Practice Labs - Ethical Hacker v10

Hacking Wireless Networks

Introduction

Ethical Hacking
Wireless Networks
Hacking Methods
Exploitation

Welcome to the **Hacking Wireless Networks** Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

Learning Outcomes

In this module, you will complete the following exercises:

- Hacking Wireless Network Techniques
- Hardening a Wireless Network

After completing this lab, you will have further knowledge of:

- Wireless Protocols
- Revealing Hidden SSIDs
- Wireless Threats
- Wireless Hacking Methodology

- Methods to Protect a Wireless Network

Exam Objectives

The following exam objectives are covered in this lab:

- **3.2** Information Security Attack Detection
- **3.3** Information Security Attack Prevention

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **45 minutes** to complete this lab.

Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for Certified Ethical Hacker v10.

Click **Next** to proceed to the first exercise.

Exercise 1 - Hacking Wireless Network Techniques

Wireless networks are everywhere now. The biggest advantage of a wireless network is that it allows user mobility. Unlike an Ethernet network, where the user is restricted due to an Ethernet cable being used, the wireless network allows the user to be mobile and connected within a certain range.

802.11 is the IEEE (Institute of Electrical and Electronics Engineers) standard for wireless networking. 802.11b/g/n are common standards supported on wireless access points for home networks and for small offices. 802.11 is a set of MAC (media access control) and PHY (physical layer) specifications for the implementation of wireless local area network (WLAN) computer communication in the 2.4GHz and 5GHz frequency bands. The standard provides the basis for wireless

There are different types of wireless networks that have different capabilities. Most wireless routers support the following Wi-Fi standards:

802.11a

This runs at 54 Mbps and is not compatible with 802.11b as it operates at the 5 GHz band. This standard was the first amendment of the original legacy IEEE 802.11 standard (1997), improving data rates from up to 2 Mbps of the original standard. It can cover an indoor area ranging from 35m to 125m.

802.11b

This provides a range of 150 feet and is the oldest standard still in use and supported by wireless routers. This is widely supported by wireless devices. IEEE 802.11b provides data rates of up to 11 Mbps using the 2.4 GHz band. This standard provides lower maximum data rates, but a greater range than the 802.11a standard since the 2.4 GHz frequencies used are not as readily absorbed by walls and obstacles as the 5 GHz frequencies

802.11g

This is supported by all wireless devices and network equipment today and is an economical option for buying a wireless access point. 802.11g is the same speed as 802.11a; however, it has a longer range of 170 feet and supports the 2.4 GHz frequency band. IEEE 802.11g provides data rates of up to 54 Mbps. This functions in the 2.4 GHz band (like 802.11b) but uses the same Orthogonal Frequency-Division Multiplexing

802.11n

This is faster than 802.11g and supported by network devices. 802.11n has a network speed of 600 Mbps and a maximum range of 230 feet. This standard uses multiple input/multiple output (MIMO) and may cause interference with nearby 802.11b/g networks. 802.11n has a higher price point than 802.11g.

802.11ac

This offers a speed of 1.33 Gigabits and a similar range to 802.11n (230 feet). IEEE 802.11ac is an amendment that improves upon the previous IEEE 802.11 standards. Characteristics of this standard include the introduction of wider channels (80 or 160 MHz compared to 40 MHz for 802.11n) in the 5 GHz band, more spatial streams (up to 8), and the addition of Multi-User MIMO (MU

Despite the speed and range of different wireless standards, they need to be used correctly. For example, if the wireless router or access points are not hardened, then no standard is safe for use.

In this exercise, you will learn about hacking wireless networks.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Wireless Protocols
- Revealing Hidden SSIDs
- Wireless Threats
- Wireless Hacking Methodology

Task 1 - Wireless Protocols

A wireless network can use different security protocols for authentication. A protocol, such as WEP, is no longer being used due to its weaknesses. There are other protocols that are stronger and are being used to protect wireless networks.

Wired Equivalent Privacy (WEP)

WEP was initially used with wireless networks, but it can be easily cracked so, it is no longer recommended for use.

WEP can be implemented in two different modes:

- **Open Authentication**: The client sends a request to connect to the WAP (Wi-Fi Protected Access), and it is then allowed to connect. The user does not require any credentials to connect to the WAP. The authentication takes place on the basis of the system's MAC address.
- **Shared Key Authentication**: The client sends an authentication request to the WAP, which, in return, sends a challenge-text. The client then encrypts the challenge-text with the WEP secret key and sends it back to the WAP. The WAP then decrypts the text. If the text is correct, then it authenticates the client and allows it to access the wireless network.

