CHAPTER

Meet the deck 1

INFORMATION IN THIS CHAPTER:

- The Deck—a custom Linux distribution
- Small computer boards running Linux
- Standard penetration testing tools
- Penetration testing desktops
- Dropboxes—attacking from within
- Drones—attacking from a distance with multiple devices

INTRODUCTION

We live in an increasingly digital world. The number of interconnected devices in our world is constantly on the rise. Businesses worldwide rely on computers, tablets, smartphones, and other digital devices in order to compete in a global economy. Many businesses are necessarily connected to the Internet. Newly connected systems can come under attack by malicious persons and/or organizations in a matter of minutes. Because of this, the demand for information security (infosec) professionals is strong. Penetration testers (pentesters) are some of the most sought after infosec people.

Chances are that if you are reading this book, you already know what penetration testing entails. Penetration testing (pentesting) is authorized hacking performed at the request of a client in order to ascertain how easily their digital security may be penetrated and steps that should be taken to improve their security posture. The need for penetration testing has led to the creation of a number of specialized Linux distributions. Up until now, these custom Linux distributions have been created almost exclusively to be run by a single penetration tester using an Intel-based (or AMD-based) desktop or laptop computer.

FEAR NOT

Before getting started with the main topic of this chapter, I wanted to provide you with some assurances up front. This book is written under the assumption that you have an understanding of general penetration testing concepts and basic Linux usage. Everything else you need to know will be provided in this book. You need not be an elite hacker (but if you are, then good for you!) or advanced Linux user/administrator to get something out of this book. Most importantly, absolutely

no hardware knowledge is assumed. While information will be provided for those wishing to create their own custom circuit boards and such, most of what is described in this book is also commercially available.

If you are new to the idea of hardware hacking, you can choose the level to which you want to push yourself. You can simply play it safe and buy commercially available BeagleBone capes (expansion boards that plug into the BeagleBone directly; see http://beagleboard.org/cape for more information). If you want to get your feet wet, you might solder four wires to a commercially available XBee adapter (such as this Adafruit adapter (http://www.adafruit.com/products/126)) to create a mini-cape as described later in this book. Information is provided for advanced users who want to etch their own custom circuit boards. You can do as little or as much hardware hacking as you wish without affecting your ability to perform powerful penetration tests as described in this book.

THE DECK

The Deck, the custom Linux distribution described in this book, breaks the traditional model by providing penetration testers with an operating system that runs on low-power ARM-based systems developed by the nonprofit BeagleBoard.org Foundation (these will be described more fully in the next chapter, but see http://beagleboard.org/Getting%20Started if you just cannot wait till then). This permits devices running The Deck to be easily hidden and opens up the possibility of running off of battery power. At the time of this writing, The Deck contained over 1600 packages, making it extremely useful for penetration testing. The Deck is extremely flexible and is equally adept at being used as a traditional desktop, dropbox, or remote hacking drone.

WHAT'S IN A NAME?

The Deck

If you are a reader of science fiction, you may already have a suspicion where the name The Deck comes from. The Deck can refer to the custom Linux distribution described in this book or to a device running The Deck operating system. In the 1984 science fiction classic *Neuromancer* by William Gibson, cyber-cowboys using computer terminals attached to the Internet are said to "punch deck." Gibson described a future where advanced devices (decks) are used to access the Internet. In my mind, the Beagles and similar small, low-power, inexpensive devices represent the future of penetration testing. Naming the system The Deck is a tribute to Gibson. Additionally, the BeagleBone is roughly the size of a deck of cards.

