Mastering Kali Linux Wireless Pentesting

This book will take you on a journey where you will learn to master advanced tools and techniques in order to conduct wireless penetration testing with Kali Linux.

You will begin by gaining an understanding of setting up and optimizing your penetration testing environment for wireless assessments. Then, the book will take you through a typical assessment from reconnaissance, information gathering, and scanning the network through exploitation and data extraction from your target. You will get to know various ways to compromise the wireless network using browser exploits, vulnerabilities in firmware, web-based attacks, client-side exploits, and many other hacking methods. You will also discover how to crack wireless networks with speed, perform man-in-the-middle and DoS attacks, and use Raspberry Pi and Android to expand your assessment methodology.

By the end of this book, you will have mastered using Kali Linux for wireless security assessments and become a more effective penetration tester and consultant.

Who this book is written for
if you are an intermediate-level wireless security consultant in Kali Linux and want to be the go-to person for Kali Linux wireless security in your organization, then this is the book for you. Basic understanding of the core Kali Linux concepts is expected.

What you will learn from this book
- Fingerprint wireless networks with the various tools available in Kali Linux
- Learn various techniques to exploit wireless access points using CSRF
- Crack WPA/WPA2/WPS and crack wireless encryption using Rainbow tables even more quickly
- Perform man-in-the-middle attack on wireless clients
- Understand client-side attacks, browser exploits, Java vulnerabilities, and social engineering
- Develop advanced sniffing and PCAP analysis skills to extract sensitive information such as DOC, XLS, and PDF documents from wireless networks
- Use Raspberry Pi and OpenWrt to perform advanced wireless attacks
- Perform a DoS test using various techniques and tools
In this package, you will find:

- The author’s biography
- A preview chapter from the book, Chapter 1 'Wireless Penetration Testing Fundamentals'
- A synopsis of the book’s content
- More information on Mastering Kali Linux Wireless Pentesting
About the Authors

**Brian Sak**, CCIE #14441 (Security), is a 20-year information security veteran who currently works as a technical solutions architect for Cisco Systems. At Cisco Systems, he is engaged in solution development, and he consults with Cisco partners to help them build and improve their processes and services in the areas of big data analytics and digitization. Prior to joining Cisco Systems, Brian performed security consulting, penetration testing, and security assessment services for large financial institutions, US government agencies, and enterprises in the Fortune 500. In addition to numerous security and industry certifications, he has a bachelor's of science degree in information technology, with an emphasis on information security, and a master's of science degree in information security and assurance. He is also a contributor to The Center for Internet Security and other publications by Packt and Cisco Press.
Jilumudi Raghu Ram is a security analyst with over 5 years of experience in
the information security domain, with a strong knowledge of incident response,
digital forensics, network security, infrastructure penetration testing, and Secure
configuration audits. He has conducted security audits for more than 70 networks,
both internal and external, re-audits, secure configuration reviews, and server
audits (Linux and Windows) for various organizations. One of his major clients
has been the Government of India, where his team was responsible for conducting
penetration testing assignments for various government bodies, as well as preparing
vulnerability assessment and penetration testing reports, and supporting the clients
to fix those vulnerabilities.

Raghu Ram's areas of expertise include incident response, digital forensics, threat
research, penetration testing, vulnerability assessment, dynamic malware analysis,
intrusion detection systems, and security operations monitoring.

Raghu Ram has written various articles related to information security in the
Hindu Group magazine Frontline. He also maintains his own website dedicated
to Penetration Testing - www.wirelesspentest.com
This book demonstrates how to perform a successful wireless assessment utilizing a selection of open source tools. Readers, from beginners to seasoned professionals, will gain an understanding of the tools and techniques used to discover, crack, and exploit wireless networks as well as learn how to extract sensitive information from the wireless traffic and the clients themselves. Wireless networks are nearly always in scope as part of a comprehensive security assessment and require special consideration and a different skill set than other aspects of the assessment. You will learn the language and technologies that differentiate 802.11 networks and be introduced to the specialized applications used to test them. This book is built around gaining hands-on experience with Kali Linux, and each chapter contains many step-by-step examples on the use and mastery of the wireless assessment tools included with this distribution.

