Building a Pentesting Lab for Wireless Networks

Learning penetration testing and hacking is an exciting experience that requires you to have a place field where you can get practical, hands-on experience of what you learn, that is, your own lab.

Starting with the basics of wireless networking and its associated risks, we will guide you through the stages of creating a penetration testing lab with wireless access and preparing your wireless penetration testing machine.

This book will guide you through configuring hardware and virtual network devices, filling the lab network with applications and security solutions. Along with a review of penetration testing frameworks, this book is also a detailed manual on preparing a platform for wireless penetration testing. By the end of this book, you will be at the point when you can practice and research without worrying about your lab environment for every task.

Who this book is written for
If you are a beginner or a security professional who wishes to learn to build a home or enterprise lab environment where you can safely practice penetration testing techniques and improve your hacking skills, then this book is for you. No prior penetration testing experience is required, as the lab environment is suitable for various skill levels and is used for a wide range of techniques from basic to advanced. Whether you are brand new to online learning or you are a seasoned expert, you will be able to set up your own hacking playground depending on your tasks.

What you will learn from this book
- Determine your needs and choose the appropriate lab components for them
- Build a virtual or hardware lab network
- Imitate an enterprise network and prepare intentionally vulnerable software and services
- Secure wired and wireless access to your lab
- Choose a penetration testing framework according to your needs
- Arm your own wireless hacking platform
- Get to know the methods of creating a strong defense mechanism for your system
In this package, you will find:

- The author's biography
- A preview chapter from the book, Chapter 1 'Understanding Wireless Network Security and Risks'
- A synopsis of the book’s content
- More information on Building a Pentesting Lab for Wireless Networks
About the Authors

**Vyacheslav Fadyushin** (CISA, CEH, PCI ASV) is a security consultant and a penetration tester with more than 9 years of professional experience and a diverse background in various aspects of information security.

His main points of interest and fields of expertise are ethical hacking and penetration testing, infrastructure and application security, mobile security, and information security management.


**Andrey Popov** is a security consultant and penetration tester with rich professional experience and a diverse background in infrastructure and application security, information security management, and ethical hacking. He has been working for a market-leading company along with another security professional since 2007.
Preface

*Building a Pentesting Lab for Wireless Networks* is a practical guide to building a penetration testing lab, accessible via Wi-Fi, which contains vulnerable components and at the same time secured from unauthorized external access. This book is intended for people learning ethical hacking and for security professionals who are responsible for penetration testing and maintaining security in their organization who wish to learn how to build a penetration testing lab for wireless networks.

The fact that the lab is secured from external access allows readers to use it both in corporate and home networks without putting themselves at risk. Thus, the book will be useful not only for people new to information security but also for security professionals who want to shift their expertise to the ethical hacking field. You will learn how to plan your lab, fill it with components, configure them, and secure the environment. Additionally, you will get an overview of the most popular hacking frameworks and toolsets and will be able to prepare your own wireless hacking platform on a Linux laptop or a virtual machine.

**What this book covers**

*Chapter 1, Understanding Wireless Network Security and Risks*, reviews which wireless technologies are used to transfer data, describes the associated risks and concludes which Wi-Fi protection mechanism is the most secure.

*Chapter 2, Planning Your Lab Environment*, designs the lab topology, plans its components to imitate a real corporate network and allow you to practice most of the possible lab tasks.

*Chapter 3, Configuring Networking Lab Components*, helps you understand the network communication and access rules in our lab environment, and you see two options on how to build your lab network, based on hardware Cisco devices and virtual ones.
Chapter 4, *Designing Application Lab Components*, shows you how to fill your lab with useful components, which actually bring sense to the whole story of building a lab network. We install the most common services that you are most likely to meet in the scope of a commercial penetration testing project and which you most probably would like to be able to hack.

Chapter 5, *Implementing Security*, shows our readers how to protect the lab network from unauthorized access and external attacks by installing and configuring network- and host-based security solutions. Additionally to securing the lab network, we prepare it for practicing important penetration testing topics, such as bypassing and evading security mechanisms and assessing their effectiveness.

Chapter 6, *Exploring Hacking Toolkits*, gives you an overview of several popular toolkits used in numerous hacking tasks and projects, along with examples of their utilization in the lab environment. It helps you get a brief understanding of their capabilities and a foundation for further learning.

Chapter 7, *Preparing a Wireless Penetration Testing Platform*, shows you how to prepare a penetration testing platform for wireless hacking, including the basic necessary tools. Additionally, the chapter explains how to choose a Wi-Fi interface suitable for penetration testing.

Chapter 8, *What’s Next?*, gives you some hints regarding what to start with and in which direction to dig if you want to develop ethical hacking skills and become a professional penetration tester.
In this chapter, we are going to review which wireless technologies allow data transfer, focusing on the Wi-Fi technology as the most important one for building our own penetration testing lab. As it is a very important topic for building a highly secure lab, we will also review the common Wi-Fi security mechanisms and their security risks in conjunction with an overview of the typical wireless attack methodology.

In this chapter, we will cover the following topics:

• Understanding wireless environment and threats
• Common WLAN protection mechanisms and their flaws
• Getting familiar with the Wi-Fi attack workflow

Understanding wireless environment and threats

As the first and the key step towards understanding wireless security and building a highly secure wireless lab, the nature of wireless media and its place in the modern life should be understood. In this section, we will be reviewing the main specifics and threats of wireless networking.

