**Vulnerabilities of wireless hotspots**

This study examines the lack of security surrounding wireless hotspots. In this study I will make reference to the risks of connecting to unsecure hotspots, the consequences of doing so, and security measures that can be implemented to reduce the risk of private information being stolen as a result of poor/no security. I will also provide examples of how hackers can take advantage of this lack of security for personal game, and show how it can often be detrimental to the victim. This will be the basis of my practical section.

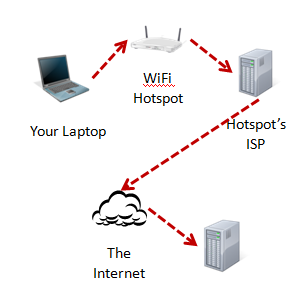
Firstly I will define exactly what a hot spot is. As defined by Webopedia, a hotspot is “an area where an access point provides public wireless broadband network services to mobile visitors through a Wlan” . (Webopedia definition). Note that even a home network is a hotspot. If a home router is not password protected, it is essentially also a hotspot.

Throughout this study, I will make reference to hackers and the ways in which they exploit unsecure connections in order to perform malicious attacks on unsuspecting victims. These attacks include Denial of Service attacks, man in the middle attacks and general illegal phishing activities, all of which will be discussed in more detail.

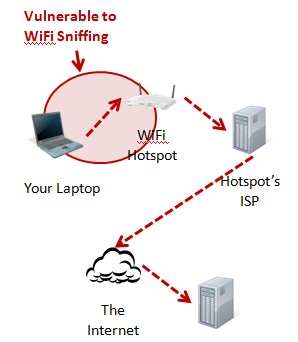
**Intro**

Each day thousands of people connect to hotspots around the world, be it in an airport, coffee shop, on a bus or train. The establishment of such a service is meant to serve as both a convenience to the user and as an incentive for people to choose an establishment over another competitor. However the lack of encryption associated with these hot spots often leaves the user susceptible to attacks, in turn, leaving them vulnerable to hackers attempting to acquire sensitive information.

**How a hot spot connection is established**

****

The image above portrays the standard way in which a connection to the internet is established at an **unsecure** wireless hot spot. The dotted lines represent unencrypted and thus, unsecure connections. <http://ask-leo.com/how_does_a_vpn_protect_me.html> . When this hierarchy is in place, the user is most vulnerable. If a hacker were to use sniffing software such as Back Track 5, NetCut, or NetTools, packets could be intercepted while they are being sent to the router.



The highlighted area shows where packet sniffing is most likely to occur. At this stage, all that is required for the hacker to sniff packets, is a connection to the same network as the victim.

**Examples of poor Wi-Fi security**

**USE PHONE AS A HOT SPOT**

Using a PS3 it was possible to connect to someone’s Sony phone a few doors down, and browse their gallery.

**Practical – Steps taken**

My aim for this project is to expose the vulnerability of someone who is connected to an unsecure hotspot. I will pose as the hacker and attempt to phish information from another person. I want to expose the poor security and expose how simple it is to acquire someone’s private information.

In order to do this, I had to install a virtual operating system. I choose to install Linux as it is supports Backtrack 5.

**What is Back Track 5?**

Back track 5 is a security testing software that allows you to access and monitor other peoples computers.

**What is a VPN?**

A VPN is essentially a private network that can be accessed by the user no matter where the user is situated, even if the user is accessing via a wireless hotspot. If I was to establish a VPN server it would be accessible from any hotspot around the world. All that is needed is an internet connection.

**How does VPN work and how does it protect me at a wireless hotspot?**

Built into the networking of computers is a protocol that allows for the implementation of VPN’s. This protocol is called Point to Point Tunnelling Protocol (PTPP). PTPP allows for a connection to be made between the user’s computer and the VPN server. The VPN then assigns an IP address to the users device once the connection is made. OpenVPN (SSL) is basically the same, just you use software that was developed and free to download at[http://openvpn.net](http://openvpn.net/) It's also more secure but a bit slower sometimes, or faster. It all depends on your ISP and how their network is. GET MORE INFO ON THIS