Encryption Algorithm: RC4

IV Size: 24-bits

Encryption Key: 40/104-Bits

Integrity Check Method: CRC-32

Wi-Fi Protected Access (WPA)

WPA uses Temporal Key Integrity Protocol (TKIP) - a 128-bit per-packet key. It will encrypt the network transmissions using TKIP, which was a replacement to WEP, but it is vulnerable and weaker than WPA2.

WPA can be implemented in two different modes:

- **Personal**: Uses a shared key between the access point (AP) and the client. After the key is shared, the connection between both is established, and the shared key is used for securing the traffic.
- **Enterprise**: Authenticates the client using an authentication server using the IEEE 802.1x protocol. The client can establish a connection only after successful authentication.

Encryption Algorithm: RC4, TKIP

IV Size: 48-bits

Encryption Key: 128-Bits

Integrity Check Method: CRC-32, Michael Algorithm

Wi-Fi Protected Access 2 (WPA2)

WPA is no longer considered a secure solution and has been replaced by WPA2, also known as 802.11i, which is currently mandatory on all Wi-Fi devices and provides CCMP and AES encryption support. WPA2-AES is the standard for newer wireless routers where all clients support AES. The WPA and WPA2 standards have adopted EAP with a myriad of EAP types as official authentication mechanisms. One of these is the EAP Transport Layer Security (EAP-TLS

WPA2 can be implemented in two modes:

- **Preshared key**: A shared secret is used to authenticate the client.

- **Authentication server**: An authentication server is used to authenticate the client.

Encryption Algorithm: AES, CCMP

IV Size: 48-bits

Encryption Key: 128-Bits

Integrity Check Method: CBC-MAC

Task 2 - Revealing Hidden SSIDs

Users can configure their wireless network not to broadcast their SSIDs, which means that the network name is not broadcasted. SSID is a unique wireless network identifier that is made up of 0 to 32 octets. It is also known as the wireless network name.

When a wireless network does not broadcast its SSID, you will not be able to find them without using a specialized tool. These tools include:

- inSSIDer
- WirelessNetView
- Winhotspot
- Homedale
- NetSurveyor
- Vistumbler

There are more tools available on the Internet that can find the hidden SSIDs. However, the above-mentioned tools are some that are widely used.