Wired networks use cables for data transmission, thus considered a "controlled" environment, protected by a physical level of security. In order to gain access to a wired network, an attacker would need to overcome any physical security systems to access buildings or other controlled zones and also overcome logical security systems, such as firewalls and intrusion detection/prevention systems (IDPS).
In the case of wireless networks, there is an open environment used with almost complete lack of control. Providing the security level equivalent to physical security in wired networks is not that easy nowadays. Wireless network segments can become available from another floor of the same building, neighboring buildings, or even outside—only signal strength limits physical borders of a wireless network. Therefore, unlike wired networks where connection points are known, a wireless network can be accessed from anywhere—as long as the signal is strong enough.

An overview of wireless technologies

Nowadays, various technologies are used for wireless data communications. They differ in used media, frequency bands, bandwidth, encoding methods, scopes of application, and other characteristics. Let's start by defining the term wireless communications. We would say it is a remote communication between two or more devices according to certain rules or specifications without establishing a physical connection via cables or wires.

In order to understand our definition more clearly, let's define the characteristics that can be assigned to the discussed method of communication:

- **Topology:**
  - Point-to-point
  - Point-to-multipoints

- **Use cases:**
  - Corporate infrastructure: Office and technological
  - Providing a service
  - Personal usage

- **Range:**
  - **Wireless personal area networks (WPAN):** Bluetooth, IrDA, and RFID
  - **Wireless local area networks (WLAN):** Wi-Fi
  - **Wireless metropolitan area networks (WMAN) and wireless wide area networks (WWAN):** WiMAX, GSM, and UMTS

- **Speed:**
  - 1 Mbit/s for WPAN
  - 54 Mbit/s for WLAN
  - 300 Mbit/s for WMAN
  - 15 Mbit/s for WWAN
A brief but very capacious way of mapping the two most important characteristics of wireless technologies (the data transmission speed and the range) is depicted in the following diagram:

As we now have a clear definition, we can proceed to look at some of the types of wireless data transfer technologies and their specifics.

Let's start with the mobile cellular communication, which is probably the most common type of wireless data transmission nowadays. Cellular communication is a mobile network—a type of mobile communication that is based on the cellular network. The key feature is that the overall coverage area is divided into cells. Cells partially overlap and together form a network. A network comprises separate base stations operating in the same frequency band and each covering its own area (cell) with a radio signal and switching equipment. Cells have unique IDs allowing to determine the current locations of subscribers and provide connection continuity when a person is moving from a coverage area of one base station into a range of another one.

The history of mobile communications began in the middle of the 20th century and has passed four major milestones in its development until and the present time:

- **1G** (G is short for generation): Analog cellular communication (based on AMPS, NAMPS, and NMT-450 standards)
- **2G**: Digital cellular communication (GSM and CDMA)
- **3G**: Broadband digital cellular communication (UMTS)
- **4G**: Cellular mobile communication with high demands (LTE)

Currently, the most forward-looking solutions are UMTS and LTE. Both data transmission standards have been inherited from GSM and allow us to transmit voice or data and provide a set of various services. The distinctive feature of these standards compared with the older generations is the ability to transfer data at a higher speed (up to 21 Mbit/s for incoming data in case of UMTS and up to 300 Mbit/s for incoming data in case of LTE). These speeds allow working on the Internet in comfortable conditions.
Since there is a large amount of existing standards and a lot of differences between the government requirements, various frequencies for data transmission and information protection techniques based on different encryption algorithms can be used in different countries and industries.

The next wireless technology that we are going to review is Bluetooth (representative of WPAN). Bluetooth allows information exchange between personal devices such as mobile phones, personal computers, tablets, input devices (microphones, keyboards, and joysticks), and output devices (printers and headsets). Bluetooth operates in the free and widely available radio frequencies (between 2.4 to 2.485 GHz) for short-range communication at a distance of typically up to 10 meters (but there are exceptions) between devices and supports two types of connection: point-to-point and point-to-multipoint.

Bluetooth has a multilevel architecture consisting of the main protocol and a set of auxiliary protocols that implement the following:

- Creating and managing a radio connection between two devices
- Discovering services provided by devices and determining parameters
- Creating a virtual serial data stream and emulating RS-232 control signals
- Data transmission from another protocol stack
- Managing high-level services like audio distribution

In addition to protocols that implement these functionalities, the Bluetooth protocol stack also contains protocols such as:

- **PPP** (Point-to-Point Protocol)
- **TCP/IP**
- **OBEX** (Object Exchange Protocol)
- **WAE** (Wireless Application Environment)
- **WAP** (Wireless Application Protocol)

Another interesting way of wireless data transmission is using waves of light. There is a group of standards describing protocols of physical and logical levels of data transmission using infrared light waves as environment. It is known as **IrDA** (Infrared Data Association). Usually, implementation of this interaction is an emitter (infrared light-emitting diode) and a receiver (photodiode) located on each side of the link.
This technology became especially popular in the late 1990s. Nowadays, it has almost entirely replaced by more modern methods of communication such as Wi-Fi and Bluetooth. But it is still used in remote controllers of home appliances and usually these devices have one-way connection (one side has an emitter only and the other side has a receiver only).

