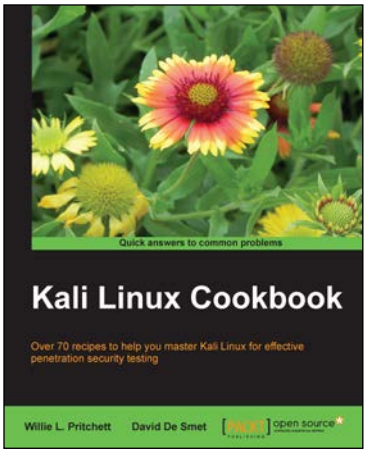
[PACKT] open source
community experience distilled
PUBLISHING

Kali Linux Cookbook

Willie L. Pritchett
David De Smet



Chapter No. 9
"Wireless Attacks"

In this package, you will find:

A Biography of the authors of the book

A preview chapter from the book, Chapter NO.9 "Wireless Attacks"

A synopsis of the book’s content

Information on where to buy this book

About the Authors

Willie L. Pritchett has a Master's in Business Administration. He is a seasoned developer and security enthusiast who has over 20 years of experience in the IT field. He is currently the Chief Executive at Mega Input Data Services, Inc., a full service database management firm specializing in secure, data-driven, application development, and staffing services. He has worked with state and local government agencies as well as helping many small businesses reach their goals through technology. Willie has several industry certifications and currently trains students on various topics including ethical hacking and penetration testing.

I would like to thank my wife Shavon for being by my side and supporting me as I undertook this endeavor. To my children, Sierra and Josiah, for helping me to understand the meaning of quality time. To my parents, Willie and Sarah, I thank you for providing a work ethic and core set of values that guide me through the roughest days. A special thanks to all of my colleagues, associates, and business partners who gave me a chance when I first started in the IT field; through you a vision of business ownership wasn't destroyed, but allowed to flourish. Finally, I would like to thank all of the reviewers and technical consultants who provided exceptional insight and feedback throughout the course of writing this book.

David De Smet has worked in the software industry since 2007 and is the founder and CEO of iSoftDev Co., where he is responsible for many varying tasks, including but not limited to consultant, customer requirements specification analysis, software design, software implementation, software testing, software maintenance, database development, and web design. He is so passionate about what he does that he spends inordinate amounts of time in the software development area. He also has a keen interest in the hacking and network security field and provides network security assessments to several companies.

I would like to extend my thanks to Usha Iyer for giving me the opportunity to get involved in this book, as well as my project coordinator Sai Gamare and the whole team behind the book. I thank my family and especially my girlfriend Paola Janahaní for the support, encouragement, and most importantly the patience while I was working on the book in the middle of the night.

Kali Linux Cookbook

Kali Linux is a Linux-based penetration testing arsenal that aids security professionals in performing assessments in a purely native environment dedicated to hacking. Kali Linux is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. It is a successor to the popular BackTrack distribution.

Kali Linux Cookbook provides you with practical recipes featuring many popular tools that cover the basics of a penetration test: information gathering, vulnerability identification, exploitation, privilege escalation, and covering your tracks.

The book begins by covering the installation of Kali Linux and setting up a virtual environment to perform your tests. We then explore recipes involving the basic principles of a penetration test such as information gathering, vulnerability identification, and exploitation. You will learn about privilege escalation, radio network analysis, voice over IP, password cracking, and Kali Linux forensics.

Kali Linux Cookbook will serve as an excellent source of information for the security professional and novice alike. The book offers detailed descriptions and example recipes that allow you to quickly get up to speed on both Kali Linux and its usage in the penetration testing field.

We hope you enjoy reading the book!

What This Book Covers

Chapter 1, Up and Running with Kali Linux, shows you how to set up Kali Linux in your testing environment and configure Kali Linux to work within your network.

Chapter 2, Customizing Kali Linux, walks you through installing and configuring drivers for some of the popular video and wireless cards.

Chapter 3, Advanced Testing Lab, covers tools that can be used to set up more advanced simulations and test cases.

Chapter 4, Information Gathering, covers tools that can be used during the information gathering phase including Maltego and Nmap.

Chapter 5, Vulnerability Assessment, walks you through the usage of the Nessus and OpenVAS vulnerability scanners.

Chapter 6, Exploiting Vulnerabilities, covers the use of Metasploit through attacks on commonly used services.

Chapter 7, Escalating Privileges, explains the usage of tools such as Ettercap, SET, and Meterpreter.

Chapter 8, Password Attacks, walks you through the use of tools to crack password hashes and user accounts.

Chapter 9, Wireless Attacks, walks you through how to use various tools to exploit the wireless network.

9
Wireless Attacks

In this chapter, we will cover:

- Wireless network WEP cracking
- Wireless network WPA/WPA2 cracking
- Automating wireless network cracking
- Accessing clients using a fake AP
- URL traffic manipulation
- Port redirection
- Sniffing network traffic

Introduction

These days, wireless networks are everywhere. With users being on the go like never before, having to remain stationary because of having to plug into an Ethernet cable to gain Internet access is not feasible. For this convenience, there is a price to be paid; wireless connections are not as secure as Ethernet connections. In this chapter, we will explore various methods for manipulating radio network traffic including mobile phones and wireless networks.