DEVICES RUNNING THE DECK

All of the devices shown in Figure 1.1 are running The Deck. At the time of this writing, The Deck runs on three devices in the Beagle family: the BeagleBoard-xM, BeagleBone, and BeagleBone Black edition. These boards will be described

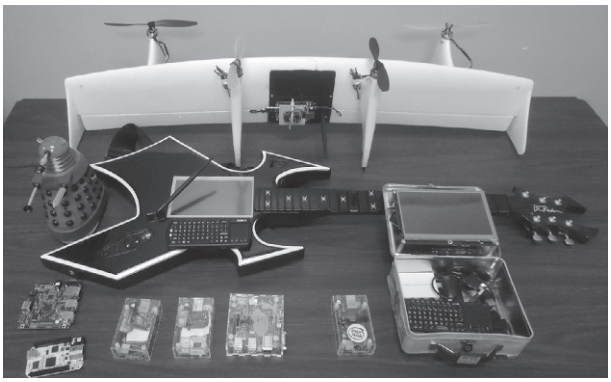

FIGURE 1.1

Collection of devices running The Deck.

more fully in the next chapter. You can also find out more about them at the BeagleBoard Web site (http://beagleboard.org). For now, we will describe them as low-power boards based on ARM Cortex-A8 processors running at up to 1 GHz. Despite providing desktop-like performance, these devices require a fraction of the power of an Intel-based or AMD-based system. Even when driving a 7 in. touchscreen (such as this one: http://elinux.org/Beagleboard:BeagleBone_LCD7) and external wireless adapter, a 10 W (2 A at 5 V) power adapter is more than sufficient. Compare this with triple- and quadruple-digit wattages found in laptop and desktop systems.

PENETRATION TESTING TOOLS

The Deck contains a large number of penetration testing tools. The intention is to have every tool you would likely need available without the trouble of downloading additional packages. Installing new packages to a hacking drone during a penetration test ranges from difficult to impossible. Some desktop-oriented penetration testing Linux distributions suffer from having many old packages that are no longer in common use. Each package included in The Deck was evaluated before inclusion. Anything deemed redundant to a new package was left out. Some of the more frequently used tools are introduced here.

Wireless networking has become extremely prevalent. As a result, many penetration tests start with the need to crack a wireless network. The aircrack-ng suite is included in The Deck for this purpose. The airodump-ng utility is used for basic packet captures and analysis. Captured packets can then be fed to aircrack-ng in order to crack network encryption. Screenshots of airodump-ng and aircrack-ng are provided in Figures 1.2 and 1.3, respectively. More details on using the aircrack-ng suite will be provided in future chapters.

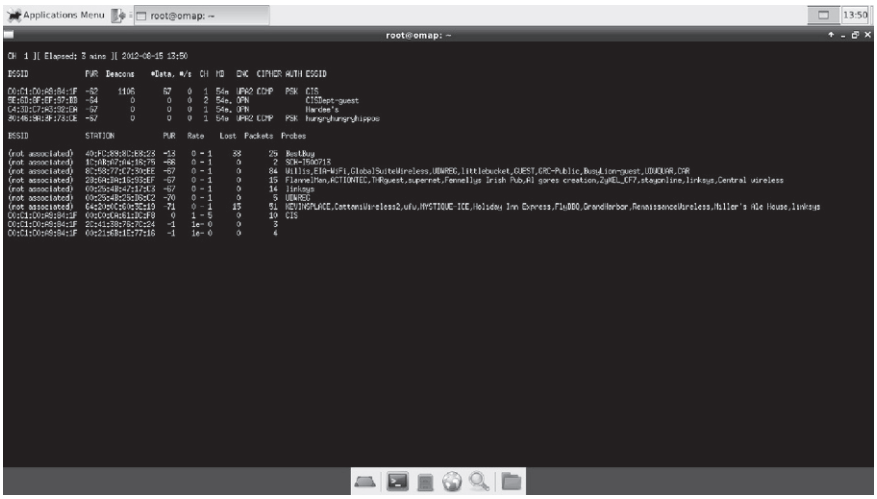

FIGURE 1.2

Using airodump-ng to capture and summarize wireless packets.