After the user has been connected, all traffic is then encrypted as opposed to when a VPN is not used and traffic is unencrypted (see diagram). The user may choose to increase the level of security by increasing their encryption level. The standard level of encryption is set to 128 by default, however levels vary from 0 – 2048 bits. The user is now safe to access the internet from the unsecure hot spot as they have their own form of security in place. The user is not restricted to using just the one device. The user can connect via laptop, Mac, phone etc,

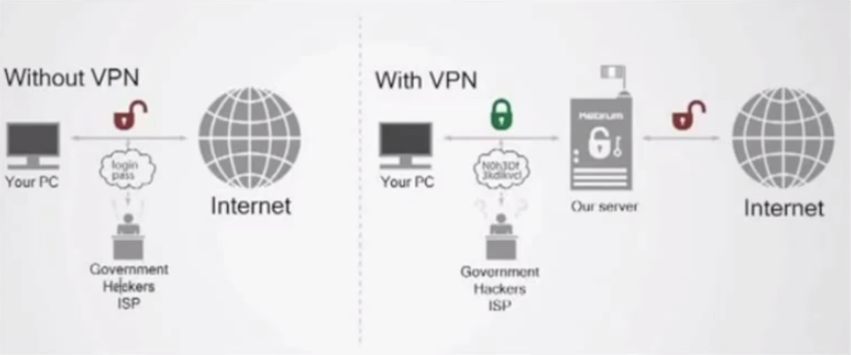
You can connect to your VPN server from all around the world, with any ISP. You just need a internet connection. You can also setup one account on as mny devices as you want...If you would set up the VPN on a router on your home network, all devices connected to the router would be covered by the VPN encryption.

How a VPN works - basically it's a built into the networking of your computer (PPTP) and allows for an encrypted connection between you and our VPN server. Once you connect you will have the IP that the VPN server assigns you. After this, sites that might be blocked are now unblocked since you are on a private encrypted network tunnel.   
OpenVPN (SSL) is basically the same, just you use software that was developed and free to download at[http://openvpn.net](http://openvpn.net/) It's also more secure but a bit slower sometimes, or faster. It all depends on your ISP and how their network is.

That's correct, once you're connected through a hotspot all your traffic is encrypted and more secure than w/o VPN. There are different encryption levels from 0 encryption up to 2048 bits. (128 bits by default, what is usually high enough

You can connect with any devices, mac, PC etc. you won't need to set it on a specific mac adress. The VPN connection itself is covererd by pdw itself.

**How can a VPN increase my personal security?**



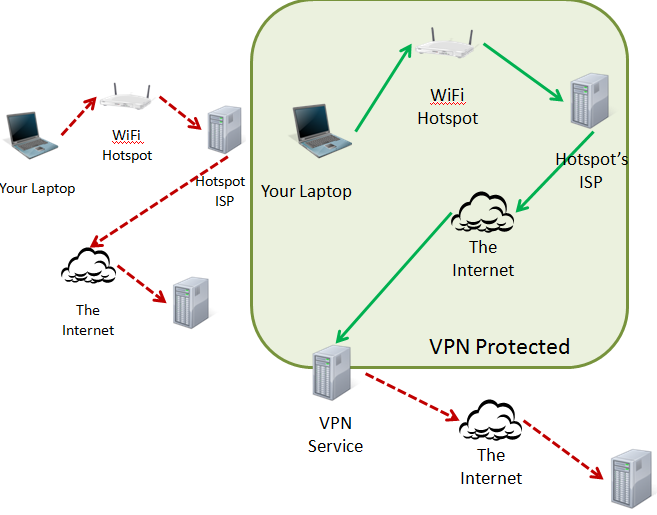
<http://www.youtube.com/watch?v=KFODy-dHcU8>

Here we can see the difference in security levels between a network supporting VPN and a network not supporting VPN. Without a VPN server in place, packets are not encrypted before they reach the web. This leaves users susceptible to having delicate personal information accessed and possibly stolen. ISP’s are free to view this information and can record any sites that are visited, and downloads that have been made.