The main reasons for the rejection of IrDA were the following:

- Limited distance of connection
- Direct visibility requirements
- Low speed of data transmission (in the later revisions of the standard, speed was increased but even the high-speed versions are not popular now)

Another example of wireless optics as data transmission is Free Space Optics (FSO). This exotic technology uses an infrared laser as the information carrier, and it is used for long-distance communications in open spaces. The disadvantage of this system, as in the case of IrDA, is the direct visibility requirement that is highly dependent on weather.

Usually FSO is used:

- When cabling is not possible or too costly
- When you require a private link that is not receptive to radio interference and does not create any (for example, at airports)

Going back to wireless data transmission using a radio signal, we need to review the IEEE 802.11 standards family, also known as Wi-Fi (Wi-Fi is a trademark of Wi-Fi Alliance for wireless networks based on IEEE 802.11 standards family).

The family of IEEE 802.11 contains a few dozen standards, but we will directly take a look at the ones designed for data transmission, omitting the auxiliary ones:

- **802.11**: This is the original standard approved in 1997, and it describes transmission at 2.4 GHz frequency with 1 Mbit/s and 2 Mbit/s speeds.
- **802.11b**: This is an improvement to 802.11 to support higher speeds (up to 5.5 Mbit/s and 11 Mbit/s). It was approved in 1999.
- **802.11a**: This is the standard approved in 1999 and used since 2001. This standard allows us to work at 5 GHz frequency with 54 Mbit/s speed.
- **802.11g**: This allows us to transfer data at 2.4 GHz frequency with 54 Mbit/s speed. It was approved in 2003.
- **802.11n**: This was approved in 2009. This standard increases the speed of data transmission up to 600 Mbit/s at 2.4 to 2.5 GHz or 5 GHz frequencies. The standard is backwards-compatible with 802.11 a/b/g.
• **802.11ac and 802.11ad**: These standards were approved in 2014. They allow data transfer at the speed up to 7 Gbit/s and have additional working frequency (60 GHz).

IEEE 802.11 is used for data transmission via radio within a range of 100 meters. Typically, the IEEE 802.11 network consists of at least one access point and at least one client, but it is possible to connect two clients in a point-to-point (ad hoc) mode. In case of point-to-point connection, the access point is not used and clients are connected directly to each other.

Due to the fact that IEEE 802.11 applies to WLAN and provides high-speed data transfer for a local area, solutions based on IEEE 802.11 are ideal to solve "the last mile" problem. IEEE 802.11 allows us to reduce costs of deploying and expanding local networks and also provides network access in difficult-to-reach places, such as outdoors or inside buildings that have historical value.

### An overview of wireless threats

Considering the specifics mentioned in the previous section, let's state the most common wireless threats.

In case of a radio signal as a transmission environment and in the case of a wired connection, there are a lot of threats, each with their own specifics.

The first threat in our list is information gathering. It usually begins with reconnaissance and mostly depends on the distance from the victim because of the radio waves nature—you don't need to connect to another network device to receive radio waves generated by that device. The result of reconnaissance can give answers about locations of network objects and users, what devices and technologies are being used, and so on. Usually, the captured network traffic contains important information. Traffic analysis can be done by checking the network packages data, the pattern of network packages, and running sessions between members of connections (access points and their clients). Also, it should be noted that the wireless network control packets (service traffic) are not encrypted. Besides, it is very difficult to distinguish between information collecting user and legal participant of the network. The fact that the radio signal coverage can go outside of a controlled zone creates easy opportunities for the realization of information gathering risk.
The second threat is problems in settings of network devices, such as using weak encryption keys or authentication methods with known vulnerabilities. Potential attackers primarily exploit these disadvantages. Incorrectly configured access points may become the cause of breaking into an entire corporate network. In addition, in the case of a corporate network, it is difficult to track using unauthorized access points; for example, a typical employee can bring an unregistered access point and connect it to a corporate network. This creates a serious threat not only to the wireless network, but also to the entire company’s infrastructure.

Incorrectly configured wireless clients are an even greater threat than incorrectly configured access points. Such devices are on the move and often they are not specifically configured to reduce the risk or use default settings.

Following the previous point, the next threat is breaking the encryption. Attackers are well informed about the flaws of the widely used encryption algorithms, and for example, in the case of the WEP protocol, they can retrieve a pre-shared key from a client in less than 10 minutes.

The fourth threat facing wireless networks is the difficulty in tracking actions of a user. As already noted, the wireless devices are not "tied" to the network and can change their point of connection to the network. Incorrectly configuring the wireless client can automatically connect to the nearest wireless network. This mechanism allows attackers to switch the unsuspecting user host on an attacker’s device instead of a legitimate access point to perform vulnerability scanning, phishing attacks, or man-in-the-middle attacks. Furthermore, if a user simultaneously connects to a wired network, it becomes a convenient entry point to a corporate network.

Impersonating a user is a serious threat to any network, not just wireless. However, in the case of wireless communication, determining the authenticity of the user is more difficult. There are network identifiers (SSID) and filtering MAC addresses in place, but both are broadcasted in clear text in service packets and can be intercepted. Impersonation allows attackers to insert wrong frames to authorized communications and carry out an attack on a corporate infrastructure.