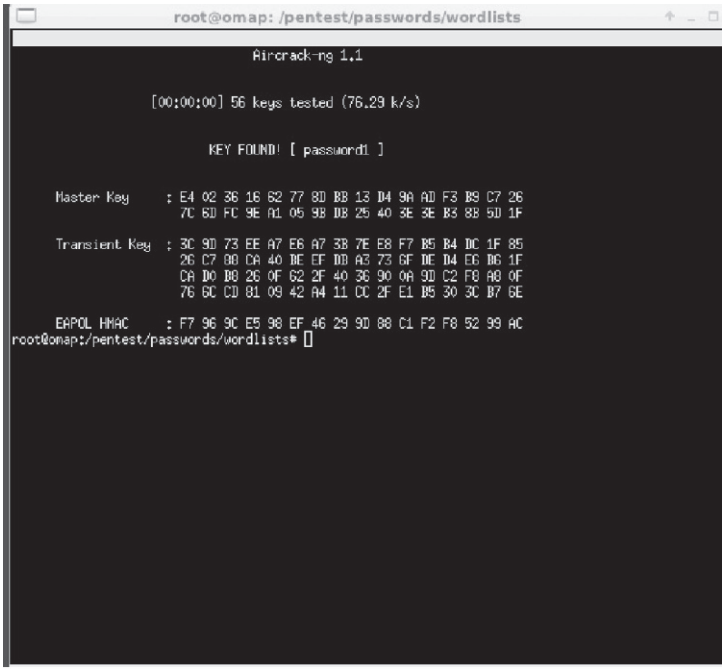

FIGURE 1.3

A successful crack with aircrack-ng.

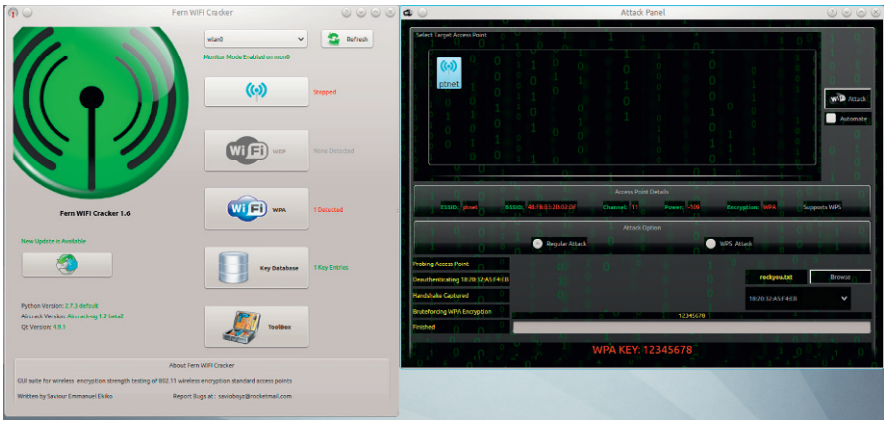

FIGURE 1.4

Fern WiFi Cracker.

Even in cases where a client is not using wireless networking, the aircrack-ng suite can be useful for detecting and possibly cracking any rogue access points on the client's network. A very easy to use point-and-click wireless cracking tool known as Fern WiFi Cracker is also included with The Deck. A screenshot showing a successful crack with Fern is shown in Figure 1.4. Those newer to penetration testing might find Fern easier to use. Due to their interactive nature, neither aircrack-ng nor Fern is suitable for use in a hacking drone. For this reason, the Scapy Python tool (http://www.secdev.org/projects/scapy/) is included in The Deck.

Regardless of whether they are from wired or wireless networks, network packets are potentially interesting to the penetration tester. The Deck includes Wireshark (http://www.wireshark.org/) for capturing and analyzing captured packets. Nmap (http://nmap.org/), a standard network mapping tool, is also provided for identifying services and hosts on a target network. A collection of vulnerability scanners and a powerful exploitation framework known as Metasploit (http://www.metasploit.com/) are also bundled in the standard version of The Deck. Some of these tools are presented in Figure 1.5.