When using a Virtual Private Network, any information your device sends out is encrypted, so if you are accessing the internet via a wireless hotspot, your outgoing packets are encrypted and thus not interpretable by hackers or ISP’s. The information is sent to the VPN server, where it is decrypted and then sent to its respective destination.

So if a person chooses to access the internet via a wireless hotspot, it is advisable that they do so only if they are accessing the internet via a VPN in order to encrypt their data, keeping if from being accessed by hackers and unwanted parties.

So let’s compare the diagrams for an unsecure wireless hotspot connection and a unsecure connection where the user has established a connection to the VPN server.



The VPN provides almost an optimal level of protection for the user. The hacker never sees the laptops IP as it is assigned an IP by the VPN server. Packets cannot be sniffed by sniffing software as the connections are encrypted.

**Using netcut**

Netcut is a free software that allows the user to monitor who is connected to a network. Ideally the following example would take place in a public environment such as a café or airport, but for the purpose of this exercise, I will use 3 laptops I have at my disposal and assume that my home network is a public hotspot we have all connected to without the need for any password verification.



The hacker runs Netcut and gets a list of IP’s connected to the public hotspot. The hacker is now aware of the two devices.

INSERT NETCUT2 FROM DEANS LAPTOP

From simply being allowed to connect to the same network as the victims, the hacker now has access to both their IP and MAC addresses. At this point, all laptops have a connection to the internet. The Netcut software allows the hacker to, with minimal effort, disconnect any user from the network. To do this, simply highlight which victim you wish to disconnect from the network, then that user will be instantly disconnected.

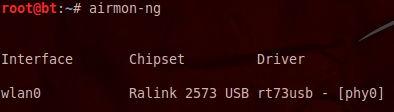
This is just an example of how by connecting to an unsecure network, your device is instantly vulnerable. I understand that the implications of being disconnected from a public hotspot are minimal, this example is just to highlight how a simple free software can empower hackers.

**Practical**

The goal of this project is to examine the vulnerabilities of unsecure wireless hotspots. In order to do this I attempted to create a DNS server in order to retrieve packets being sent by an unsuspecting victim and to then examine the packets in order to retrieve sensitive information.

The first step was to download Virtual Box in order to allow me to run Backtrack 5. After I installed the necessary software, I used “route –n” to see what other devices were connected to the network. Unfortunately the table entry was empty as no connection to the internet. After trying several ways to connect, such as downloading winPcap, I could get nothing to work.

Eventually I discovered that in order to be able to get a wireless connection it is necessary to use a USB adapter, so after getting a Belkin external wireless adapter and selecting it via Back Track, I was then able to get a connection established. From this, I learned that Virtual machines don’t recognise built in wireless adapters as independent functioning adapters and so they create a bridge and creates a virtual network adapter that runs off the already built in adapter.

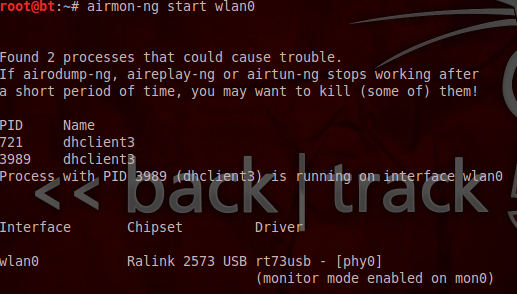


The next thing to do is to activate monitoring mode on the on the wireless card. <http://www.exploit-db.com/wp-content/themes/exploit/docs/20875.pdf>

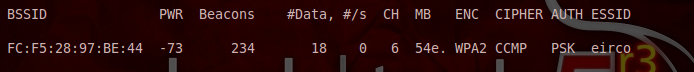
**Why is it necessary to put the card in monitor mode?**

When a wireless card is in monitoring mode, it actively listens for packets without being directly associated with a network.

To put the card in wireless mode, I used the following format *airmon –ng start wlan0.*We can see that a new interface has become active. This interface supports monitor mode.



After putting the card into listening mode, the next step is to listen for activity on nearby networks. By entering airodump-ng mon0, the selected interface begins listening to traffic across networks.



In the screenshot above we can see the active eircom network.