What this book covers

Chapter 1, Wireless Penetration Testing Fundamentals, introduces you to the hardware, software, and terminology associated with wireless penetration tests. It guides you through deploying Kali and verifying your wireless hardware required to conduct a successful wireless assessment.

Chapter 2, Wireless Network Scanning, covers the steps that are to be performed in order to discover, identify, and catalog wireless networks and clients that are in the scope of your penetration test.

Chapter 3, Exploiting Wireless Devices, describes weaknesses that may be present in the wireless equipment itself and tools and techniques you can use to exploit these weaknesses.
Chapter 4, *Wireless Cracking*, digs into the interception of wireless key exchanges and authentication between the clients and the infrastructure. It also shows you practical techniques to crack these various security mechanisms and expose the encrypted data transmissions.

Chapter 5, *Man-in-the Middle Attacks*, explains and demonstrates ways to extract sensitive information from the clients who are using the wireless infrastructure by enabling you to intercept their traffic and manipulate critical network resources.

Chapter 6, *Man-in-the Middle Attacks Using Evil Twin Access Points*, expands on the previous chapter by showing you techniques to set up a parallel wireless infrastructure to emulate the production network. This enables additional attacks against the clients utilizing the wireless network.

Chapter 7, *Advanced Wireless Sniffing*, covers the use of traffic captures and decryption as a means to extract sensitive information from the data that is traversing the wireless network. Tools and techniques used to collect and analyze the data are provided.

Chapter 8, *Denial of Service Attacks*, discusses the use of targeted or broad disruptions in the performance or availability of the wireless network as an element of a wireless assessment.

Chapter 9, *Wireless Pen-Testing from Non-Traditional Platforms*, expands upon the previous chapters and introduces additional hardware and software platforms that can be used during a wireless assessment, including Raspberry Pi and Android devices.
Before you begin to scan, inject, crack, sniff, spoof, and DoS (Denial of Service) wireless networks, it helps to have an understanding of the fundamentals of conducting a wireless assessment. You should have an understanding of the equipment you will need, the environment where the assessment will occur, and the basics of the regulatory standards for wireless communication. This book is a collection of practical applications that tell you how one would go about actually testing the security of wireless networks. It should be mentioned upfront that it is intended to provide some guidance for wireless security professionals and those who are looking to learn what it takes to attack and defend against wireless threats. It probably goes without saying, however, that before you proceed to try any of what you are about to learn against a production network, or any equipment you do not own, you must get written permission from the organization or individual you are providing the wireless assessment for. Unauthorized wireless cracking, traffic capture, or any other attacks that will be presented are a good way to find yourself in hot water and are not condoned or intended by the authors or the publisher of this content. This chapter will set the stage and help guide you through the basics of wireless communication, selecting the hardware that will provide you with all of the functionality required to conduct a wireless pentest, the procurement and installation of Kali Linux, the security professional's distribution of choice, and finally, validating that our configuration is sound and supports all of the tools we will be using throughout this publication.

We will cover the following topics in this chapter:

- Wireless terminology and standards
- Wireless adapters and antennas
- Kali Linux installation and configuration
- Configuration validation
Wireless communication

The term *wireless* can be construed in many different ways depending on who you are speaking to. In general, this can encompass any transmission of data using a technology where the sender and the receiver of the data are not connected by a physical medium. From an information technology context, this will cover technologies such as microwave, cellular, mobile broadband, Bluetooth, LoRa, Zigbee, and of course, Wi-Fi, or Wireless Fidelity. While some of the other areas of wireless are intriguing from a security perspective, we have chosen to keep the scope of this book down to only Wi-Fi technologies. This section will discuss the basics of Wi-Fi communications and the protocols and standards at a level appropriate for security professionals. Thankfully for us, we are able to benefit from lots of work done by our electrical engineering and software engineering counterparts, who have reduced the complexity of magically sending packets through the air at great speeds down to something manageable.