Metasploit is a very popular tool maintained by Rapid 7 (http://www.rapid7.com/). Numerous books, training classes, and videos covering Metasploit have been created. Offensive Security has published an online book Metasploit Unleashed (http://www.offensive-security.com/metasploit-unleashed/Main_Page), which is freely available (although a donation to Hackers for Charity is encouraged). Metasploit is billed as a framework and features a large number of vulnerabilities, which may be exploited to deliver one of several hundred available payloads. Metasploit may be run in scripts, as an interactive console, or with a Web interface. Complete coverage of Metasploit is well beyond the scope of this book. Readers who are unfamiliar with Metasploit are encouraged to learn more about this amazing tool.

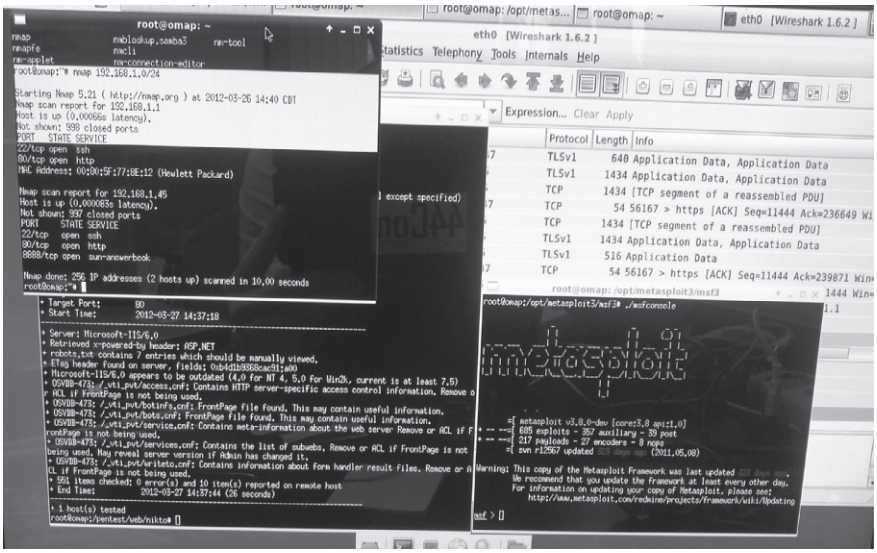

FIGURE 1.5

Wireshark, Nmap, Nikto, and Metasploit.

Cracking user passwords is frequently a component in penetration tests. The Deck includes a collection of online password crackers, offline password crackers, and password lists. One of the online cracking tools, Hydra (https://www.thc.org/thc-hydra/) is presented in Figure 1.6. Numerous additional tools are included in The Deck, not the least of which is a collection of Python libraries. Some of these packages will be highlighted in case studies later in this book.

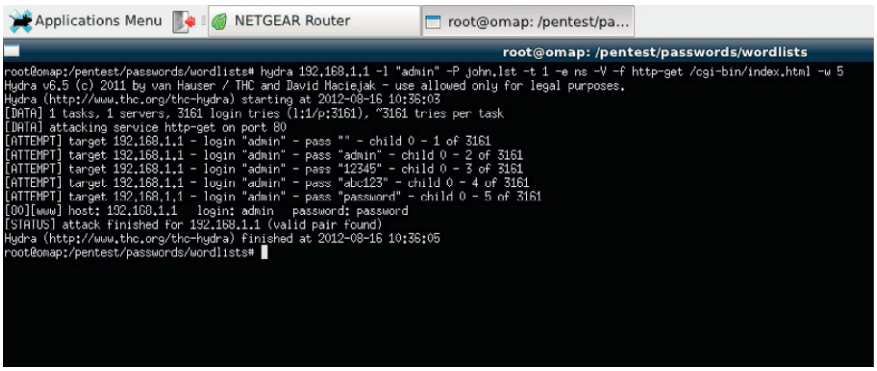

FIGURE 1.6

Hydra online password cracker.

MODES OF OPERATION

One of the strengths of The Deck is that a device running The Deck is capable of operating as a traditional graphical user interface (GUI) desktop system, dropbox, or hacking drone. No software changes are required to switch between modes of operation. This adds a great deal of flexibility to a penetration test. You can literally show up at a penetration test with a dozen devices running The Deck and select power and other options (such as wireless adapters and 802.15.4 modems) on the spot. No need to bring separate devices for use as penetration testing workstations, dropboxes, and drones, some of which might never be used in the engagement.