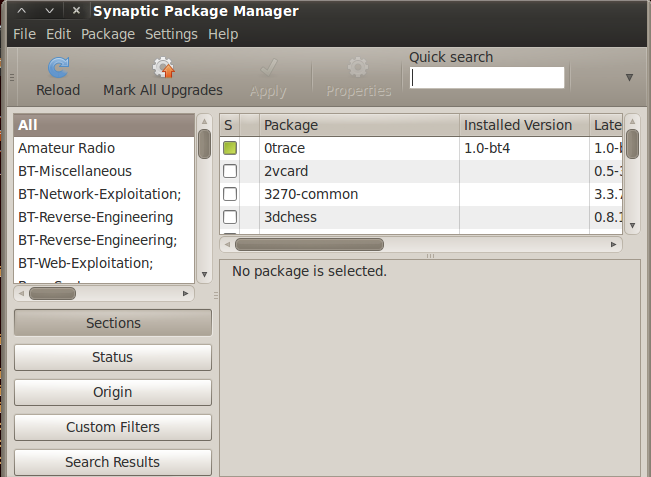
In the screenshot above, we can see the users connected to the network. After cross referencing the MAC addresses, I can confirm that the addresses match those of the three laptops being used for this practical. At this stage the wireless card is in monitor mode and is actively listening to packets being sent across the network.

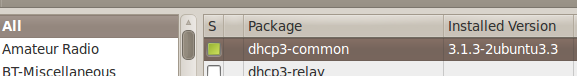
The next step was to install Synaptic, which is a management program that allows for the customization of packages and programs through a GUI interface. <http://www.nongnu.org/synaptic/> That would allow me configure (install) the relevant files. Entering the command “*apt-get install synaptic* “installs the files necessary to create a server. It also uninstalls unnecessary default files that are preconfigured.

**(extract)

<http://backtrack4beginners.blogspot.ie/2012/09/3-installing-dhcp3-server.html>

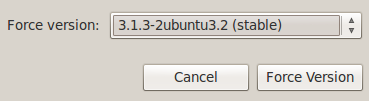
After the relevant files are downloaded, inputting “synaptic” will open the synaptic package manager. The Synaptic Package Manager is a package management program that allows the user to customise packages and programs within the system through a GUI interface. The interface is pictured below.



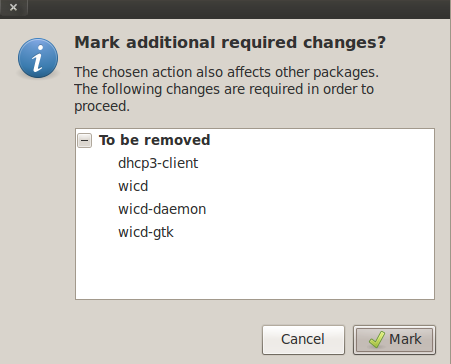


<http://backtrack4beginners.blogspot.ie/2012/09/3-installing-dhcp3-server.html>

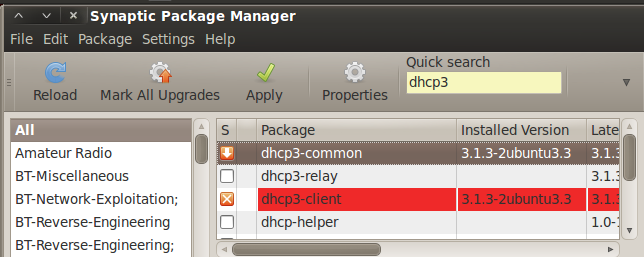
I then selected the dhcp common package and selected “force version” from the package tab.

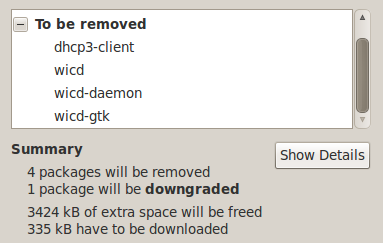


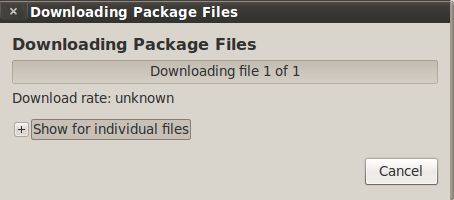
After forcing the version, a window appears that lists the files that will be removed.



