
HOW TO
HACK WIFI

(NOTE: If you are using a virtual lab to run your attacks you will need an external Wi-Fi attachment. The other option is to have a direct install on your computer. Virtual labs cannot access your wireless card directly.)

Wireless technology has become a staple of our modern society. It seems that everywhere you go you can find a wireless network. Though mobile devices that connect to cell towers are quickly becoming the norm, people still find value in local wireless networks to connect their laptops, tablets, and smartphones to the Internet. Many times a wireless network is faster than a mobile device network, and transmitting data via a Wi-Fi hotspot is more favorable because it doesn't affect a mobile user's data plan.

Because wireless networks are so popular, the IEEE has done a lot to ensure that wireless networks remain secure. We have seen dramatic improvements in wireless security technologies over the years, but some of the older standards are extremely flawed. When they first came out, the older technologies were secure enough. But as time moved forward, people found ways to crack wireless encryption standards – making these older technologies worthless.

You might be thinking that if these old technologies are so easily cracked that people would stop using them. However, that just simply isn't true for a variety of reasons. The biggest reason is that of pure ignorance. How many people want to take the time to research the technology they are using? Not many. Unless an individual has an Interest in I.T. or security, they are more often than not bored to tears with the various security standards.

This couldn't be truer in home environments and consumer scenarios. The vast majority of people don't understand how to lock down their SOHO router – which almost always comes with wireless capabilities these days – and they fail to implement strong security protocols. If that weren't bad enough, some people even leave the username and password for their wireless router set to its default settings. Either configuration mistake makes it extremely easy for an attacker to gain access to the network to conduct penetration testing and foot-printing.

This may not sound like a big problem at first. After all, in a home environment, the only people that could threaten your network are your immediate neighbors since they are the only ones in range of the wireless signal, right? Unfortunately, that is not the case. Some attackers engage in the practice of war-driving, whereby they drive around in their automobile with a laptop or scanner and actively seek out wireless networks to crack. After gaining access to the wireless network, there's no telling what kind of data they could capture. They might choose to perform a man-in-the-middle attack to intercept all communications before it is sent to its intended host. This would allow an attacker to capture sensitive information such as security keys, credit card numbers, and a whole host of other personal information.

But take a moment and consider what this could mean in a corporate environment. Sometimes, but not always, corporations create a security policy that prevents users from adding networking devices to Ethernet ports in their office. However, in many corporations, they either don't have this security policy or it isn't implemented or stringently enforced. An employee who lacks advanced knowledge of network security could run down to their local electronics retailer, purchase a SOHO wireless router, and connect it to their corporate

network. If they fail to use a secure wireless protocol, they are giving attackers a foothold into their corporate network. After an attacker has successfully cracked the insecure wireless protocol, they will have access to the local LAN and who knows what other network services. Then the attacker can begin employing reconnaissance techniques, such as using NMAP to feel out the local network.

The bottom line is this: whether in a home or office setting, weak wireless security provides hackers with a veritable digital gold mine of information. If you are interested in network penetration testing, you should at least know the different wireless standards and which ones are insecure.

Wireless Security Algorithms

There are at least 3 wireless security algorithms that you need to know: WEP, WPA, and WPA2. They were all created at different times, and each one attempted to improve upon the older standard.

WEP, or Wired Equivalent Privacy, is anything but secure. As the oldest of the three algorithms, it provides an attacker with the greatest opportunity to penetrate a network. However, it is still widely implemented due to how old it is, backwards compatibility purposes, and because it usually is the first security algorithm on the list in drop down menus on wireless devices.

This algorithm is really quite old, and it was created in 1999 (16 years ago). Even when this algorithm was released for use, it wasn't especially strong. It was limited to 64-bit encryption due to government regulations on cryptography. Eventually the regulations were changed to allow 128-bit encryption. 256-bit WEP encryption was created, but 128-bit encryption is the most used implementation.

To no avail, a lot of work was done to make this algorithm more secure. Many security flaws were discovered, and as time moved forward, hardware resources and processing power increased exponentially which made it that much easier to take advantage of exploits. In fact, the FBI showed a public case study whereby they were able to crack WEP in a matter of mere minutes.