The fact that many laptop users prefer switching to WLANs if they are dissatisfied with the quality of the wired network service (weak connection, URL-filtering, or port-filtering) increases the risk. In most cases, operating systems do it automatically when a wired network is down.
The last threat that we would like to mention is **Denial of Service (DoS)**. The aim of a typical DoS attack is the violation of network service availability or a complete blocking of an authorized client access. Such an attack can be carried out, for example, by flooding a network with de-authentication or "junk" packets sent from a spoofed address. Tracking an attack source in this case is not an easy task. In addition, there is a possibility to organize a DoS attack on the physical level, running a fairly powerful jammer in the special frequency range.

**Wi-Fi media specifics**

Despite the wide variety of wireless technologies, the overwhelming majority of corporate and personal networking communications are based on Wi-Fi technology and this is the reason why we are going deep into this certain type of wireless technology.

Wi-Fi is prone to all threats mentioned earlier that are common for all the wireless technologies—the absence of any cables or other physical connections between clients and network devices creates great mobility for users, but also become the root cause for the most of Wi-Fi security flaws and challenges. This is both the main advantage and the main disadvantage of WLANs.

The first specification of Wi-Fi, the 802.11 standard, regulates operation of the equipment at a center frequency of 2.4 GHz with a maximum speed of up to 2 Mbit/s and was approved in 1997.

The standards of the 802.11 family regulate architectures of networks and devices, and describe the first and second of seven layers of the OSI model, along with the interaction protocols. The standards specify the base frequency, modulation techniques, and spread spectrum at the physical level.

The IEEE 802.11 standards strictly regulate only the two lower levels of the OSI model: the physical and data link layers that determine the specific features of local networks. The upper OSI levels are the same in wireless and wired LANs:
The need to distinguish features of various LANs is reflected by separating the data link layer into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). The MAC layer provides correct sharing of the overall environment. After gaining access to the environment it may use the higher LLC, which implements the functions of the interface with an adjacent network layer. In the 802.11 standard, MAC is similar to the implementation of Ethernet networks. The fundamental difference is that the 802.11 uses a half-duplex transceiver and cannot detect collisions during communication sessions. MAC uses a special protocol Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in the 802.11 standard or the distributed coordination function (DCF). Moreover, 802.11 MAC supports two modes of energy consumption: continuous operation mode and the saving mode.

The 802.11 standard was updated to the standard 802.11b version in 1999, which operates on the same main frequency of 2.4 GHz with a maximum speed of up to 22 Mbit/s.

The base architecture, ideology, and characteristics of the new 802.11b standard are similar to the original version of 802.11, and only the physical layer with a higher access speed and data transmission layer have been changed.
The standard also introduces error corrections and the possibility to work in conditions of strong interference and weak signal. For this purpose, the standard describes automatic methods of data transmission speed modification based on current signal strength and interference. The development of the Wi-Fi technology has drastically increased the number of different wireless devices in the world and created the problem of interference and congestion at the 2.4 GHz band due to the fact that such devices as microwave ovens, mobile phones and Bluetooth equipment noticeably influence each other.

The 802.11a standard (operating on a 5 GHz frequency band) was developed to unload the 2.4 GHz band. There are fewer sources of interference in the new range comparing to the 2.4 GHz band and the average level of noise is much lower. The 802.11a standard uses two basic frequencies around 5 GHz and a maximum data transfer rate of up to 54 Mbit/s.

It should be mentioned that the 5 GHz band is adjacent to the frequencies that are partly used for satellite and microwave communications. To eliminate interference between Wi-Fi equipment and the other departmental systems, the European Telecommunications Standards Institute (ETSI) has developed two additional protocols: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). Wi-Fi devices can automatically change frequency channels or decrease transmission power in the case of conflict on the carrier frequencies using these protocols.

The next step in the development of Wi-Fi is the standard 802.11g, approved in 2003. 802.11g is an improved version of 802.11b and is designed for devices operating at frequencies of 2.4 GHz with a maximum speed of 54 Mbit/s.

Now, the 802.11n standard has become the most widely used Wi-Fi technology. The developers have attempted to combine all the good features that were implemented in the previous versions in this new one. The 802.11n standard is designed for equipment operating at center frequencies of 2.4 GHz to 5 GHz as quickly as possible up to 600 Mbit/s. This standard was approved by the IEEE in September 2009. The standard is based on the technology of MIMO-OFDM. In IEEE, the maximum data rate of 802.11n is several times greater than the previous ones. This is achieved by doubling the width of the channel from 20 MHz to 40 MHz and due to implementation of MIMO technology with multiple antennas.

The last standard, which is rapidly gaining popularity, is 802.11ac. It is a wireless network standard adopted in January 2014. It operates in the 5 GHz frequency band and is backward compatible with IEEE 802.11n.