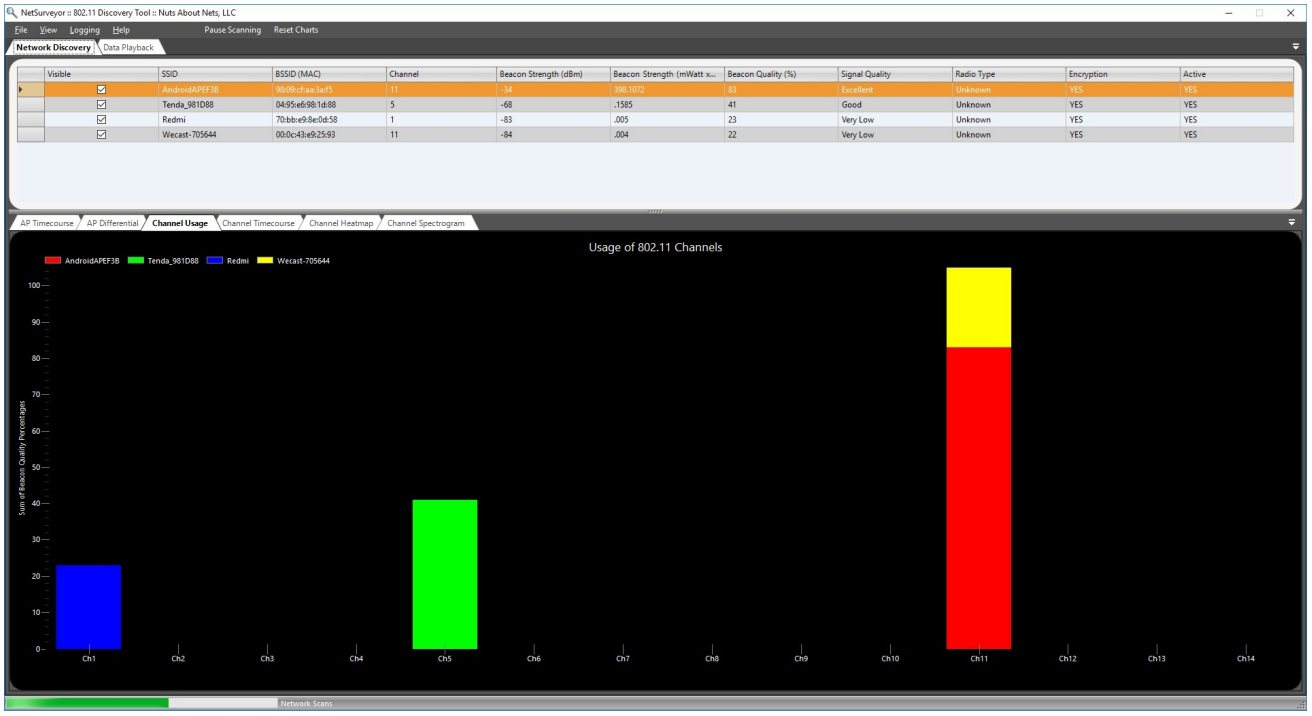

Figure 1.1 Screenshot of NetSurveyor: Showing the list of available wireless networks.

You can also use this as a wardriving tool. Wardriving is a method of searching for a wireless network while being on the move.

Also, you can find the hidden wireless networks without using any third-party utility. You can simply use the netsh command to locate a hidden wireless network.

To do this, you open a command prompt window and enter the following command:

```
netsh wlan show networks mode=bssid
```