The WPA Standard

Next WPA (Wi-Fi Protected Access) was introduced to combat the shortcomings of WEP. In 2003, WPA was made into a standard. At the time, 256-bit PSKs (Pre-Shared Keys) were used to make it much more secure than the 64-bit and 128-bit WEP security standards. There were many additions to the WPA algorithm to improve on WEP such as TKIP (Temporal Key Integrity Protocol), integrity checking algorithms, and a per-packet checking algorithm. Eventually, TKIP would be replaced by AES (Advanced Encryption Standard).

Though the WPA standard provided massive improvements over WEP, it was still flawed. Portions of the code, such as TKIP, essentially reused portions of the algorithm from WEP. Eventually these flaws and vulnerabilities were discovered and WPA was also exploited.

Interestingly enough, most of the attacks that are performed to take advantage of the vulnerabilities are not performed by attacking the WPA algorithm directly. Though there

are certainly exploits that can be performed by directly attacking WPA. Instead, many attackers take advantage of code that was meant to augment WPA – a system called WPS (Wi-Fi Protected Setup).

The WPA2 Standard

As the newest of the three wireless security standards, WPA2 (Wi-Fi Protected Access 2) offers the most security. The standard is not perfect, but it is vastly more secure than its predecessors. One reason it is so much stronger is due to the requirement to use AES exclusively instead of giving the option for TKIP and other outdated algorithms.

The largest vulnerability with standard doesn't even apply to home environments. Instead, it can really only be used in corporate settings. The exploit requires that the hacker already has access to the wireless network before the hacker can obtain specific keys and then use the keys to attack other network devices. This vulnerability is extremely specific and doesn't apply to the vast majority of WPA2 implementations. So, to sum up WPA2's vulnerability, it does have an exploit but it really isn't applicable to most environments.

However, though not directly related to WPA2, the same WPS vulnerability contained in WPA is also applicable to WPA2. It is pretty difficult to exploit and takes a fair amount of time, though. It can take anywhere from a couple hours up to about 14 hours, and it only works if WPS is enabled.

Cracking WEP

Ok, so now it is time for the good stuff. To actually crack WEP, we are going to run our demo in the Kali Linux environment. To follow along, I would recommend that you download a Kali image and install it on a virtual machine if you haven't done so already. If aircrack-ng isn't already installed on your Linux operating system, we will need to install it to begin. The application is only about 6 megabytes, so it hardly takes up any disk space. Use the following command to install aircrack-ng:

- apt-get install aircrack-ng

```
root@kali:/opt/metasploit-framework# apt-get install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  ieee-data libiw30 wireless-tools
The following NEW packages will be installed:
  aircrack-ng ieee-data libiw30 wireless-tools
0 upgraded, 4 newly installed, 0 to remove and 1 not upgraded.
Need to get 2,181 kB of archives.
After this operation, 6,194 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://http.kali.org/kali/ kali/main libiw30 i386 30~pre9-8 [37.2 kB]
Get:2 http://http.kali.org/kali/ kali/main wireless-tools i386 30~pre9-8 [133 kB
]
Get:3 http://http.kali.org/kali/ kali/main aircrack-ng i386 1:1.2-0~rc2-0kali3 [
815 kB]
Get:4 http://http.kali.org/kali/ kali/main ieee-data all 20141019.1kali1 [1,196
kB]
Fetched 2,181 kB in 6s (342 kB/s)
Selecting previously unselected package libiw30:i386.
(Reading database ... 151860 files and directories currently installed.)
Unpacking libiw30:i386 (from .../libiw30 30~pre9-8 i386.deb) ...
```

During the installation process, a prompt will ask you if you want to continue. Just enter a "Y" and proceed with the installation. Now we will want to run the software to listen to wireless data on a specific interface. To see a list of available interfaces, use the **ifconfig** command. Locate your wireless interface, and run the following command:

- airmon-ng start [INTERFACE NAME]

```
root@kali:~# airmon-ng start wlan0
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
 2896 NetworkManager
 3569 dhclient
```

There may be some background processes that will cause a conflict. Depending on which processes they are, you may want to kill them before proceeding. In addition, there is the possibility that the command will fail because you are missing the dependency named **ethtools**. If you encounter this problem, just run the following command before attempting to start listening on your wireless interface:

- apt-get install ethtool

Now try to run the airmon-ng command again. The name of your interface is most likely wlan0, but there can be some issues getting it to appear in the virtual machine. If you are

using VMWare Player, you will need to make sure that you browse to Player > Manage > Virtual Machine Settings. From here, you can place the network adapter in bridged mode as well as add your wireless chipset to the virtual machine. After running the airmon-ng command, it should return with process IDs.