This standard allows us to significantly expand the network bandwidth from 433 Mbit/s to 6.77 Gb/s at an 8x MU-MIMO-antenna. This is the most significant innovation with respect to IEEE 802.11n. In addition, significantly less energy is used, which extends the battery life of mobile devices.
A summary of the technical information is presented in the following table:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequencies, MHz</th>
<th>Channels</th>
<th>Speeds, Mbit/s</th>
<th>Power, mW</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2400-2483.5</td>
<td>20</td>
<td>1; 2</td>
<td>100</td>
</tr>
<tr>
<td>802.11b</td>
<td>2400-2483.5</td>
<td>13</td>
<td>1; 2; 5; 5; 11; 22</td>
<td>100</td>
</tr>
<tr>
<td>802.11a</td>
<td>5150-5350</td>
<td>20</td>
<td>6; 9; 12; 18; 24; 36; 48; 54; 108</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>5650-6425</td>
<td></td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>802.11g</td>
<td>2400-2483.5</td>
<td>13</td>
<td>1; 2; 5; 5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48; 54; 108</td>
<td>250</td>
</tr>
<tr>
<td>802.11n</td>
<td>2400-2483.5</td>
<td>-</td>
<td>150</td>
<td>250</td>
</tr>
<tr>
<td></td>
<td>5150-5350</td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>5650-6425</td>
<td></td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>802.11ac</td>
<td>5170-5905</td>
<td>-</td>
<td>433</td>
<td>500</td>
</tr>
</tbody>
</table>

**Common WLAN protection mechanisms and their flaws**

To be able to protect a wireless network, it is crucial to clearly understand which protection mechanisms exist and which security flaws they have. This topic will be useful not only for those readers who are new to Wi-Fi security, but also as a refresher for experienced security specialists. Understanding this topic will help you understand one of the important aspects of this book: you should properly plan the security of your wireless penetration testing lab.

**Hiding SSID**

Let's start with one of the common mistakes made by network administrators: relying only on security by obscurity. In the frames of the current subject, it means using a hidden WLAN **SSID** (short for service set identification) or simply a WLAN name.

Hidden SSID means that a WLAN does not send its SSID in broadcast beacons advertising itself and doesn't respond to broadcast probe requests, thus making itself unavailable in the list of networks on Wi-Fi-enabled devices. It also means that normal users do not see the WLAN in their available networks list.
But the lack of WLAN advertising does not mean that an SSID is never transmitted in the air—it is actually transmitted in plaintext with a lot of packets between access points and devices connected to them, regardless of the security type used. Therefore, SSIDs are always available for all the Wi-Fi network interfaces in a range and are visible to any attacker using various passive sniffing tools.

**MAC filtering**

To be honest, MAC filtering cannot even be considered as a security or protection mechanism for a wireless network, but it is still called so in various sources. So let's clarify why we cannot call it a security feature.

Basically, MAC filtering means allowing only those devices that have MAC addresses from a pre-defined list to connect to a WLAN, and not allowing connections from other devices. MAC addresses are transmitted unencrypted in Wi-Fi and are extremely easy for an attacker to intercept without even being noticed (refer to the following screenshot):

<table>
<thead>
<tr>
<th>BSSID</th>
<th>PWR</th>
<th>Becons</th>
<th>#Data, #/s</th>
<th>CH</th>
<th>MB</th>
<th>ENC</th>
<th>CIPHER</th>
<th>AUTH</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:65:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>: :</td>
<td>232</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>54e</td>
</tr>
<tr>
<td>5C:35:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>113</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>24:65:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>93</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>00:10:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>184</td>
<td>26</td>
<td>0</td>
<td>2</td>
<td>54</td>
</tr>
<tr>
<td>5C:35:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>85</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>08:10:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>239</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>54e</td>
</tr>
<tr>
<td>54:64:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>54e</td>
</tr>
<tr>
<td>34:31:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>54e</td>
</tr>
<tr>
<td>84:9C:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>54e</td>
</tr>
<tr>
<td>00:25:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>46</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>54e</td>
</tr>
<tr>
<td>24:65:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>54e</td>
</tr>
<tr>
<td>84:94:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>9C:80:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>73</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>34:81:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>84:94:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>54e</td>
</tr>
<tr>
<td>6E:72:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>54e</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BSSID</th>
<th>STATION</th>
<th>PWR</th>
<th>Rate</th>
<th>Lost</th>
<th>Frames</th>
<th>Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:18: :</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>(not associated) :</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

An example of a wireless traffic sniffing tool easily revealing MAC addresses
Keeping in mind the extreme simplicity of changing a physical address (MAC address) of a network interface, it becomes obvious why MAC filtering should not be treated as a reliable security mechanism.

MAC filtering can be used to support other security mechanisms, but it should not be used as the only security measure for a WLAN.

**WEP**

*Wired equivalent privacy (WEP)* was born almost 20 years ago at the same time as the Wi-Fi technology and was integrated as a security mechanism for the IEEE 802.11 standard.

As often happens with new technologies, it soon became clear that WEP contained weaknesses in design and was unable to provide reliable security for wireless networks. Several attack techniques were developed by security researchers that allowed them to crack a WEP key in a reasonable amount of time and use it to connect to a WLAN or intercept network communications between WLAN and client devices.

Let's briefly review how WEP encryption works and why is it so easy to break.