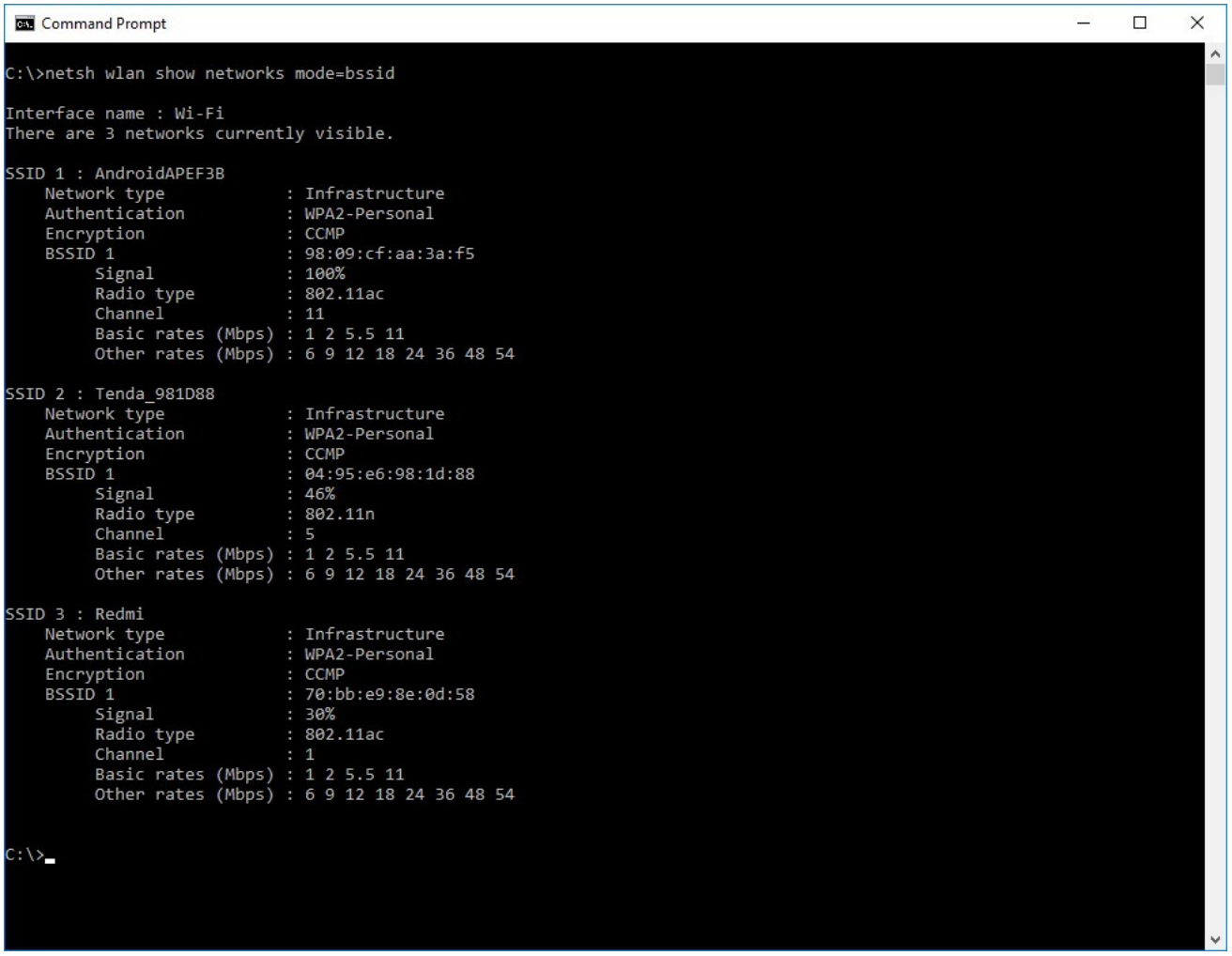

Figure 1.2 Screenshot of Command Prompt: Showing the list of available wireless networks.

Task 3 - Wireless Threats

Wireless networks are prone to various types of threats. Some of the common threats are:

- Rogue Access Points
- Ad-Hoc Networks
- Denial of Service (DoS)
- Configuration Issues
- Passive Capturing

In this task, you will learn about wireless network threats.

Rogue Access Points

Setting up a rogue access point requires you to have physical access to the network. The attacker can install the rogue access point on the physical network, and users can then connect to it. Over time, the attacker will keep capturing information. A user can also bring an access point and connect to the company's network and offer connectivity to the other users. This user can then capture the information that they were not supposed to have access to.

Ad-hoc Networks

An ad-hoc network, also known as the peer-to-peer network, is pretty simple to set up. A user on the network can simply connect a Bluetooth device with another Bluetooth device. Because there is a direct connection between two devices, there is no access point present. This creates an ad-hoc network. However, users typically do not implement proper security measures, which makes this type of network prone to attacks.

Denial of Service (DoS)

Wireless access points (WAP) that provide connectivity to the wireless network can be prone to DoS attacks. The purpose of the DoS attack is to bring down the WAP and prevent it from serving the legitimate users. In this attack, a large amount of traffic is sent to the WAP. This overwhelms the WAP and keeps it busy in responding to the attacking traffic. Meanwhile, it is unable to serve to the legitimate users.

Interference

A wireless network, which uses a 2.4 GHz band, is prone to interference. The attacker can use various devices or equipment to do this. For example, a cordless phone and microwave also work using the same band. The attacker can use multiple of these devices to cause interference in the wireless network and bring it down.

Configuration Problems

When a wireless access point (WAP) is set up, its default configuration should be changed. However, in many cases, this does not happen. Users tend to keep the default configuration, which makes the wireless network vulnerable to external attackers. For example, a user may leave the WAP with the default configuration, such as:

- Default admin password
- Default SSID
- Use of weak authentication protocol, such as WEP

Passive Capturing

An attacker can perform passive capturing to intercept data in transit. This is possible if the data in transit is not encrypted. The attacker can capture and extract the required information, such as usernames and passwords.

Wireless Network Abuse

When a wireless network is configured in an organization, the users can abuse it without using any sophisticated tools. For example, users can start sharing heavy files, such as MP3 or MP4, with other users. If a WAP is configured to provide Internet connectivity, the users can start downloading large files, such as software or movies. This can hinder wireless network performance. Such an issue is hard to detect unless you decide to perform network monitoring.

MAC spoofing

An organization with a wireless network can choose to implement MAC filtering, which will allow the system to connect only if the MAC address is listed in the WAP configuration. However, an attacker can also break this security method by getting access to a whitelisted MAC address, then replacing theirs with the captured one. Now, the attacker's system has the captured MAC address. The wireless network will check for the MAC address, and since it is whitelisted in its configuration, the attacker's system will be able to connect.

Man-in-the-middle

A man-in-the-middle attacker allows the users on the wireless network to connect to their WAP. Using another wireless connection on the same system, the attacker connects to the real WAP and allows the traffic to flow from his WAP to the real WAP, meanwhile intercepting the traffic.

