-ng
./recon-ng.py
```

For More Information:

Finally, some applications must be manually installed. For example, to restore the asynchronous port scanner Unicornscan, can back to Kali, you must:

- Ensure the dependencies are first present: `apt-get install flex`
- Download the latest version of Unicornscan (www.unicornscan.org – the current version is unicornscan-0.4.7-2)
- Extract the contents of the file to a new directory: `tar jxf unicornscan-0.4.7-2.tar.bz2`
- Change to the directory containing Unicornscan: `cd unicornscan-0.4.7/`
- Compile the source code: `./configure CFLAGS=-D_GNU_SOURCE && make && make install`

The exact dependencies and make install process will vary for each application, so you will need to refer to the developer's README file to ensure correct installation and configuration of these applications.

### Running third-party applications with non-root privileges

Kali Linux is intended to support penetration testing. Most of the tools require root-level access, which is why access to the toolset and data is protected with passwords and encryption.

However, some third-party tools are not meant to run with root-level privileges. Tools such as web browsers may be compromised, and giving an attacker access to root privileges can have a significant security impact.

If root access is not required, tools should follow the principle of least privilege and run as non-root users.

To run an application that normally runs as a non-root user, log on to Kali using a root account. Kali should be configured with a non-root account. In this example, we will use the noroot account previously created with the adduser command.

Perform the following steps to run the web browser Iceweasel as non-root:

1. Create a non-root user account. In this example, we will use noroot.
2. We will use sux, which is a wrapper application that transfers credentials from a privileged user to a target non-root user. Download and install sux using the `apt-get install` command.

For More Information:
3. Start the web browser, and then minimize it.

4. Enter the command line: `ps aux | grep iceweasel`. As you can see, Iceweasel is running with root privileges.

5. Close Iceweasel, and relaunch using the command `su - noroot iceweasel`, as shown in the following screenshot:

```bash
root@test:~# ps aux | grep iceweasel
root  4694  5.1 17.9 585844 89084 ?    SL   17:56   0:81 iceweasel
root  4697  0.0  0.1  7768  860 pts/0   S+   17:56   0:00 grep iceweasel

root@test:~# su - noroot iceweasel
```

If you examine the Iceweasel title bar, shown in the following screenshot, you will see that it was invoked as the user `noroot`, an account that did not have administrator privileges.

![Iceweasel Title Bar](image)

You can also confirm that Iceweasel is running under the `noroot` account by examining the open processes, as shown in the following screenshot:

```bash
root@test:~# ps aux | grep iceweasel
eval $TERM; exec env TERM='xterm' DISPLAY=:0.0 "iceweasel";
root  4758  0.8 19.0 592224 94976 ?    Ssl  17:57   0:02 iceweasel
root  4847  3.0  0.1  7768  860 pts/1   S+   18:02   0:00 grep iceweasel
```

**Effective management of penetration tests**

One of the most difficult aspects of penetration testing is remembering to test all of the relevant parts of the network or system target, or trying to remember if the target was actually tested, after the testing has been completed.
BT 5r3 emphasized the use of management tools such as Draedis and MagicTree. These tools facilitate group testing by providing a central repository for test data. In addition, they usually provide some framework so that testers know where they are within a testing methodology, and what tests remain to be completed. Tools of this nature are excellent in coordinating defined group activities during a vulnerability assessment or penetration test.

These tools remain in the Applications | Kali Linux | Reporting Tools | Evidence Management menu.

But what about complex penetration tests where the methodology may be more fluid as it adapts to the network target?

Some testers use keyloggers or Wireshark during testing to record keystrokes and packet traffic generated during the test. This data can be especially useful if the testing is causing a network or application outage, because replaying and analyzing the packets sent can identify which packet tools impacted the network.

Kali Linux includes several tools that are more suited to making rapid notes and serving as a repository of rapidly added cut-and-paste data, including KeepNote and the Zim desktop wiki.

Testers not only need to perform tests and collect data, they also need to be able to provide their findings to the client. This can be difficult, as some results are transient—a test demonstrates a finding at one point in time, and then something is changed on the target system, and future testing fails to demonstrate the exploitable vulnerability, even though it's possible for it to re-emerge.

The other challenge with positive results is that they need to be demonstrated to a client in a way that's understandable.

The golden rule is to always grab a screenshot of any positive, or potential, finding. Use a tool such as Shutter to capture images from the desktop.

By default, Kali is configured with CutyCapt, which is a cross-platform command-line utility that captures a web page and creates a variety of image types, including PDF, PS, PNG, JPEG, TIFF, GIF, and BMP.

For More Information:
For example, to create an image of a specific size from the Google search page, enter the following from a command-line prompt:

```
cutycapt --url=http://www.google.com --out=google.png --min-width=300 --min-height=250.
```

On execution, an image of the size specified in the previous command is displayed, as shown in the following screenshot:

Cutycapt is especially useful when demonstrating the presence of web-based vulnerabilities such as cross-site scripting.

Static images can be very useful, however, a video of an exploit that compromises a target network and shows the actions of an attacker as they compromise sensitive data is a very compelling tool. The instanbul screen recorder creates a video of an "exploit in progress," which allows the exploit to be replayed for training purposes, or to demonstrate the vulnerability to the client.

**Summary**

In this chapter, we examined Kali, a collection of tools widely used by legitimate penetration testers and hackers to assess the security of data systems and networks. We emphasized Kali as a virtual machine, allowing both the host operating system and the VM guest to support testing.
Kali is a repository of tools, and one of the challenges in using it is ensuring that the tools are up-to-date. We reviewed the Debian packet management system, and how updates could be initiated from both the command line and from GUI applications. Most importantly, we learned how to customize Kali to increase the security of our tools and the data that they collect. We are working to achieve the goal of making tools support our process, instead of the other way around!

In the next chapter, we will learn how to effectively use Open Source Intelligence (OSINT) to identify the vulnerable attack surfaces of our target and create customized username:password lists to facilitate social engineering attacks and other exploits.
Chapter 11, *Client-side Exploitation*, focuses on attacks against applications on the end-user's systems, which are frequently not protected to the same degree as the organization's primary network.

Appendix, *Installing Kali Linux*, provides an overview of how to install Kali Linux, and how to employ a whole-disk encryption to avoid an intercept of confidential testing data.

For More Information:
Where to buy this book


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

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