WEP uses so-called *initialization vectors (IV)* concatenated with a WLAN's shared key to encrypt transmitted packets. After encrypting a network packet, an IV is added to a packet as it is and sent to a receiving side, for example, an access point. This process is depicted in the following flowchart:

![The WEP encryption process](image-url)
An attacker just needs to collect enough IVs, which is also a trivial task using additional reply attacks to force victims to generate more IVs.

Even worse, there are attack techniques that allow an attacker to penetrate WEP-protected WLANs even without connected clients, which makes those WLANs vulnerable by default.

Additionally, WEP does not have a cryptographic integrity control, which also makes it vulnerable to attacks on confidentiality.

There are numerous ways an attacker can abuse a WEP-protected WLAN, for example:

- Decrypt network traffic using passive sniffing and statistical cryptanalysis
- Decrypt network traffic using active attacks (reply attack, for example)
- Traffic injection attacks
- Unauthorized WLAN access

Although WEP was officially superseded by the WPA technology in 2003, it can still be sometimes found in private home networks and even in some corporate networks (mostly belonging to small companies nowadays).

But this security technology has become very rare and will not be used in future, largely due to awareness in corporate networks and because manufacturers no longer activate WEP by default on new devices.

In our humble opinion, device manufacturers should not include WEP support in their new devices to avoid its usage and increase their customers' security.

From the security specialist's point of view, WEP should never be used to protect a WLAN, but it can be used for Wi-Fi security training purposes.

Regardless of the security type in use, shared keys always add an additional security risk; users often tend to share keys, thus increasing the risk of compromising the key and reducing accountability for key privacy.

Moreover, the more devices use the same key, the greater the amount of traffic becomes suitable for an attacker during cryptanalytic attacks, increasing their performance and chances of success. This risk can be minimized by using personal identifiers (key, certificate) for users and devices.
WPA/WPA2
Due to numerous WEP security flaws, the next generation of Wi-Fi security mechanisms became available in 2003: Wi-Fi Protected Access (WPA). It was announced as an intermediate solution until WPA2 became available and contained significant security improvements over WEP.

Those improvements include:

- **Stronger encryption**: The new standards use longer encryption keys than WEP (256-bit versus 64- and 128-bit) and became capable of utilizing the Advanced Encryption Standard (AES) algorithm.

- **Cryptographic integrity control**: WPA uses an algorithm called Michael instead of CRC used in WEP. This is supposed to prevent altering data packets on the fly and prevents resending sniffed packets.

- **Usage of temporary keys**: The Temporal Key Integrity Protocol (TKIP) automatically changes the encryption keys generated for every packet. This is a major improvement over the static WEP where encryption keys could be entered manually in an AP config. TKIP also operates RC4, but the way it is used was improved.

- **Support for client authentication**: The capability to use dedicated authentication servers for user and device authentication made WPA suitable for use in large enterprise networks.

The support for the cryptographically strong AES algorithm was implemented in WPA, but it was not set as mandatory, only optional.

Although WPA was a significant improvement over WEP, it was a temporary solution before WPA2 was released in 2004 and became mandatory for all new Wi-Fi devices.

WPA2 works very similarly to WPA and the main differences between WPA and WPA2 are in the algorithms used to provide security:

- AES became the mandatory algorithm for encryption in WPA2 instead of the default RC4 in WPA

- TKIP used in WPA was replaced by Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)

Because of the very similar workflows, WPA and WPA2 are also vulnerable to the similar or the same attacks and are usually known as and written as one word, WPA/WPA2. Both WPA and WPA2 can work in two modes: **pre-shared key (PSK)** or personal mode and enterprise mode.
Pre-shared key mode

Pre-shared key or personal mode was intended for home and small office use where networks have low complexity. We are more than sure that all our readers have met this mode and that most of you use it at home to connect your laptops, mobile phones, tablets, and so on to home networks.

The general idea of PSK mode is using the same secret key on an access point and on a client device to authenticate the device and establish an encrypted connection for networking. The process of WPA/WPA2 authentication using a PSK consists of four phases and is also called a **4-way handshake**. It is depicted in the following diagram:

![WPA/WPA2 4-way handshake](image)

The main WPA/WPA2 flaw in PSK mode is the possibility to sniff a whole 4-way handshake and to brute force a security key offline without any interaction with a target WLAN. Generally, the security of a WLAN mostly depends on the complexity of the chosen PSK.
Computing a **PMK** (short for **primary master key**) used in 4-way handshakes (refer to the handshake diagram) is a very time-consuming process compared to other computing operations and computing hundreds of thousands of them can take a very long time. But in the case of a short and low complexity PSK being in use, a brute-force attack does not take long even on a not-so-powerful computer. If a key is complex and long enough, cracking it can take much longer, but still there are ways to speed up this process:

- Using powerful computers with **CUDA** (short for **Compute Unified Device Architecture**), which allows a software to directly communicate with GPUs for computing. As GPUs are natively designed to perform mathematical operations and do them much faster than CPUs, the process of cracking works several times faster with CUDA.

- Using rainbow tables that contain pairs of various PSKs and their corresponding precomputed hashes. They save a lot of time for an attacker because the cracking software just searches for a value from an intercepted 4-way handshake in rainbow tables and returns a key corresponding to the given PMK if there was a match, instead of computing PMKs for every possible character combination. Because WLAN SSIDs are used in 4-way handshakes analogous to a cryptographic salt, PMKs for the same key will differ for different SSIDs. This limits the application of rainbow tables to a number of the most popular SSIDs.