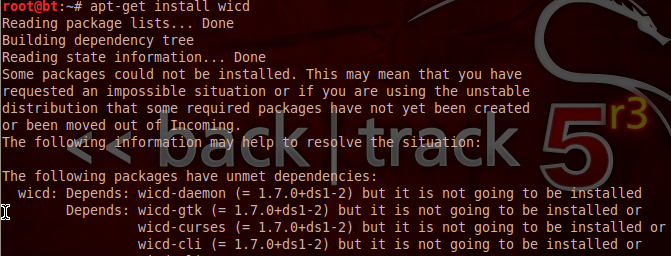
Note how upon returning to the package manager screen, the dhcp-client is no longer active.



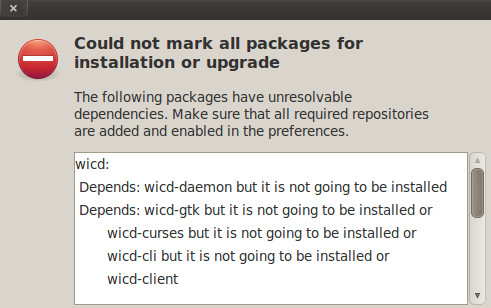




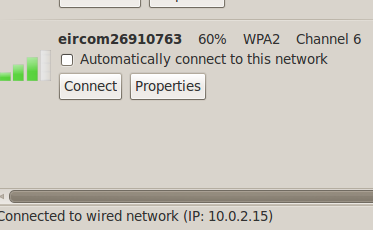
**Error Message**



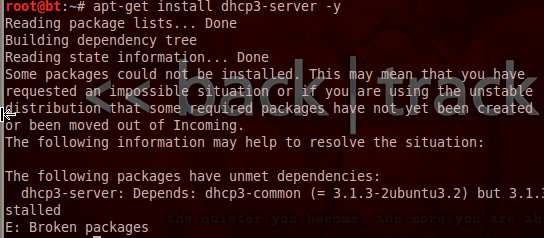
While following the steps to install the DHCP server, I encountered a problem when trying to install WICD. To try resolve this problem, I installed the wicd and wicd-daemon packages.



After backtrack was successfully installed, I repeated the steps up to and including using the airodump command to monitor the network. I then accessed the Application tab on the back track desktop and followed the path Application > Internet > Wicd Network Manager, which unlike before, was now available. After opening the Wicd Network Manager, I specified opened the preferences section and entered the name of my wireless connection, wlan0. After scanning for wireless connections, my eircom connection was eventually detected.

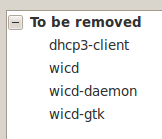


After returning to the command terminal and entering the code to establish a dhcp server, I onec again received an error message, telling me the attempt was unsuccessful.



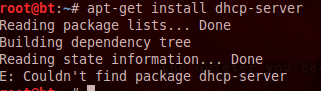
After re-entering the code to install the Synaptic Manager, after I force install the desired version of Ubuntu (the one to satisfy the dependency in the screenshot above) one of my files appears different to the instructions I am following.

The instructions suggest that the files being removed are to be dhcp3-common, dhcp3-gtk, dhcp3-daemon, and also Wicd. Whereas when I follow the instructions, the files that are selected are as follows



Note how the dhcp3-common file is not selected, and instead a dhcp3-client is selected.

After noting the difference in file names I cancelled the operation and instead returned to the terminal and tried the command apt-get install dhcp3-server, but it was unsuccessful as it could not find the server package.



The unmarking of the dhcp-client file was not permitted, and so after it was deleted I used the command apt get install-dhcp-client to reinstall the client.

I then checked a forum and was informed of the command to search for a package.

<http://forums.debian.net/viewtopic.php?p=13867>

And so I used the “apt-cache search dhcp client” command which brought up a list of results.



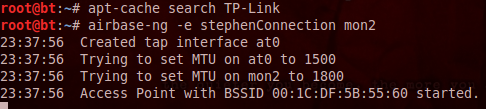
After searching the results, I saw the package “dhcp3-server” command and so I entered “apt-get install dhcp3-server” and the server was, at last created.