Let’s start by discussing the wireless LAN networking technology defined by the IEEE 802.11 working group. Wireless Local Area Networks, typically referred to simply as WLANs, are very popular technologies that are used to create a network of clients and devices that do not require each host to be connected to the network via a wired Ethernet connection. The biggest advantages of WLANs are their ease of use, low cost of deployment, and dynamic operational model. As mentioned, WLANs are easy to deploy, and even home users can buy an access point and start networking it with available mobile devices, such as laptops, smartphones, and tablets, with little skill and in a short amount of time. It’s typically just a matter of plugging in the access point and correctly configuring your mobile devices, and the WLAN will be operational within a few minutes. For WLANs in a corporate environment, many of the same principles apply, though the complexity and security considerations will typically increase linearly to the size of the deployment. Organizations typically have many access points and configurations to manage, and it’s common to see them deployed, leveraging a controller model to ensure consistency. While this model varies from what you will typically see in a residential or SMB scenario, the underlying technologies (and weaknesses) still exist. To better understand the security risks associated with WLANs, we need to know how wireless stations and clients communicate and the underlying technologies that enable this communication.

Some WLAN components are as follows:

- **Radio**: This is defined as a *station* in 802.11 standards, and it will sometimes be abbreviated as STA. It is the component that transmits the wireless signal.

- **Access Points (AP)**: This provides connectivity between STAs (most likely, laptops and other mobile devices).
The preceding components alone provide the hardware required to build a WLAN. From a software perspective, wireless drivers and firmware on access points enable this hardware, and an operating system and an application stack will provide the management, user control, encryption, and other functionalities.

As we look at the security considerations for each part of the stack that enables wireless connectivity, we have to ensure that all components are scrutinized. It is possible that vulnerabilities in something as fundamental as device drivers may lead to the compromise of the AP or client. Additionally, firmware in an access point can potentially be infected with malware, which can lead to the compromise of the clients that are connected to them. If you are a security professional reading this book, to be better informed and better understand how to test and protect a wireless network you are responsible for, subsequent chapters will provide you with some guidance on known vulnerabilities, what to look out for, and operational best practices in addition to the demonstrated penetration testing exercises.

**Wireless standards**

The Wi-Fi Alliance ([www.wi-fi.org](http://www.wi-fi.org)) is an organization that supports and certifies wireless technologies to ensure interoperability between vendors, and it has been instrumental in bringing Wi-Fi to homes and businesses around the world. Early implementations of wireless technologies for network communications were hampered by interoperability issues and conflicting implementations because the IEEE did not have the testing equipment to ensure compliance with its standards. This led to the creation of the Wireless Ethernet Compatibility Alliance, or WECA, who were promoting a new higher speed standard for wireless communication, which ultimately became 802.11b. WECA was rebranded in 2002 as the Wi-Fi Alliance continues to validate and certify wireless technologies until this day in order to ensure interoperability and promote standards in the industry. Today, wireless networking technologies used to implement WLANs (Wireless Local Area Networks) are organized under the IEEE 802.11 specifications. They are an alphabet soup of protocols that define the frequencies, transmission rates, bandwidth, and modulation of the wireless communications. The following is a list of the protocols we will be focusing on in this book and those that are the most relevant to wireless security professionals:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Frequency</th>
<th>Bandwidth</th>
<th>Maximum data rate</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>2.4 GHz</td>
<td>22 MHz</td>
<td>11 Mbps</td>
<td>DSSS</td>
</tr>
<tr>
<td>802.11a</td>
<td>5 GHz</td>
<td>20 MHz</td>
<td>54 Mbps</td>
<td>OFDM</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4 GHz</td>
<td>20 MHz</td>
<td>54 Mbps</td>
<td>OFDM</td>
</tr>
</tbody>
</table>
In the preceding table, DSSS indicates Direct-Sequence Spread Spectrum, and OFDM is Orthogonal Frequency-Division Multiplexing. These technologies refer to how the radio allocates the bandwidth to transmit the data over the air. Again, a big thanks to wireless engineers for incorporating this complexity into a standard so that we don't necessarily need to know exactly how this works in order to send and receive packets wirelessly.