Wireless network WEP cracking

Wireless Equivalent Privacy, or **WEP** as it's commonly referred to, has been around since 1999 and is an older security standard that was used to secure wireless networks. In 2003, WEP was replaced by WPA and later by WPA2. Due to having more secure protocols available, WEP encryption is rarely used. As a matter of fact, it is *highly* recommended that you never use WEP encryption to secure your network! There are many known ways to exploit WEP encryption and we will explore one of those ways in this recipe.

In this recipe, we will use the AirCrack suite to crack a WEP key. The AirCrack suite (or AirCrack NG as it's commonly referred to) is a WEP and WPA key cracking program that captures network packets, analyzes them, and uses this data to crack the WEP key.

Getting ready

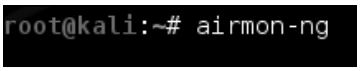
In order to perform the tasks of this recipe, experience with the Kali terminal window is required. A supported wireless card configured for packet injection will also be required. In case of a wireless card, packet injection involves sending a packet, or injecting it onto an already established connection between two parties. Please ensure your wireless card allows for packet injection as this is not something that all wireless cards support.

How to do it...

Let's begin the process of using AirCrack to crack a network session secured by WEP.

1. Open a terminal window and bring up a list of wireless network interfaces:

   ```
   airmon-ng
   ```

2. Under the `interface` column, select one of your interfaces. In this case, we will use `wlan0`. If you have a different interface, such as `mon0`, please substitute it at every location where `wlan0` is mentioned.
3. Next, we need to stop the `wlan0` interface and take it down so that we can change our MAC address in the next step.

   ```
   airmon-ng stop
   ifconfig wlan0 down
   ```

4. Next, we need to change the MAC address of our interface. Since the MAC address of your machine identifies you on any network, changing the identity of our machine allows us to keep our true MAC address hidden. In this case, we will use `00:11:22:33:44:55`.

   ```
   macchanger --mac 00:11:22:33:44:55 wlan0
   ```

5. Now we need to restart `airmon-ng`.

   ```
   airmon-ng start wlan0
   ```

6. Next, we will use `airodump` to locate the available wireless networks nearby.

   ```
   airodump-ng wlan0
   ```

7. A listing of available networks will begin to appear. Once you find the one you want to attack, press *Ctrl* + *C* to stop the search. Highlight the MAC address in the `BSSID` column, right click your mouse, and select copy. Also, make note of the channel that the network is transmitting its signal upon. You will find this information in the `Channel` column. In this case, the channel is `10`.

8. Now we run `airodump` and copy the information for the selected BSSID to a file. We will utilize the following options:

   - `–c` allows us to select our channel. In this case, we use `10`.
   - `–w` allows us to select the name of our file. In this case, we have chosen `wirelessattack`.
   - `–bssid` allows us to select our BSSID. In this case, we will paste `09:AC:90:AB:78` from the clipboard.

   ```
   airodump-ng –c 10 –w wirelessattack --bssid 09:AC:90:AB:78 wlan0
   ```

9. A new terminal window will open displaying the output from the previous command. Leave this window open.

10. Open another terminal window; to attempt to make an association, we will run `aireplay`, which has the following syntax: `aireplay-ng -1 0 –a [BSSID] –h [our chosen MAC address] –e [ESSID] [Interface]`

    ```
    aireplay-ng -1 0 -a 09:AC:90:AB:78 –h 00:11:22:33:44:55 –e
    backtrack wlan0
    ```

11. Next, we send some traffic to the router so that we have some data to capture. We use `aireplay` again in the following format: `aireplay-ng -3 –b [BSSID] – h [Our chosen MAC address] [Interface]`

    ```
    aireplay-ng -3 –b 09:AC:90:AB:78 –h 00:11:22:33:44:55 wlan0
    ```

12. Your screen will begin to fill with traffic. Let this process run for a minute or two until we have information to run the crack.

13. Finally, we run AirCrack to crack the WEP key.

```
aircrack-ng -b 09:AC:90:AB:78 wirelessattack.cap
```

That's it!

How it works...

In this recipe, we used the AirCrack suite to crack the WEP key of a wireless network. AirCrack is one of the most popular programs for cracking WEP. AirCrack works by gathering packets from a wireless connection over WEP and then mathematically analyzing the data to crack the WEP encrypted key. We began the recipe by starting AirCrack and selecting our desired interface. Next, we changed our MAC address which allowed us to change our identity on the network and then searched for available wireless networks to attack using `airodump`. Once we found the network we wanted to attack, we used `aireplay` to associate our machine with the MAC address of the wireless device we were attacking. We concluded by gathering some traffic and then brute-forced the generated CAP file in order to get the wireless password.

Wireless network WPA/WPA2 cracking

WiFi Protected Access, or **WPA** as it's commonly referred to, has been around since 2003 and was created to secure wireless networks and replace the outdated previous standard, WEP encryption. In 2003, WEP was replaced by WPA and later by WPA2. Due to having more secure protocols available, WEP encryption is rarely used.