The Deck as a desktop system

The Deck debuted at the 44CON security conference in London in September 2012. It originally ran only on the BeagleBoard-xM. Two configurations were demonstrated. The first configuration was a desktop system with external monitor, keyboard, and mouse. A portable system with a 7 in. touchscreen and compact presenter keyboard/mouse was also presented. At 44CON, I made the statement that these devices could easily fit in a child's lunchbox. When I saw a Buzz Lightyear lunchbox on sale after returning home, the penetration testing lunchbox was born. Buzz Lightyear was chosen because using this lunchbox, you can hack someone to infinity and beyond. Both of these devices are shown in Figure 1.7.

Several desktop configurations of The Deck have been created since its debut in September 2012. A system with a 7 in. touchscreen, Alfa wireless adapter (the whammy bar was replaced with a 5 dB antenna), and RFID reader was installed inside a video game guitar. This system, dubbed the haxtar, looks like a toy and is easily dismissed as nonthreatening. In reality, this is a powerful portable penetration testing

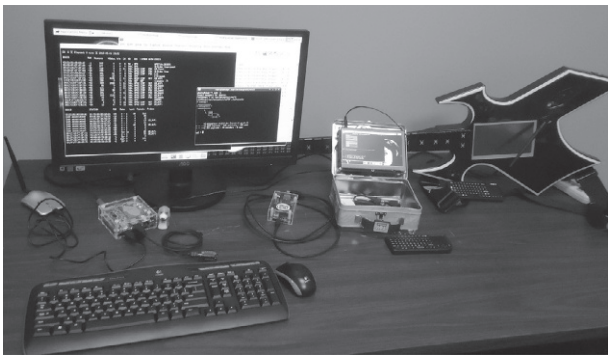

FIGURE 1.7

Desktops running The Deck. From the left, a BeagleBoard-xM with external monitor, keyboard, and mouse; a BeagleBone Black with HDMI cable for a television or digital monitor; a BeagleBoard-xM with a 7 in. touchscreen and wireless keyboard/mouse installed in a Buzz Lightyear lunchbox; and a BeagleBoard-xM with 7 in. touchscreen, wireless keyboard/mouse, and RFID reader installed inside a video game guitar.

system that even has a strap so you can use it while standing. A wireless presenter keyboard/mouse combination is used for input. There is enough free space inside the haxtar to add 802.15.4 and Bluetooth as well. The haxtar appears in Figure 1.7.

In April 2013, the BeagleBoard organization released a new board, the BeagleBone Black edition (BBB). This new system has approximately the same processing power as the BeagleBoard-xM (BB-xM) at less than a third of the price. Unlike the original BeagleBone, the BeagleBone Black featured HDMI output making it suitable for use as a desktop system. Like the BeagleBoard-xM, both versions of the BeagleBone can be directly connected to a touchscreen. The original BeagleBone is not recommended for use as a desktop as it is not as powerful as the BeagleBoard-xM or BeagleBone Black. A desktop system based on the BeagleBone Black is shown in Figure 1.7.

SERENDIPITY

From whence cometh The Deck

I have been asked on multiple occasions where the idea for The Deck originated. Prior to developing The Deck, I had done considerable work in the field of USB mass storage forensics. In conjunction with this work, I had the privilege of presenting a microcontroller-based pocket USB mass storage forensic duplicator at the very first 44CON in London in September 2011. One of the limitations of the microcontrollers I was using was that they did not support high-speed USB. This meant that the devices I developed were perfectly fine for duplicating USB flash drives, but much too slow to be used for larger storage media such as external hard drives. I wanted to recreate my USB forensics work with support for high-speed USB.

As luck would have it, I exhibited several of my microcontroller-based devices at Maker Faire Detroit in summer 2011. I just happened to have a booth right next to Jason Kridner from the BeagleBoard organization. The BeagleBoard-xM had been recently released and Jason was doing some impressive demonstrations over the two days of the show. I had never heard of the BeagleBoard before, but immediately saw lots of potential in this little board. I filed the BeagleBoard away in the back of my mind as something to use for a future projects.