De-authentication Attack

The attacker, using software like Air Jack, can force the users to disconnect from the real WAP and allow them to connect to the attacker's own WAP. It is easy for the attacker to then intercept the information from the connected systems.

Task 4 - Wireless Hacking Methodology

There are various methods that can be used to initiate wireless hacking. Some of the key ones are:

Wi-Fi Discovery

Just like a normal attack on a system or a network, the wireless network is also probed for more information using active or passive footprinting. There are tools like NetSurveyor that can provide a lot of information about the wireless network that is nearby.

Figure 1.3 Screenshot of NetSurveyor: Showing the list of available wireless networks with their detailed information.

GPS Mapping

You can use GPS to create a list of the discovered wireless networks. This information can be shared between hackers to explore opportunities in their regions.

Traffic Analysis

You can monitor and capture the wireless network traffic, which can help you with the following information:

- SSID of the wireless network
- Authentication method
- Encryption type

This information can be crucial in planning an attack on the wireless network.

Some of the important tools that can help in gathering information are:

- Wireshark
- Omni Peek

- Commview

Wireless Attacks

There are various types of attacks that can be conducted on a wireless network. The choice of attack would depend on the information that you have captured and where you can find a weakness or a loophole. For example, if the wireless network is using a specific type of WAP, you can explore and find out if this WAP has a security vulnerability. If you are lucky, the WAP is not patched. You will have an easy time exploiting the vulnerability.

Some of the wireless attacks that can be conducted are:

- Man-in-the-Middle (MITM)
- ARP Poisoning
- MAC Spoofing
- De-authentication

Exercise 2 - Hardening a Wireless Network

Wireless networks are prone to different attacks, as covered in the previous exercise. You need to use methods that can strengthen the security of the wireless network. It is important to remember that no single method can safeguard a wireless network. You would need to ensure the protection methods are customized to meet the wireless network's architecture requirements.

In this exercise, you will learn about some of the common methods to harden a wireless network.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Methods to protect a wireless network

Task 1 - Methods to Protect a Wireless Network

Wireless networks must be protected using various methods. Remember to use a method that meets your needs and fits the wireless architecture.

In this task, you will learn about these methods.

Encryption

The WAP will be receiving and transmitting information with the clients. You need to ensure that the WAP you are using has the ability to use encryption. If you are using an outdated WAP, consider replacing it with a newer one to use encryption.

In some cases, the manufacturers do not enable the encryption and leave it to the user to configure it. In these cases, you should enable encryption to protect the information being sent and received.

Security Protocol

Remember to use a security protocol that can protect the wireless network. For example, in an organization, it could be good to use WPA2-Enterprise.

Antivirus and Firewalls

Systems on the wireless network are no different than the systems on a wired network. The systems on the wireless network also need basic protection, such as an antivirus and a firewall. However, just having an antivirus and a firewall does not protect the systems. You need to ensure that you regularly update the systems with the latest patches for the antivirus, operating system, and applications.

SSID Broadcasting

By default, most of the wireless networks are configured to broadcast their SSIDs. You should disable SSID broadcasting. Even though a hacker can still use a tool such

as NetSurveyor to discover it, without a tool the SSID will not be discovered by systems. This can prevent attacks, such as wardriving.

Default Admin Password

All WAPs have a default admin password, which is used for initial login and configuration. However, the default admin password must be changed and replaced with a complex password.

There are websites that provide the default username and passwords for various WAP models. Anyone can go and find the login details for a specific model.

MAC Filtering

Even though MAC filtering is not a complete solution to protecting a wireless network from hackers, it still protects from unwanted individuals connecting to it. With the whitelisting of MAC addresses, you can only allow specific systems to connect to the wireless network to which they belong.

Radio Transmission

You should lower the radio transmission to prevent the wireless network from being broadcasted to a large area. This can prevent attacks, such as wardriving.

Network Auditing

You must audit the wireless network on a regular basis. In the audit, you can track if there are rogue access points or unwanted individuals who have connected (when you don't have MAC filtering enabled).

Review

Well done, you have completed the **Hacking Wireless Networks** Practice Lab.

Summary

You completed the following exercises:

- Hacking Wireless Network Techniques
- Hardening a Wireless Network

You should now have further knowledge of:

- Wireless Protocols
- Revealing Hidden SSIDs
- Wireless Threats
- Wireless Hacking Methodology
- Methods to Protect a Wireless Network

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.