In this recipe, we will use the AirCrack suite to crack a WPA key. The AirCrack suite (or AirCrack NG as it's commonly referred) is a WEP and WPA key cracking program that captures network packets, analyzes them, and uses this data to crack the WPA key.

Getting ready

In order to perform the tasks of this recipe, experience with the Kali Linux terminal windows is required. A supported wireless card configured for packet injection will also be required. In the case of a wireless card, packet injection involves sending a packet, or injecting it onto an already established connection between two parties.

How to do it...

Let's begin the process of using AirCrack to crack a network session secured by WPA.

1. Open a terminal window and bring up a list of wireless network interfaces.

   airmon-ng

2. Under the interface column, select one of your interfaces. In this case, we will use `wlan0`. If you have a different interface, such as `mon0`, please substitute it at every location where `wlan0` is mentioned.
3. Next, we need to stop the `wlan0` interface and take it down.

   airmon-ng stop wlan0

   ifconfig wlan0 down

4. Next, we need to change the MAC address of our interface. In this case, we will use `00:11:22:33:44:55`.

   macchanger --mac 00:11:22:33:44:55 wlan0

5. Now we need to restart `airmon-ng`.

   airmon-ng start wlan0

6. Next, we will use `airodump` to locate the available wireless networks nearby.

   airodump-ng wlan0

7. A listing of available networks will begin to appear. Once you find the one you want to attack, press *Ctrl* + *C* to stop the search. Highlight the MAC address in the `BSSID` column, right-click, and select copy. Also, make note of the channel that the network is transmitting its signal upon. You will find this information in the `Channel` column. In this case, the channel is `10`.
8. Now we run `airodump` and copy the information for the selected BSSID to a file. We will utilize the following options:
   - `-c` allows us to select our channel. In this case, we use 10.
   - `-w` allows us to select the name of our file. In this case, we have chosen `wirelessattack`.
   - `-bssid` allows us to select our BSSID. In this case, we will paste `09:AC:90:AB:78` from the clipboard.

   airodump-ng -c 10 -w wirelessattack --bssid 09:AC:90:AB:78 wlan0

9. A new terminal window will open displaying the output from the previous command. Leave this window open.
10. Open another terminal window; to attempt to make an association, we will run `aireplay`, which has the following syntax: `aireplay-ng –dauth 1 –a [BSSID] –c [our chosen MAC address] [Interface]`. This process may take a few moments.

    ```
    Aireplay-ng --deauth 1 –a 09:AC:90:AB:78 –c 00:11:22:33:44:55
    wlan0
    ```

11. Finally, we run AirCrack to crack the WPA key. The `–w` option allows us to specify the location of our wordlist. We will use the `.cap` file that we named earlier. In this case, the file's name is `wirelessattack.cap`.

    ```
    Aircrack-ng –w ./wordlist.lst wirelessattack.cap
    ```

    That's it!

How it works...

In this recipe, we used the AirCrack suite to crack the WPA key of a wireless network. AirCrack is one of the most popular programs for cracking WPA. AirCrack works by gathering packets from a wireless connection over WPA and then brute-forcing passwords against the gathered data until a successful handshake is established. We began the recipe by starting AirCrack and selecting our desired interface. Next, we changed our MAC address which allowed us to change our identity on the network and then searched for available wireless networks to attack using `airodump`. Once we found the network we wanted to attack, we used `aireplay` to associate our machine with the MAC address of the wireless device we were attacking. We concluded by gathering some traffic and then brute forced the generated CAP file in order to get the wireless password.

Automating wireless network cracking

In this recipe we will use Gerix to automate a wireless network attack. Gerix is an automated GUI for AirCrack. Gerix comes installed by default on Kali Linux and will speed up your wireless network cracking efforts.

Getting ready

A supported wireless card configured for packet injection will be required to complete this recipe. In the case of a wireless card, packet injection involves sending a packet, or injecting it, onto an already established connection between two parties.

How to do it...

Let's begin the process of performing an automated wireless network crack with Gerix by downloading it.

1. Using `wget`, navigate to the following website to download Gerix.

   ```
   wget https://bitbucket.org/Skin36/gerix-wifi-cracker-pyqt4/
   downloads/gerix-wifi-cracker-master.rar
   ```

2. Once the file has been downloaded, we now need to extract the data from the RAR file.

   ```
   unrar x gerix-wifi-cracker-master.rar
   ```

3. Now, to keep things consistent, let's move the Gerix folder to the `/usr/share` directory with the other penetration testing tools.