So after getting the server up and running, I then restarted my wireless interface.

So the next step was to configure the dhcp server to allow networking. After checking the network address (10.0.2.0), and calculating the relevant fields, ie range and broadcast addresses. I created a a dhcpd.conf file.

INSERT IMAGE

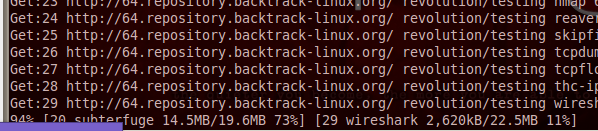
Then I made the fake access point which I should have called eircom but for this I called it stephensConnection



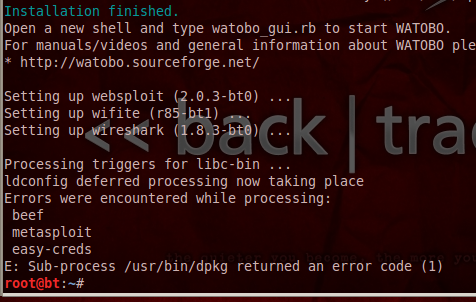
Then had to create a fakeDNS TO SET UP FAKE DNS SERVER

<http://www.darkoperator.com/installing-metasploit-in-ubunt/>

This website taught me about metasploiT. I then followed the steps to get the most up to date version so I could create a fake DNS server



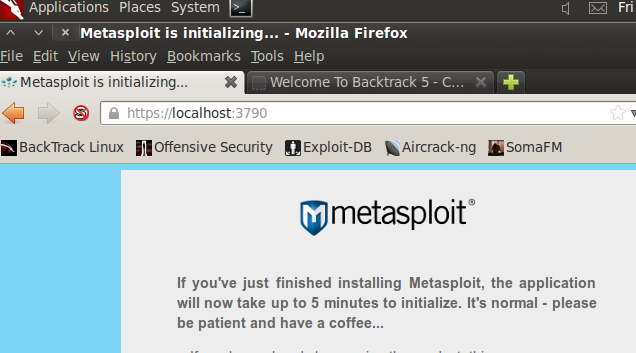
The purpose of updating was to allow me to install the latest version of metasploit. The goal was to import the metasploit auxillary package fakeDNS, in order to create a fake DNS. After about forty minutes, the installastion finished, however I was unsure if it was successful as the end of the thousands of lines of code read as follow



After researching this error, I found out that the latest version of metasploit actually comes pre-installed with Backtrack 5. It is accessible via the main menu by navigating the “Application tab”. Application > BackTrack > Exploitation Tools > Network Exploitation Tools > Metaspoilt framework.

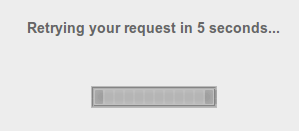
<https://community.rapid7.com/community/metasploit/blog/2013/01/03/using-backtrack-5-r3-with-metasploit-community-or-metasploit-pro>

Connected to metasploit via the browser in firefox



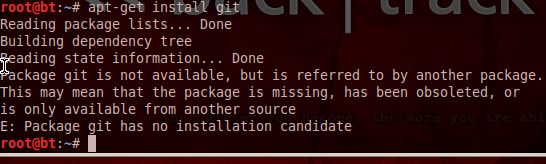


Got stuck on this for over 20 minutes

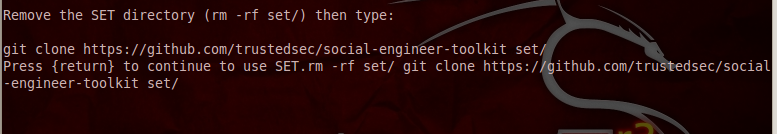


After all that, McAfee had to be uninstalled or disabled. So after further research, I saw that it was possible to do a DNS spoof through the Social Engineer Toolkit package. I as advised to install git, but of fucking course, that didn’t work.

<https://community.rapid7.com/message/4981#4981>



So after that didn’t work, I entered this.



Big fucking surprise, actuallt got in