As we get into wirelessly capturing packets from the air, the concept of channels will come into play. The term channel refers to a specific frequency within either the 2.4 GHz or 5 GHz frequency spectrum that the wireless radios on the access point and the client have either negotiated or been told to use for the communication of the data between them. This is similar to the channel on your television set—think analog here—where the station transmits at a specific frequency and the television is configured to receive that specific frequency by you tuning it to a specific channel. If both sides are configured to talk on the same channel, then the communication between the two devices can proceed. A side note: there is an entirely tangential discussion we could launch into here about the channel selection, co-channel interference, and channel design, but for the purposes of this discussion, we will focus on the channels available in each range and the frequency on which they run. This is explained in detail in the next section.

### The 2.4 GHz spectrum

The 2.4 GHz spectrum is commonly used for wireless deployments due to its range and support for many common Wi-Fi protocols, such as 802.11b, g, and n. You will typically find it used either exclusively in your target network or as a co-resident with the 5 GHz spectrum in dual-mode access points. The following table lists the channels and associated frequencies that you will encounter when you conduct your wireless penetration test. We will be using these channel numbers in the subsequent chapters as we set up our captures and define channels for our virtual access points.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
</tr>
</tbody>
</table>
In North America, only channels 1-11 are used, while in most of the world, 1-13 are used. Channel 14 is only used in Japan under the 802.11b protocol. These same channels apply whether your wireless interface is using 802.11b, 802.11g, or 802.11n. In the next chapter, when we look at wireless scanning, you will be able to see which channel the access point and client are communicating on using the airmon-ng application. You will then proceed to specifically select one of these channels when we want to capture the traffic being sent between the wireless devices.

The 5 GHz spectrum
The 5 GHz spectrum is massive and varies widely in its implementation depending on which part of the world it is operating in. Fundamentally, it ranges between Channel 36 at 5180 MHz and Channel 165 at 5825 MHz; however, some parts of the world use frequencies ranging down to 4915 MHz, and channels range from 7 to 196. The most common channels and frequencies are represented in the following table. However, you should reference the standards that are in use in your geography before conducting a wireless security assessment as the range might be expanded in your area.
The same principles come into play when you are capturing the traffic from the 802.11a or 802.11n networks running at 5 GHz, as they do at 2.4 GHz. The tools provided by Kali will let you specify the frequency your wireless adapter is listening on by the associated channel number. You will identify the channel that the client and access point are communicating over and then set up your capture accordingly.

**Choosing the right equipment**

Though you may be eager to grab a laptop, install Kali on it, and jump right into running the tools, you'd be best served to spend some time researching and validating the devices you plan to use. It can be very frustrating to begin working through the tutorials and exercises in this book only to be thwarted by hardware that is not working right or doesn't support all of the features required to complete your assessment. This section will discuss wireless adapters, antennas, and other considerations that provide you the best chance of success.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>5300</td>
</tr>
<tr>
<td>64</td>
<td>5320</td>
</tr>
<tr>
<td>100</td>
<td>5500</td>
</tr>
<tr>
<td>104</td>
<td>5520</td>
</tr>
<tr>
<td>108</td>
<td>5540</td>
</tr>
<tr>
<td>112</td>
<td>5560</td>
</tr>
<tr>
<td>116</td>
<td>5580</td>
</tr>
<tr>
<td>132</td>
<td>5660</td>
</tr>
<tr>
<td>136</td>
<td>5680</td>
</tr>
<tr>
<td>140</td>
<td>5700</td>
</tr>
<tr>
<td>149</td>
<td>5745</td>
</tr>
<tr>
<td>153</td>
<td>5765</td>
</tr>
<tr>
<td>157</td>
<td>5785</td>
</tr>
<tr>
<td>161</td>
<td>5805</td>
</tr>
<tr>
<td>165</td>
<td>5825</td>
</tr>
</tbody>
</table>
Supported wireless modes

In this book, we will extensively make use of the advanced features of the wireless client that are not supported on all adapters. Two of these features, monitor and master modes, will help us capture the traffic and set up virtual access points, respectively. In the monitor mode, you are able to put your wireless adapter in a promiscuous (or listening) mode, which is capable of capturing the wireless frames from the air, while the master mode is essential for the setting up of an evil twin attack. These two modes are just some of the several supported modes in various wireless adapters, and the following are the commonly available modes and they explain what they are used for:

- **The managed mode**: This is the default mode for most wireless connections. In this mode, the wireless adapter is only capable of receiving packets from SSIDs that it is associated with. For instance, if the adapter is associated with a "packt" SSID, then it filters out packets from the other SSIDs. This is the common operating mode for clients who are actively associated with an access point and assigned an IP address and who carry on regular communications with their intended wireless network.