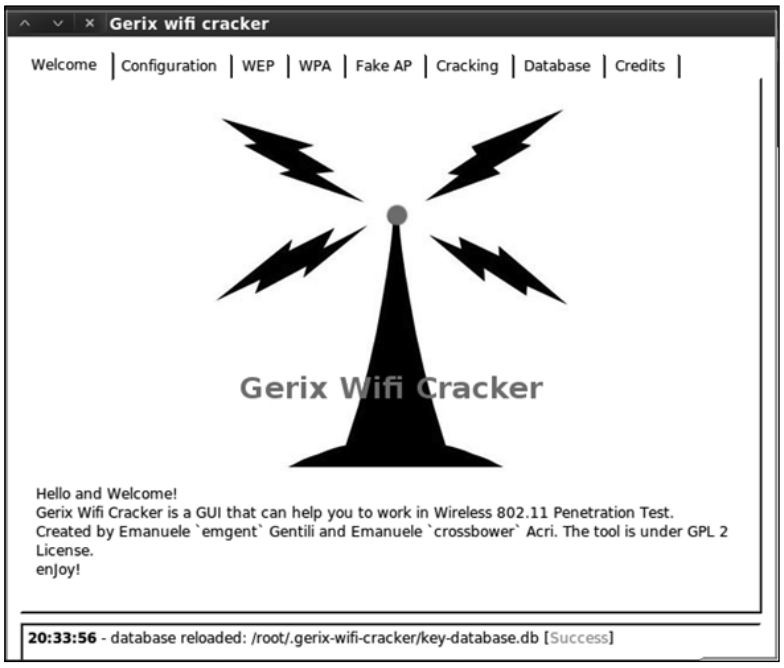
   ```
   mv gerix-wifi-cracker-master /usr/share/gerix-wifi-cracker
   ```

4. Let's navigate to the directory where Gerix is located.

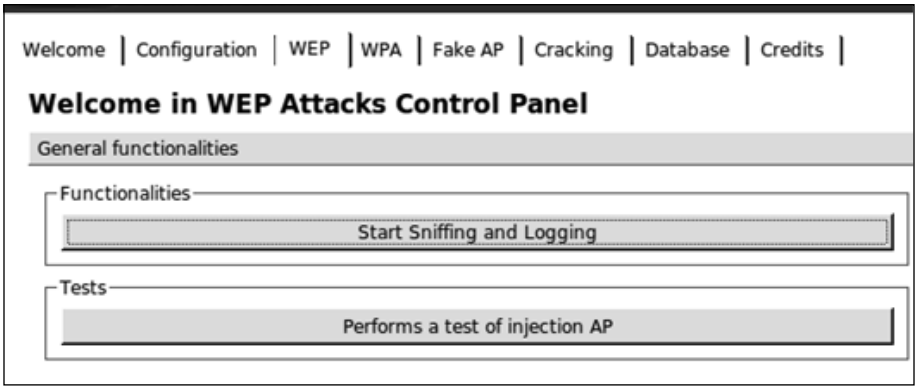
   ```
   cd /usr/share/gerix-wifi-cracker
   ```

5. To begin using Gerix, we issue the following command:

   ```
   python gerix.py
   ```



6. Click on the **Configuration** tab.
7. On the **Configuration** tab, select your wireless interface.
8. Click on the **Enable/Disable Monitor Mode** button.
9. Once Monitor mode has been enabled successfully, under **Select Target Network**, click on the **Rescan Networks** button.
10. The list of targeted networks will begin to fill. Select a wireless network to target. In this case, we select a WEP encrypted network.
11. Click on the **WEP** tab.



12. Under **Functionalities**, click on the **Start Sniffing and Logging** button.
13. Click on the subtab **WEP Attacks (No Client)**.
14. Click on the **Start false access point authentication on victim** button.
15. Click on the **Start the ChopChop attack** button.
16. In the terminal window that opens, answer **Y** to the **Use this packet** question.
17. Once completed, copy the `.cap` file generated.
18. Click on the **Create the ARP packet to be injected on the victim access point** button.
19. Click on the **Inject the created packet on victim access point** button.
20. In the terminal window that opens, answer **Y** to the **Use this packet** question.
21. Once you have gathered approximately 20,000 packets, click on the **Cracking** tab.
22. Click on the **Aircrack-ng – Decrypt WEP Password** button.

That's it!

How it works...

In this recipe, we used Gerix to automate a crack on a wireless network in order to obtain the WEP key. We began the recipe by launching Gerix and enabling the monitoring mode interface. Next, we selected our victim from a list of attack targets provided by Gerix. After we started sniffing the network traffic, we then used Chop Chop to generate the CAP file. We concluded the recipe by gathering 20,000 packets and brute-forced the CAP file with AirCrack.

With Gerix, we were able to automate the steps to crack a WEP key without having to manually type commands in a terminal window. This is an excellent way to quickly and efficiently break into a WEP secured network.

Accessing clients using a fake AP

In this recipe, we will use Gerix to create and set up a fake **access point** (**AP**). Setting up a fake access point gives us the ability to gather information on each of the computers that access it. People in this day and age will often sacrifice security for convenience. Connecting to an open wireless access point to send a quick e-mail or to quickly log into a social network is rather convenient. Gerix is an automated GUI for AirCrack.

Getting ready

A supported wireless card configured for packet injection will be required to complete this recipe. In the case of a wireless card, packet injection involves sending a packet, or injecting it onto an already established connection between two parties.