When I decided to extend my USB work to support high-speed USB, the BeagleBoard-xM was a natural choice. As I started working with the BeagleBoard-xM, I quickly realized that to use the board solely for creating a forensic duplicator would be a real waste of some nice hardware. I decided to create a penetration testing device. Before I knew it, I found myself creating my own Linux distribution. I became so engrossed in creating a device for penetration testing that I almost forgot about the forensics functionality. The forensic functionality is provided in a module known as the 4Deck, which was released simultaneously with The Deck 1.0 in September 2012.

The Deck as a dropbox

Dropboxes are small devices that can be planted inside a target organization. Ideally, these devices are cheap enough that losing a few isn't too painful. With some commercial dropboxes selling for $1000 or more, the loss of even a single device can have a significant effect on your bottom line. In addition to high cost, many commercial dropboxes suffer from other limitations.

Many of the lower-cost devices either send data out on the target's network or require physical retrieval in order to exfiltrate the data they have collected. Sending data over the target's network can lead to discovery of the dropbox. A dropbox that

stores data only on a local media makes the penetration tester wait for results. Additionally, if the device is discovered by the target, you will have gained no information from using the dropbox. Repeatedly visiting your dropbox increases your risk of detection.

Higher-end commercial dropboxes use 4G/GSM cellular networks for data exfiltration. While this has the advantage of being out of band, it does have some disadvantages as well. In some countries, 4G/GSM service is a bit pricey. Coverage may be poor or nonexistent at the penetration test site. Some nations have laws and regulations that make obtaining 4G/GSM service difficult. Even when performing tests in locations with good service and lax regulations, managing a collection of accounts and associated SIM cards can quickly become an administrative nightmare. Additionally, caching and compressing data to economize on bandwidth leads to complications.

An additional limitation of many dropboxes is that they lack many of the standard penetration testing tools. In part, this is due to limited storage and insufficient processing power to run some of the more hefty tools like Metasploit. Contrast this with a device running The Deck with all of the tools found on a desktop penetration system.

A dropbox based on a BeagleBone running The Deck erases many of these limitations. The BeagleBone is small and can be battery-powered, which makes it easy to hide. With a list price of US$45, the BeagleBone Black is inexpensive enough that losing one occasionally isn't too painful. When outfitted with an IEEE 802.15.4 radio, a dropbox can transmit data up to a mile (1.6 km) away without requiring 4G/GSM service. As previously mentioned, The Deck also contains a large collection of tools not found in most dropboxes.

The Deck as a hacking drone

When many people think of dropboxes, they envision a social engineering exercise in which they must breach a target's security in order to hide devices inside a facility. In the traditional penetration testing model, a penetration tester might use one or more dropboxes to collect data and possibly execute some simple commands, but the bulk of the work is done on his or her laptop. Here in this book, a new model is presented in which the hacking is spread across multiple devices, which we'll call hacking drones that are given orders by and report to a command console operated by the penetration tester.

The line between dropbox and drone is a bit fuzzy. Indeed, dropboxes running The Deck may be commanded like drones provided they have IEEE 802.15.4 connectivity. Thanks to their low-power requirements, devices running The Deck may be battery-powered and potentially placed outside your target's secured perimeter. Eliminating the need to social engineer your way into the client's facility significantly reduces the chances that people will become suspicious.