- **The ad-hoc mode**: This mode is rarely used since the majority of wireless networks participate in infrastructure mode and host clients directly. This mode is used only when an access point is not in place and clients are participating in a peer-to-peer mesh. The lack of an access point usually restricts the functionality and usefulness of the connecting clients and hence is rarely used in modern deployments.

- **The master mode**: This mode allows us to configure our wireless client as a base station or a wireless access point. In most production networks, clients are clients and access points are access points. This seems funny to say, but as a penetration tester, it is common for us to want to emulate an access point where we control the configuration and, more importantly, have visibility about all of the traffic traversing the wireless device. This mode is required if you intend to set up a virtual access point as part of your assessment.

- **The monitor mode**: The support for this mode is essential if you want to be able to capture all the traffic on the wireless spectrum. With the monitor mode, the wireless adapter is placed into a passive state, where it does not attempt to interact with any of the wireless devices around it. Instead, it enables us to sniff and capture the traffic for analysis, cracking, or decryption.
As mentioned, not all devices support all four of the preceding modes, notably missing either the monitor mode or the master mode. These two modes are important to many of the provided examples, and it might not be immediately clear that your chosen adapter does not support them. Next, we will discuss adapters that have been known to be successful in penetration tests, specifically with Kali Linux.

**Wireless adapters**

The first thing you'll look for when selecting a wireless adapter is the chipset used in the adapter. Many adapters may have different vendors and names printed on the outside of the device but use the same chipsets underneath the plastic where it really matters. The chipsets that have been known to be compatible are discussed in the upcoming sections.

**Ralink RT3070**

This chipset is used in many different USB wireless adapters that are available in different form factors.

The following are examples of several common adapters at the time of writing this book. There are hundred more adapters that also use this chipset, which comes in a variety of sizes and hardware configurations.

This model is **ALFA AWUS036NH** (image courtesy: [http://www.alfa.com.tw](http://www.alfa.com.tw))

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>USB 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Protocols</td>
<td>802.11 b/g/n</td>
</tr>
<tr>
<td>Band</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Speed</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>Gain</td>
<td>2000 mW</td>
</tr>
</tbody>
</table>
This model is **ALFA AWUS036NEH** (image courtesy: http://www.alfa.com.tw)

![ALFA AWUS036NEH](image.png)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>USB 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Protocols</td>
<td>802.11 b/g/n</td>
</tr>
<tr>
<td>Band</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Speed</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>Gain</td>
<td>1000 mW</td>
</tr>
</tbody>
</table>

This model is **Tenda UH151** (image courtesy: http://www.tendacn.com)

![Tenda UH151](image.png)
### Atheros AR9271

Similar to the RT3070, this chipset also supports 2.4 GHz and is used by several vendors, including ALFA, TP-LINK, D-Link, and others. You will find these adapters regularly recommended by pentesters on Kali and aircrack-ng forums. Here are a few adapters shown along with their specifications.

This model is **ALFA AWUS036NHA** (image courtesy: http://www.alfa.com.tw)

![ALFA AWUS036NHA](http://www.alfa.com.tw)
This model is **ALFA AWUS036NH** (image courtesy: [http://www.alfa.com.tw](http://www.alfa.com.tw))

![ALFA AWUS036NH](image)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Type</td>
<td>USB 2.0</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>802.1 b/g/n</td>
</tr>
<tr>
<td>Band</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Speed</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>Gain</td>
<td>2000 mW</td>
</tr>
</tbody>
</table>

**Ralink RT3572**

This is the newer Ralink chipset, that has been found to be very compatible with Kali Linux, and it supports the modes that we are interested in. This chipset is capable of both 2.4 GHz and 5.0 GHz, making it very attractive for pentesters. A common example that uses this chipset is as follows:
This model is **ALFA AWUS051NH** (image courtesy: [http://www.alfa.com.tw](http://www.alfa.com.tw))