How to do it...

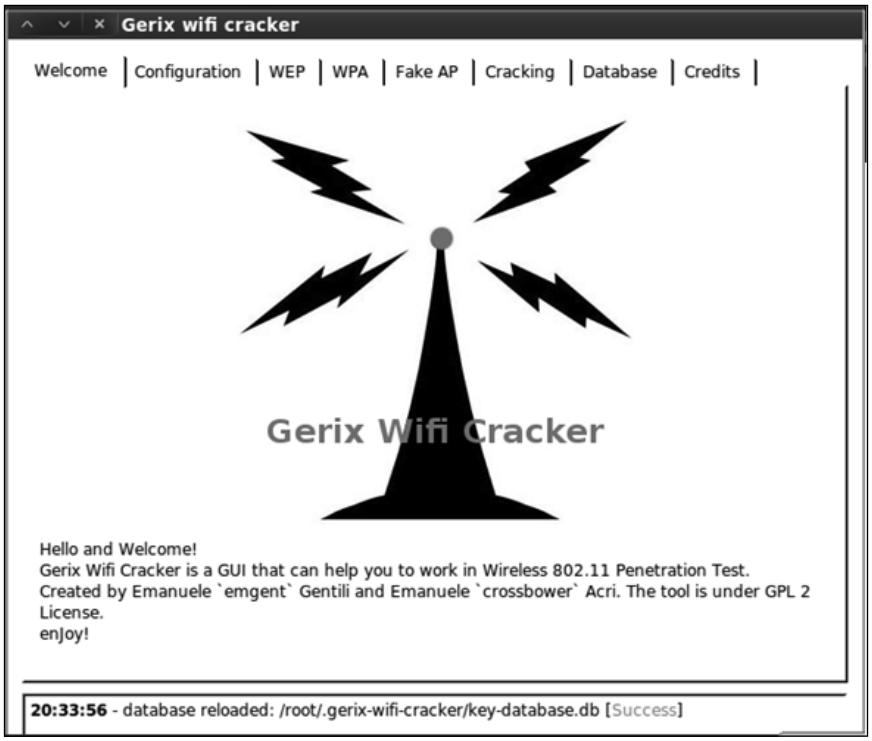
Let's begin the process of creating a fake AP with Gerix.

1. Let's navigate to the directory where Gerix is located:

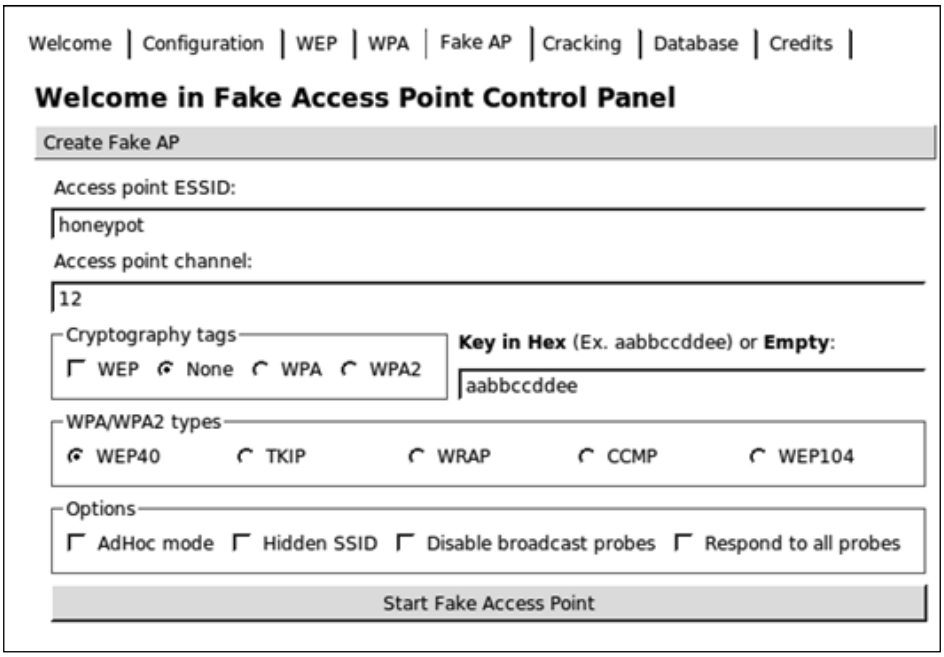
```
cd /usr/share/gerix-wifi-cracker
```

2. To begin using Gerix, we issue the following command:

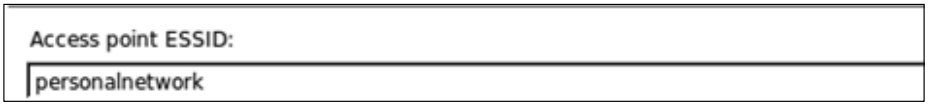
```
python gerix.py
```



3. Click on the **Configuration** tab.
4. On the **Configuration** tab, select your wireless interface.
5. Click on the **Enable/Disable Monitor Mode** button.
6. Once Monitor mode has been enabled successfully, under **Select Target Network**, press the **Rescan Networks** button.
7. The list of targeted networks will begin to fill. Select a wireless network to target. In this case, we select a WEP encrypted network.
8. Click on the **Fake AP** tab.