While you certainly can perform a penetration test with a collection of drones that are little more than BeagleBones with batteries and IEEE 802.15.4 modems, you are not limited to this. The small size and weight open up many fun and useful

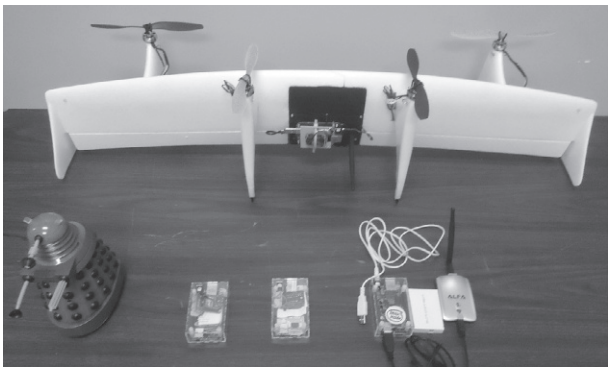

FIGURE 1.8

Devices running The Deck configured as dropboxes and/or drones. Bottom row from the left: a Dalek desktop defender with a BeagleBone, Alfa wireless adapter, and IEEE 802.15.4 radio hidden inside; a BeagleBone Black with IEEE 802.15.4 radio; an original BeagleBone with IEEE 802.15.4 radio; and a BeagleBone Black with network switch, USB hub, and Alfa wireless adapter for use as a dropbox. Back row: an aerial hacking drone (AirDeck) with a BeagleBone Black, IEEE 802.15.4 radio, and Alfa wireless adapter.

possibilities. For example, the Dalek desktop defender toy shown in Figure 1.8 has a hacking drone (or is it a dropbox?) hidden inside. There is enough space inside this toy for a BeagleBone, Alfa wireless adapter, and IEEE 802.15.4 modem. The aerial hacking drone, which has been dubbed the AirDeck, is also presented in Figure 1.8. The AirDeck can be used for initial reconnaissance and/or landed on a roof for penetration tests where physical access is difficult.

Another advantage of using drones is that you can increase the distance between you and the client. Sitting outside their office all day long in a van with a high-gain directional antenna can be quite conspicuous. It is much better to run your penetration test sitting by the hotel pool down the street from your client. Another nicety of using drones is that they can work 24×7 for you. In the traditional penetration model, not much is happening while you sleep. All the details of how to build and use drones will be covered later in this book.

SERENDIPITY

From whence cometh the idea for hacking drones

My most asked question regards the origin of the name The Deck. A close second would be questions around how I came up with the idea of using hacking drones. The honest answer is that I was looking at my collection of spare components in my home workshop one day and I noticed a few IEEE 802.15.4 (XBee) adapters were in my collection. I had originally acquired the XBee radios to use in a project for an intensive 13-day microcontroller class I taught at the university where I worked. I ended up not using them for the class. I also had a few extra original BeagleBones sitting on my workbench.

I knew that The Deck, which was originally designed to run on the BeagleBoard-xM (BB-xM), would run without modification on the BeagleBone. The original BeagleBone had a slightly slower processor, only half the RAM of the BB-xM, and no inbuilt video output, however. So by attaching the XBee radios to the BeagleBone, I could do something useful with extra hardware I had laying around and have some fun playing with XBee, which was somewhat new to me at the time. As I worked on building the first drones, I quickly realized that doing penetration testing with drones had lots of great potential.

I really liked the idea of fitting an entire army of drones, batteries, and accessories in one small bag. I routinely fly to conferences with as many as eight drones complete with batteries and accessories, a laptop, and a tablet all in a small carry on or laptop case. I realized that having devices that were easily configured to match the needs of a penetration test was really powerful. The fact that the devices were also inexpensive was a bonus. This became even more true with the release of the BeagleBone Black with more power than the original BeagleBone at half the price.

SUMMARY

This chapter provided a brief introduction to The Deck, a custom penetration testing-oriented Linux distribution, which is designed to run on the BeagleBoard and BeagleBone family of ARM-based devices. The Deck is a powerful and complete operating system containing over 1600 packages. Devices running The Deck can be operated as desktops, dropboxes, or drones with no software changes. Drones equipped with IEEE 802.15.4 radios can be commanded from up to a mile away. Devices running The Deck can come in many forms including raw computer boards, common office objects with hidden functionality, and radio-controlled aircraft.

In the next chapter, we will take a more detailed look at the devices in the BeagleBoard and BeagleBone family. We will examine their history, differences, and capabilities. Basic operations will also be discussed.

This page intentionally left blank