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>USB 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Protocols</td>
<td>802.11 a/b/g/n</td>
</tr>
<tr>
<td>Band</td>
<td>2.4 GHz and 5 GHz</td>
</tr>
<tr>
<td>Speed</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>Gain</td>
<td>500 mW</td>
</tr>
</tbody>
</table>

You will notice that all of the wireless adapters that we recommend in this section have several things in common. First, they all utilize a USB connection rather than being embedded in the device. This is advantageous for a number of reasons. Embedded wireless devices, such as those that ship with your laptop, may have limited advanced functionality support due to driver and firmware limitations. Most pentesters will also use USB devices because of their portability. The USB wireless adapter can easily be disconnected from your primary penetration testing device and be moved to an alternate platform. We will be covering some of these platforms in the last chapter of the book. USB devices can also be easily mapped through to a virtual machine running on top of their existing operating system. This will be demonstrated later, when we cover the installation of Kali Linux on a VM running in Virtual Box.

Another common trait of these adapters is that they all support an external antenna connected to their radio. On the ALFA USB adapters, the antenna is connected via an RP-SMA, or a Reverse Polarity SubMiniature Version A screw-on connection. This is a very common connection for antennas, and it allows you to select an antenna to fit the situation and environment where you are operating. The antenna types vary in their construction and design to optimize either the gain or focus their radio signals in a particular direction, increasing the distance in which they can transmit and receive. The next section will cover several antenna types and detail when each could be used during your wireless assessment.
Antennas

Having the ability to replace the antenna on your wireless adapter, while penetration testing provides you some flexibility on how you conduct your wireless assessment. When testing the target environment, you must be within the RF range of the target network in order to do the majority of your testing. This limits how far away you can be from the physical location where the wireless is being utilized and, sometimes, your ability to be inconspicuous while conducting the testing. Increasing the gain and focusing the power of your wireless adapter may allow you to set up camp in a place that is a little more covert while still being able to see the target network. In this section, we will look at three common antenna choices that can be affixed to the wireless adapters mentioned earlier. Each has their own unique advantages and drawbacks.

Omnidirectional antennas

Omnidirectional antenna, as the name implies, sends and receives wireless traffic in all directions around the circumference of the antenna. The amount of gain provided by these antennas varies between 5 dBi and 14 dBi. This is a great general-purpose antenna and will typically ship with an adapter that allows an external antenna. These antennas can be designed for 2.4 GHz, 5.0 GHz, or both, so ensure what band you will be utilizing and select the antenna that supports it.
Patch antennas

Patch antennas allow you to focus the signal of your wireless interface in a particular direction that can improve the accuracy and range of the transmission over a long distance. The radiation pattern of the antenna only extends from one face of the patch antenna and typically has gains in the 7 dBi to 10 dBi range. This antenna will be beneficial if all of the devices you were testing or capturing from were located in the same direction from your testing location.

![Patch Antenna Image](http://www.alfa.com.tw)

Yagi antennas

Yagi antennas are highly directional antennas, similar to patch antennas. They tend to be capable of even higher gains than the other two discussed antenna types since their radiation pattern is very focused in a particular direction. It is common to find these types of antennas with 18 dBi or higher gains, which allow you to be further away from the target wireless network you are testing if your directional aim with the antenna is true.

![Yagi Antenna Image](http://www.alfa.com.tw)
Kali Linux for the wireless pentester

The operating environment that we will use throughout this book is Kali Linux version 2.0. This is a Debian-based distribution that has been purpose-built for the security professional. It is preloaded with many of the applications that are commonly used during a penetration test and also includes a set of drivers that enable the advanced functionality of wireless adapters. The process of finding, patching, and compiling wireless drivers on generic Linux platforms to support the monitor mode, injection, and deauthentication can be very cumbersome if you choose to venture out on your own. However, Kali has precompiled drivers for the wireless adapters we discussed in the previous section and others that have been tested to ensure that the adapters will work in a plug-and-play fashion.

In the next section, we will show how to download and install Kali for use during our penetration test as a Virtual Box image. The benefits of utilizing a virtual image for Kali are that it can run as a co-resident with your other operating system and applications, but in a protected environment, this can be dedicated to your penetration testing environment.