9. Change the **Access Point ESSID** from `honeypot` to something less suspicious. In this case, we are going to use `personalnetwork`.



10. We will use the defaults on each of the other options. To start the fake access point, click on the **Start Face Access Point** button.

That's it!

How it works...

In this recipe, we used Gerix to create a fake AP. Creating a fake AP is an excellent way of collecting information from unsuspecting users. The reason fake access points are a great tool to use is that to your victim, they appear to be a legitimate access point, thus making it trusted by the user. Using Gerix, we were able to automate the creation of setting up a fake access point in a few short clicks.

URL traffic manipulation

In this recipe, we will perform a URL traffic manipulation attack. URL traffic manipulation is very similar to a Man In The Middle attack, in that we will route traffic destined for the Internet to pass through our machine first. We will perform this attack through ARP poisoning. ARP poisoning is a technique that allows you to send spoofed ARP messages to a victim on the local network. We will execute this recipe using arpspoof.

How to do it...

Let's begin the process of URL traffic manipulation.

1. Open a terminal window and execute the following command to configure IP tables that will allow our machine to route traffic:

   ```
   sudo echo 1 >> /proc/sys/net/ipv4/ip_forward
   ```

2. Next, we launch arpspoof to poison traffic going from our victim's machine to the default gateway. In this example, we will use a Windows 7 machine on my local network with an address of `192.168.10.115`. Arpspoof has a couple of options that we will select and they include:

   - `-i` allows us to select our target interface. In this case, we will select `wlan0`.
   - `-t` allows us to specify our target.

   The syntax for completing this command is `arpspoof -i [interface] -t [target IP address] [destination IP address]`.

   ```
   sudo arpspoof -i wlan0 -t 192.168.10.115 192.168.10.1
   ```

3. Next, we will execute another arpspoof command that will take traffic from the destination in the previous command (which was the default gateway) and route that traffic back to our Kali machine. In this example our IP address is `192.168.10.110`.

   ```
   sudo arpspoof -i wlan0     -t 192.168.10.1 192.168.10.110
   ```

   That's it!

How it works...

In this recipe, we used ARP poisoning with arpspoof to manipulate traffic on our victim's machine to ultimately route back through our Kali Linux machine. Once traffic has been rerouted, there are other attacks that you can run against the victim, including recording their keystrokes, following websites they have visited, and much more!

Port redirection

In this recipe, we will use Kali to perform port redirection, also known as port forwarding or port mapping. Port redirection involves the process of accepting a packet destined for one port, say port 80, and redirecting its traffic to a different port, such as 8080. The benefits of being able to perform this type of attack are endless because with it you can redirect secure ports to unsecure ports, redirect traffic to a specific port on a specific device, and so on.

How to do it...

Let's begin the process of port redirection/forwarding.

1. Open a terminal window and execute the following command to configure IP tables that will allow our machine to route traffic:

   ```
   Sudo echo 1 >> /proc/sys/net/ipv4/ip_forward
   ```

2. Next, we launch arpspoof to poison traffic going to our default gateway. In this example, the IP address of our default gateway is `192.168.10.1`. Arpspoof has a couple of options that we will select and they include:

   - `-i` allows us to select our target interface. In this case, we will select `wlan0`.

   The syntax for completing this command is `arpspoof -i [interface] [destination IP address]`.

   ```
   sudo arpspoof -i wlan0 192.168.10.1
   ```

3. Next, we will execute another arpspoof command that will take traffic from our destination in the previous command (which was the default gateway) and route that traffic back to our Kali Linux machine. In this example our IP address is `192.168.10.110`.

   ```
   iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
   REDIRECT --to-port 8080
   ```

   That's it!

How it works...

In this recipe, we used ARP poisoning with arpspoof and IPTables routing to manipulate traffic on our network destined for port 80 to be redirected to port 8080. The benefits of being able to perform this type of attack are endless because with it you can redirect secure ports to unsecure ports, redirect traffic to a specific port on a specific device, and so on.

Sniffing network traffic

In this recipe, we will examine the process of sniffing network traffic. Sniffing network traffic involves the process of intercepting network packets, analyzing it, and then decoding the traffic (if necessary) displaying the information contained within the packet. Sniffing traffic is particularly useful in gathering information from a target, because depending on the websites visited, you will be able to see the URLs visited, usernames, passwords, and other details that you can use against them.

We will use Ettercap for this recipe, but you could also use Wireshark. For demonstration purposes, Ettercap is a lot easier to understand and apply sniffing principles. Once an understanding of the sniffing process is established, Wireshark can be utilized to provide more detailed analysis.

Getting ready

A wireless card configured for packet injection is required to complete this recipe although you can perform the same steps over a wired network. In case of a wireless card, packet injection involves sending a packet, or injecting it, onto an already established connection between two parties.