After it has had a chance to gather some wireless network traffic, you are going to want to perform a dump. You do this with the following command:

- airodump-ng mon0

Please note that the name of the interface you are performing the dump on could be different that mon0. You will see this information after you run the airmon-ng [INTERFACE] command. After the dump, you should see a lot of hex code and SSID information. Not only will you be able to see the various wireless networks in your area, but you will also see a list of which ones are using WEP encryption. You will want to wait a little longer until the SSID you want to crack has about 10,000 to 15,000 packets stored. Then you will want to enter the following command to actually crack WEP:

- airodump-ng –w [ESSID] –c [CHANNEL] –bssid [BSSID] [INTERFACE NAME]

You will need to plug in the appropriate values that you gathered from the data dump performed earlier. Take note of the "-c" argument, though. This specifies the numeric value of a channel the wireless network is operating on. This can be found under the "CH" column.

Finally, you should receive a message that confirms the key was found and spit out some hex code as well as ASCII text values.

Cracking WPA

In order to crack WPA, the process is very similar. You need the same software running inside of Kali. There are a few differences to cracking WPA because it is a different algorithm, but you need to start capturing packets and monitoring your wireless interface just like we did with WEP.

After you perform the airodump command, though, things are a little different. This time, you need to select a Wi-Fi network that is using WPA. Then, you need to run the following command:

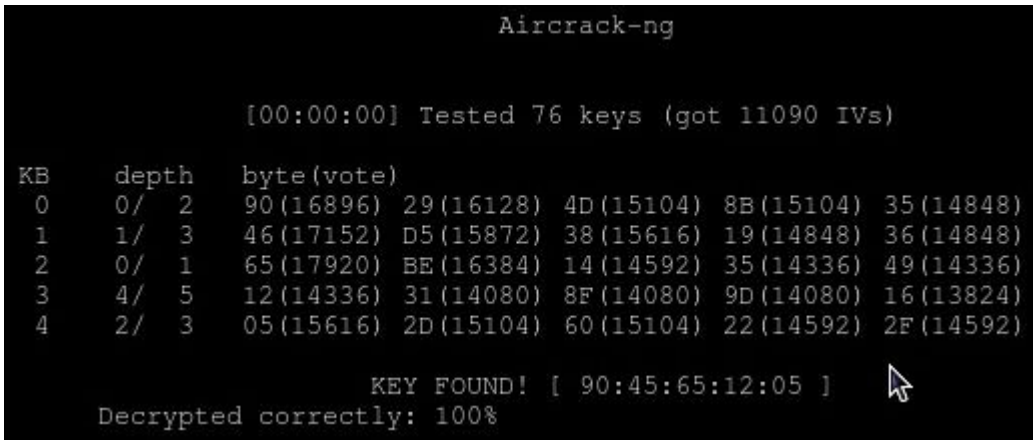
- airodump-ng -c [CHANNEL] –bssid [BSSID] -w /root/Desktop/ mon0

This part is also different, because the exploit is dependent upon another device connecting or reconnecting to the target wireless network. The above command will monitor the network waiting for a connection attempt to be made by another party. This will cause the wireless device to perform a specific handshake that needs to be captured to crack WPA. Once a client does attempt to connect, you will see output that confirms the attempt with text that says "WPA Handshake" followed by hex code. Now that the handshake has been captured, we can begin the process of actually cracking WPA.

Run the following command to crack WPA:

- aircrack-ng –a2 –b [HANDSHAKE HEX CODE] –w /root/wpa.txt /root/Desktop/*.cap

The process should complete by providing you with the network key. Understand though, that this really doesn't *crack* WPA. Instead, it performs a dictionary based attack that attempts to connect with many different passwords. The only drawback to this procedure is that the process will fail if you can't capture a handshake or if the password isn't contained within the dictionary.



In Summary

Wireless networks are unbelievably easy to crack. Using the processes listed above, you could have access to a WEP or WPA protected network in a matter of minutes. Attackers are well aware of these exploits, and the software makes the process mostly automatic. Not only are home users at risk to these types of attacks, but unsecure corporate networks can also be victimized.