- Using cloud computing is another way to speed up the cracking process, but it usually costs additional money. The more computing power an attacker can rent (or get through another ways), the faster the process is. There are also online cloud-cracking services available on the Internet for various cracking purposes including cracking 4-way handshakes.

Furthermore, as with WEP, the more users know a WPA/WPA2 PSK, the greater the risk of compromise—that's why it is also not an option for big complex corporate networks.

WPA/WPA2 PSK mode provides the sufficient level of security for home and small office networks only when a key is long and complex enough and is used with a unique (or at least not popular) WLAN SSID.
Enterprise mode

As already mentioned in the previous section, using shared keys poses a security risk and in the case of WPA/WPA2 highly relies on a key length and complexity. But there are several factors in enterprise networks that should be taken into account when talking about WLAN infrastructure: flexibility, manageability, and accountability.

There are various components that implement those functions in big networks, but in the context of our topic, we are mostly interested in two of them: AAA (short for authentication, authorization, and accounting) servers and wireless controllers.

WPA-Enterprise or 802.1x mode was designed for enterprise networks where a high security level is needed and the use of an AAA server is required. In most cases, a RADIUS server is used as an AAA server and the following EAP (Extensible Authentication Protocol) types are supported (and several more, depending on a wireless device) with WPA/WPA2 to perform authentication:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- PEAP-TLS
- EAP-FAST

You can find a simplified WPA-Enterprise authentication workflow in the following diagram:
Depending on an EAP-type configuration, WPA-Enterprise can provide various authentication options.

The most popular EAP type (based on our own experience in numerous pentests) is PEAPv0/MSCHAPv2, which is relatively easily integrated with existing Microsoft Active Directory infrastructures and is relatively easy to manage. But this type of WPA protection is relatively easy to defeat by stealing and brute-forcing user credentials with a rogue access point.

The most secure EAP type (at least, when configured and managed correctly) is EAP-TLS, which employs certificate-based authentication for both users and authentication servers. During this type of authentication, clients also check server's identity and a successful attack with a rogue access point becomes possible only if there are errors in configuration or insecurities in certificate maintenance and distribution.

It is recommended to protect enterprise WLANs with WPA-Enterprise in EAP-TLS mode with mutual client and server certificate-based authentication. But this type of security requires additional work and resources.

**WPS**

*Wi-Fi Protected Setup (WPS)* is actually not a security mechanism, but a key exchange mechanism which plays an important role in establishing connections between devices and access points. It was developed to make the process of connecting a device to an access point easier, but it turned out to be one of the biggest holes in modern WLANs if activated.

WPS works with WPA/WPA2-PSK and allows devices to connect to WLANs with one of the following methods:

- **PIN**: Entering a PIN on a device. A PIN is usually printed on a sticker at the back of a Wi-Fi access point.
- **Push button**: Special buttons should be pushed on both an access point and a client device during the connection phase. Buttons on devices can be physical and virtual.
- **NFC**: A client should bring a device close to an access point to utilize the Near Field Communication technology.
- **USB drive**: Necessary connection information exchange between an access point and a device is done using a USB drive.
Because WPS PINs are very short and their first and second parts are validated separately, an online brute-force attack on a PIN can be done in several hours allowing an attacker to connect to a WLAN.

Furthermore, the possibility of offline PIN cracking was found in 2014, which allows attackers to crack pins in 1 to 30 seconds, but it works only on certain devices.

You should also not forget that a person who is not permitted to connect to a WLAN but who can physically access a Wi-Fi router or access point can also read and use a PIN or connect via the push button method.

Getting familiar with the Wi-Fi attack workflow
In our opinion (and we hope you agree with us), planning and building a secure WLAN is not possible without the understanding of various attack methods and their workflow. In this topic, we will give you an overview of how attackers work when they are hacking WLANs.

General Wi-Fi attack methodology
After refreshing our knowledge about wireless threats and Wi-Fi security mechanisms, let's have a look at the attack methodology used by attackers in the real world. Of course, as with all other types of network attack, wireless attack workflows depend on certain situations and targets, but they still align with the following general sequence in almost all cases:

1. The first step is planning. Normally, attackers need to plan what are they going to attack, how can they do it, which tools are necessary for the task, when is the best time and place to attack certain targets, and which configuration templates will be useful so that they can be prepared in advance. White-hat hackers or penetration testers need to set schedules and coordinate project plans with their customers, choose contact persons on the customer side, define project deliverables, and do other organizational work if required. As with every penetration testing project, the better a project was planned (and we can use the word "project" for black-hat hackers' tasks), the greater the chances of a successful result.
2. The next step is **surveying**. Getting as accurate as possible and as much as possible information about a target is crucial for a successful hack, especially in uncommon network infrastructures. To hack a WLAN or its wireless clients, an attacker would normally collect at least SSIDs or MAC addresses of access points and clients and information about the security type in use. It is also very helpful for an attacker to understand if WPS is enabled on a target access point. All that data allows attackers not only to set proper configs and choose the right options for their tools, but also to choose appropriate attack types and conditions for a certain WLAN or Wi-Fi client. All collected information, especially non-technical (for example, company and department names, brands, or employee names), can also become useful at the cracking phase to build dictionaries for brute-force attacks.