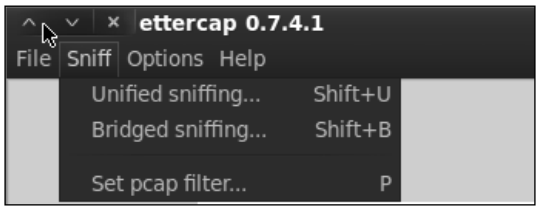
How to do it...

Let's begin the process of sniffing network traffic by launching Ettercap.

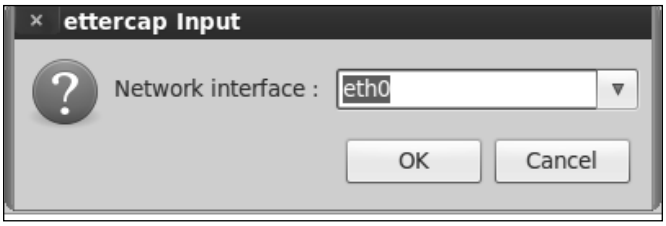
1. Open a terminal window and start Ettercap. Using the `-G` option, launch the GUI:

```
ettercap -G
```

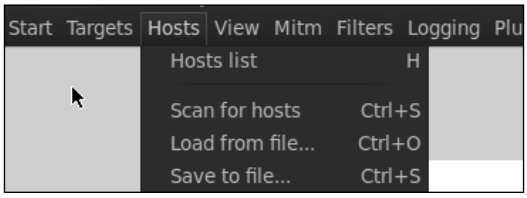
2. We begin the process by turning on **Unified sniffing**. You can press *Shift + U* or use the menu and navigate to **Sniff** | **Unified sniffing**.



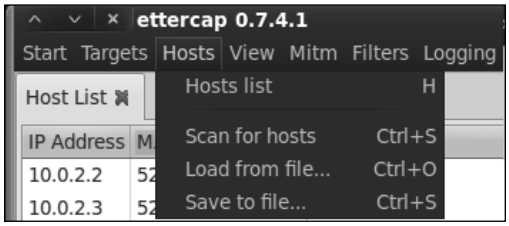
3. Select the network interface. In case of using a MITM attack, we should select our wireless interface.



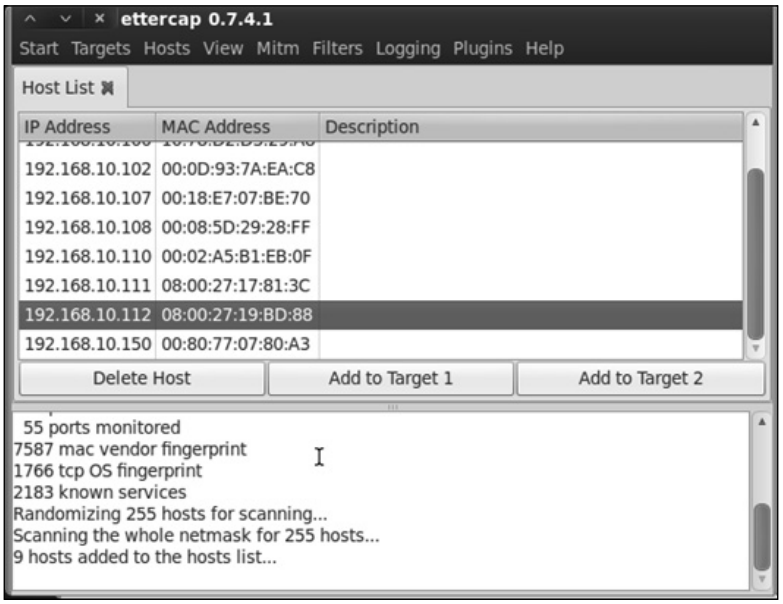
4. Next, we turn on **Scan for hosts**. This can be accomplished by pressing *Ctrl* + S or use the menu and navigate to **Hosts** | **Scan for hosts**.



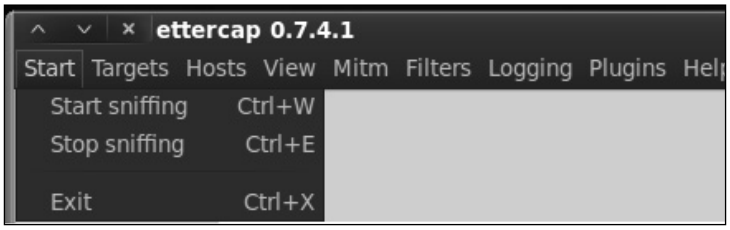
5. Next, we bring up the **Host List**. You can either press *H* or use the menu and navigate to **Hosts** | **Host List**.