Downloading Virtual Box

In this example, we will be downloading the components required to run Kali Linux in VirtualBox, a virtual machine environment that can run on top of Windows, Mac OS X, Linux, or Solaris hosts. It is available from https://virtualbox.org as an Open Source Software package distributed under GPL (GNU General Public Licensing).

Browse to https://virtualbox.org and pull down the distribution for the host operating system you will be running it on.

VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- VirtualBox platform packages. The binaries are released under the terms of the GPL version 2.
  - VirtualBox 5.0.10 for Windows hosts
  - VirtualBox 5.0.10 for OS X hosts
  - VirtualBox 5.0.10 for Linux hosts
  - VirtualBox 5.0.10 for Solaris hosts
Installing Virtual Box

Run through the installation wizard for your operating system, typically accepting the defaults when prompted. Any configuration changes will be noted as we install Kali into the virtual environment and map the local host resources to the virtual environment.

After VirtualBox is installed, you will need to download Kali 2.0 from https://kali.org.

Kali Linux deployment

Kali Linux is distributed in a number of different formats for various operating environments and devices. For our VirtualBox deployment, you can either choose to download the .ISO file and build your virtual machine as you would for other operating systems, or you can use a prepackaged distribution that is specific to VirtualBox. In this example, we will be choosing the route that enables us to get started sooner with our pentest, which is the prebuilt image. Follow these steps:

1. Browse to http://www.offensive-security.com/kali-linux-vmware-arm-image-download/ and look for the prepackaged VirtualBox images. You should see something like what is shown in the following screenshot:
Chapter 1

Download Kali Linux VMware and VirtualBox images

Want to download Kali Linux custom images? We have generated several Kali Linux VMware, VirtualBox and ARM images which we would like to share with the community. Note that the images provided below are maintained on a “best effort” basis and all future updates will be listed on this page. Furthermore, Offensive Security does not provide technical support for our contributed Kali Linux images. Support for Kali can be obtained via various methods listed on the Kali Linux Community page. These images have a default password of “toor” and may have pre-generated SSH host keys.

<table>
<thead>
<tr>
<th>Prebuilt Kali Linux VMware Images</th>
<th>Prebuilt Kali Linux VirtualBox Images</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Name</strong></td>
<td><strong>Torrent</strong></td>
</tr>
<tr>
<td>Kali Linux 64 bit VBox</td>
<td>Torrent</td>
</tr>
<tr>
<td>Kali Linux 32 bit VBox PAE</td>
<td>Torrent</td>
</tr>
<tr>
<td>Kali Linux 32 bit</td>
<td>N/A</td>
</tr>
</tbody>
</table>

There are two 32-bit images available and one 64-bit image. Of the two 32-bit images, the one denoted as **Kali Linux 32-bit VBox PAE** designates that this version is running a kernel with the **Physical Address Extension** memory enhancement enabled, which can allow the 32-bit architecture to reference physical memory quantities greater than 4 GB. Either of these will work for all of the exercises in this book.

2. Download the image for your architecture and uncompress it to a folder. The resulting image will have a `.ova` extension.

3. We will now import the new image into VirtualBox. Navigate to **File | Import Appliance**... from the VirtualBox application.
4. Choose the \texttt{.ova} file that you extracted and choose \textbf{Continue}.

Since we're importing from an \texttt{.ova} file, the software developer has chosen the configuration that is optimal for the running of the virtual machine and the applications that run on top of it. This saves us the headache of trying to determine the virtual resources and the settings we will need to configure in order to successfully install and run the distribution.
Once deployed, this image will require a minimum of 10 GB of disk space and 2 GB of physical memory dedicated to running the virtual machine. The Kali 2.0 image is deployed with a thin virtual disk that is actually configured for 30 GB; however, it will only use the amount of disk space that it has allocated. This deployment, after successful import, was around 8 GB of the used space.

5. Click on **Import** and wait for the virtual image to be deployed:
6. Now, you can start your newly deployed VirtualBox image by right-clicking on the image and navigating to **Start | Normal Start**, as shown in the following screenshot:

![VirtualBox Start Menu Screenshot]

7. Choose the default selection, **Kali GNU/Linux**, from the GRUB launcher:

![GRUB Launcher Screenshot]

(use the ↑ and ↓ keys to select which entry is highlighted. Press enter to boot the selected OS. ‘c’ to edit the commands before booting or ‘e’ for a command-line.)
8. The default username and password for the new Kali instance should be root and toor, respectively.