3. Depending on the type of security and attacker's luck, data collected at the survey phase can even make the active attack phase unnecessary and allow an attacker to proceed directly with the **cracking** phase. The **active attacks** phase involves active interaction between an attacker and targets (WLANs and Wi-Fi clients). At this phase, attackers have to create conditions necessary for a chosen attack type and execute it. It includes sending various Wi-Fi management and control frames and installing rogue access points. If an attacker wants to cause a denial of service in a target WLAN as a goal, such attacks are also executed at this phase. Some of active attacks are essential for successfully hacking a WLAN, but some of them are intended to just speed up hacking and can be omitted to avoid causing alarm on various wireless intrusion detection/prevention systems (WIDPS), which can possibly be installed in a target network. Thus, the active attacks phase can be called optional.

4. Cracking is another important phase where an attacker cracks 4-way handshakes, WEP data, NTLM hashes, and so on, which were intercepted at the previous phases. There are plenty of various free and commercial tools and services including cloud cracking services. In the case of success at this phase, an attacker gets the target WLAN's secret(s) and can proceed with connecting to the WLAN, decrypt intercepted traffic, and so on.

---

**The active attacking phase**

Let's have a closer look at the most interesting parts of the active attack phase—WPA-PSK and WPA-Enterprise attacks—in the following sections.
WPA-PSK attacks
As both WPA and WPA2 are based on the 4-way handshake, attacking them doesn't differ—an attacker needs to sniff a 4-way handshake in a moment, establishing a connection between an access point and an arbitrary wireless client and brute forcing a matching PSK. It does not matter whose handshake is intercepted, because all clients use the same PSK for a given target WLAN.

Sometimes, attackers have to wait long until a device connects to a WLAN to intercept a 4-way handshake and of course they would like to speed up the process when possible. For that purpose, they force an already connected device to disconnect from the access point sending control frames (deauthentication attack) on behalf of a target access point. When a device receives such a frame, it disconnects from the WLAN and tries to reconnect again if the "automatic reconnect" feature is enabled (it is enabled by default on most devices), thus performing another 4-way handshake that can be intercepted by an attacker.

Another possibility to hack a WPA-PSK protected network is to crack a WPS PIN if WPS is enabled on a target WLAN.

Enterprise WLAN attacks
Attacking becomes a little bit more complicated if WPA-Enterprise security is in place, but could be executed in several minutes by a properly prepared attacker by imitating a legitimate access point with a RADIUS server and by gathering user credentials for further analysis (cracking).

To settle this attack, an attacker needs to install a rogue access point with an SSID identical to the target WLAN's SSID and set other parameters (like EAP type) similar to the target WLAN to increase chances of success and reduce the probability of the attack to be quickly detected.

Most user Wi-Fi devices choose an access point for a connection to a certain WLAN by a signal strength—they connect to that one which has the strongest signal. That is why an attacker needs to use a powerful Wi-Fi interface for a rogue access point to override signals from legitimate ones and make devices connect to the rogue access point.

A RADIUS server used during such attacks should have the capability to record authentication data, NTLM hashes, for example.
From a user perspective, being attacked in such way looks like just being unable to connect to a WLAN for an unknown reason and could even be not seen if a user is not using a device at that moment and is just passing by a rogue access point. It is worth mentioning that classic physical security or wireless IDPS solutions are not always effective in such cases. An attacker or a penetration tester can install a rogue access point outside of the range of a target WLAN. It will allow the hacker to attack user devices without the need to get into a physically controlled area (for example, an office building), thus making the rogue access point unreachable and invisible for wireless IDPS systems. Such a place could be a bus or train station, parking lot, or a café where a lot of users of a target WLAN go with their Wi-Fi devices.

Unlike WPA-PSK with only one key shared between all WLAN users, the Enterprise mode employs personified credentials for each user whose credentials could be more or less complex depending only on a certain user. That is why it is better to collect as many user credentials and hashes as possible, thus increasing the chances of successful cracking.

**Summary**

In this chapter, we reviewed which wireless technologies are used to transfer data and especially highlighted the Wi-Fi technology as the technology that we will employ to provide network access to our penetration testing lab.

During our journey through this chapter, we also looked at the security mechanisms that are used to secure access to wireless networks, their typical threads, and common misconfigurations that lead to security breaches and allow attackers to harm corporate and private wireless networks.

The brief attack methodology overview has given us a general understanding of how attackers normally act during wireless attacks and how they bypass common security mechanisms by exploiting certain flaws in those mechanisms.

We also saw that the most secure and preferable way to protect a wireless network is to use WPA2-Enterprise security along with a mutual client and server authentication, which we are going to implement in our penetration testing lab.

Now, we are ready to proceed with building a wireless lab protected from the flaws listed previously. In the next chapter, we are going to help you to first determine the tasks that a lab should fulfill for you and then we will guide you through the whole lab planning process. The guidance is organized in such a way that you can decide which lab components and technologies you need to implement based on your own requirements.
Where to buy this book

You can buy Building a Pentesting Lab for Wireless Networks 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.