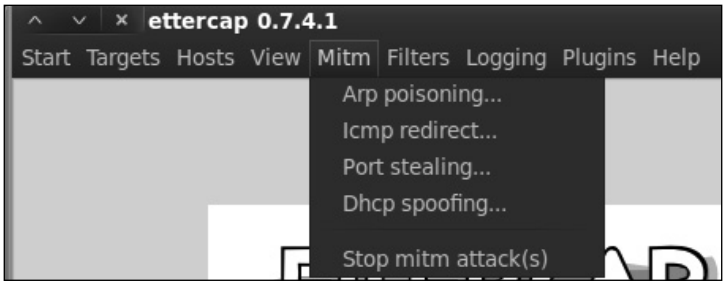
6. We next need to select and set our targets. In our case, we will select `192.168.10.111` as our Target 1 by highlighting its IP address and pressing the **Add To Target 1** button.



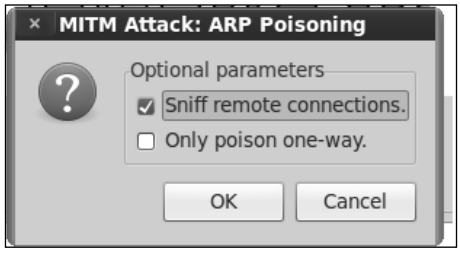
7. Now we are able to allow Ettercap to begin sniffing. You can either press *Ctrl + W* or use the menu and navigate to **Start | Start sniffing**.



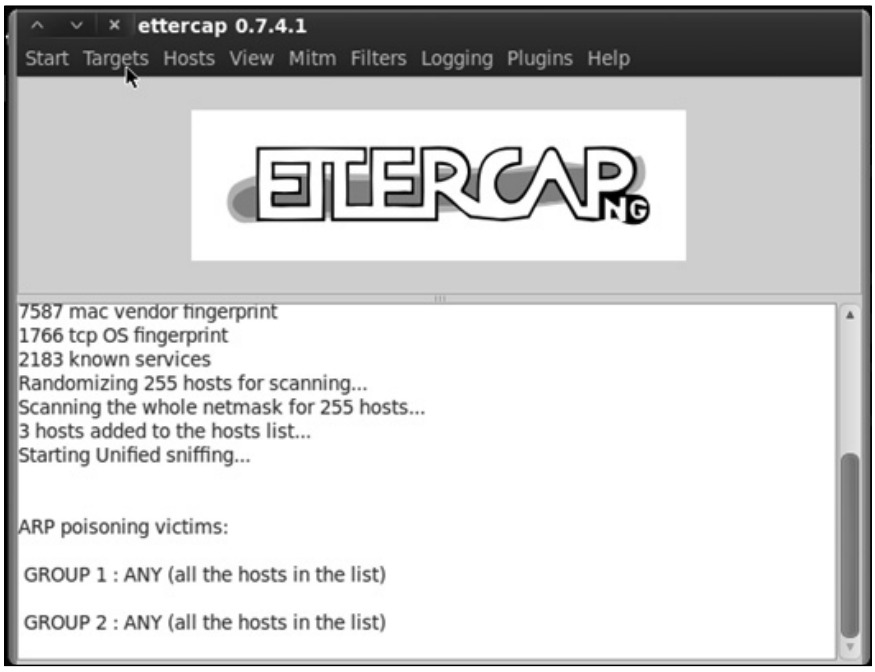
8. Finally, we begin the ARP poisoning process. From the menu, navigate to **Mitm | Arp poisoning...**.



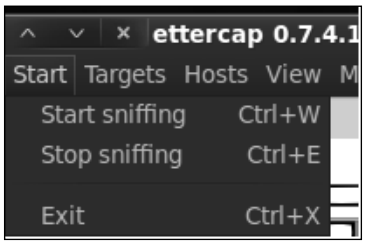
9. In the window that appears, check the optional parameter for **Sniff remote connections**.



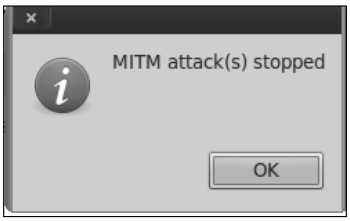
10. Depending on the network traffic, we will begin to see information.



11. Once we have found what we are looking for (usernames and passwords). We will turn off Ettercap. You can do this by either pressing *Ctrl + E* or by using the menu and navigating to **Start** | **Stop sniffing**.



12. Now we need to turn off ARP poisoning and return the network to normal.



How it works...

This recipe included an MITM attack that works by using ARP packet poisoning to eavesdrop on wireless communications transmitted by a user. We began the recipe by launching Ettercap and scanning for our hosts. We then began the process of ARP poisoning the network. ARP poisoning is a technique that allows you to send spoofed ARP messages to a victim on the local network.

We concluded the recipe by starting the packet sniffer and demonstrated a way to stop ARP poisoning and return the network back to normal. This step is key in the detection process as it allows you to not leave the network down once you have stopped poisoning the network.

This process is useful for gathering information as it's being transmitted across the wireless network. Depending on the traffic, you will be able to gather usernames, passwords, bank account details, and other information your targets send across the network. This information can also be used as a springboard for larger attacks.

Where to buy this book

You can buy Kali Linux Cookbook from the Packt Publishing website:
`http://www.packtpub.com/kali-linux-cookbook/book`.

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

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

www.PacktPub.com

For More Information:
www.packtpub.com/kali-linux-cookbook/book