That concludes the deployment of the virtual machine into VirtualBox!

It is recommended that you update the apt repository and install updates to the distribution using the following commands:

```
# apt-get update
# apt-get upgrade
```
You should see the following as a result:

Mapping the wireless adapter into Kali

If you have chosen to use an external USB wireless adapter, you will need to get the device mapped through into the Kali virtual machine in order to allow you to use it. This is done through the VirtualBox menu by navigating to Devices | USB and then identifying the USB device that corresponds to your WiFi adapter:
This simulates the plugging of the USB adapter directly into the operating system, and you will now be able to access it directly from Kali using either the command line or GUI tools. To begin validating that your wireless adapter is properly identified by Kali and supports all of the modes you will be using during your assessment, open up a terminal window and run the following commands:

```
# lsusb
# iwconfig
```

You should be able to see the following screen as a result:

![Terminal Output]

Let's understand what the earlier two commands are used for:

- **lsusb**: This lists the devices that are connected to the USB bus. Here, you should be able to identify whether your wireless adapter is seen by the operating system, and if so, include a short description of the device. You should be able to identify the chipset that is present in the adapter; in this example, it is using the Ralink 3070 chipset.

- **iwconfig**: This is used to set and view the parameters of the wireless interfaces seen by the operating system. Here, you are able to bring the interfaces up and down and see which mode the interface is operating in. It is important to make note of the virtual interface that is assigned to this device as it will be used in nearly all of the exercises. Typically, this is wlan0, but it can also be wlan1, wlan2, and so on if you have more than one wireless adapter in the system.
Next, you will need to verify that all of the modes are supported by the hardware and drivers of your wireless adapter. This can be accomplished using the `iw` command in Kali:

```
#iw phy phy1 info
```

The `iw` command is used to show or manipulate wireless devices and their configurations. The `phy` option tells the command to select the interface by its physical address. This is followed by the physical device identifier, `phy1` in this example. The trailing `info` command tells `iw` to print out all of the details associated with this particular wireless adapter.

A lot of information is returned by this command, so you may have to scroll back up through the list to identify which interface modes are supported by this wireless adapter. At the minimum, you should see managed and mesh, but the ones we are most interested in are AP and monitor. These correspond to master and monitor, the two modes that will be required to execute all of the procedures that will follow.
Depending on which part of the world you are in, you may encounter wireless networks operating on different frequencies across different channels. It is a good idea to validate that your wireless adapter is capable of scanning across all of these frequencies so that wireless networks are not missed during your penetration test. This can be accomplished by running `iwlist`:

```
#iwlist wlan0 channel
```

![iwlist output example](image)

The `iwlist` command provides detailed information about the capabilities of the wireless adapter. This command allows you to enumerate many details about your wireless device, including encryption capabilities, transmission rate, keys in use, and power levels. The earlier option, channels, displays the available channels and the frequencies available to this wireless adapter. This example shows a 2.4 GHz adapter capable of operating across 14 channels.
Summary

Make sure you do a little prework upfront before starting your wireless penetration testing as it will save you a significant amount of frustration later on. In this chapter, we discussed the hardware and software that will be required to successfully conduct a wireless penetration test. Choosing the right wireless adapter is critical as not all of the required features are supported in all devices. As you work through the various scenarios presented to you during your test, it may be necessary to utilize different external antennas connected to your wireless adapter, and each of these was discussed in turn. From a software perspective, Kali Linux provides an excellent framework on which to build your wireless testing toolset. Driver support is solid and many security assessment tools are already preconfigured and tested using this distribution. Lastly, once the hardware and software are configured, you’ll want to validate the capabilities of your wireless adapter to ensure it is fully supported by the operating system.

With these steps completed, you are ready to proceed to the remaining chapters in the book to identify, exploit, sniff, and manipulate the target wireless networks.
Where to buy this book

You can buy Mastering Kali Linux Wireless Pentesting from the Packt Publishing website.

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

Click here for ordering and shipping details.