Step by Step Backtrack 5 and wireless Hacking basics

Installing Backtrack 5

Creating a Backtrack 5 R3 Live CD

Installing to the Hard drive

Installing and running with VMware

Reaver

WPA dictionary attack

Getting a handshake and a data capture

Using aircrack and a dictionary to crack a WPA data capture

www.wirelesshack.org

Step by Step Backtrack 5 and wireless Hacking basics

All information in this book is for testing and educational purposes only; for use by network security administrators or testing the security of your own wireless connection.

Introduction

Backtrack 5 R3 is a notorious Digital Forensic and Intrusion Detection software bundle with a whole lot of tools for Penetration Testing, It is based on Linux and includes 300 plus tools.

If you have never used Backtrack before all you really need to know it is the best software to use for Digital Forensics, Intrusion Detection and Penetration Testing.

There are different types of wireless attacks but in reality only two main types are used. I will go step by step through each. If you have Backtrack 5 installed the first chapter can be skipped directly to the hack you would like to use.

The two main types of wireless hacks are WPA dictionary attack, and Reaver.

In the past WEP used to be the main encryption used on routers but WEP was notoriously easy to crack and is rarely seen any more. WPA or WPA2, which are really the same thing, are the way in which routers are now encrypted and much harder to crack.

The way you think about these attacks are as important as the attacks themselves. There is no point and click option. Learning commands and typing them in a terminal window is a must.

Buying multiple routers to play with is also a good idea. There are plenty to be found at yard sales and swap meets on the cheap. Different manufactures do different things and have different setups so some have a weakness another will not.

One thing to mention also is that a internal wireless network adapter will not work with Backtrack and wireless penetration testing. This is not because the adapter is not supported it may or may not be. It is because most wireless chipsets do not support packet injections or the things required to do a wireless attack.

The most common wireless USB adapter currently used are the Alfa AWUS036H and the Alfa AWUS036NH. I have used both and both are good, but if possible get the Alfa AWUS036NH because it supports wireless N. While the Alfa AWUS036H supports wireless G.

To see a updated list go here www.wirelesshack.org/backtrack-compatible-adapters

Installing Backtrack 5

Backtrack 5 is free to download and install and can be downloaded here.
http://www.wirelesshack.org/backtrack-5-download

The Backtrack file is big 2-4 GB depending on the type of file you download. There is three ways to install Backtrack, install to the hard drive, boot off a DVD or flash drive, or run it in virtualization.

I will talk about how each install works, but if you are new to Backtrack 5 the easiest way is to burn the Backtrack 5 ISO to a DVD or a flash drive and boot from it, of course once the computer restarts data can be lost if not stored correctly.

Installing Backtrack 5 to the Hard drive is the same as installing any Operating System, which most everyone is familiar with, by booting from a disk, choosing install and answering questions such as time, date, language, and formatting the disk.

Running Backtrack 5 within virtualization is possibly the most common way. Mainly because a familiar operating system such as Windows can be run at the same time and files transferred between the two easily. This does take up computing resources, and can add another layer of troubleshooting if a problem arises, such as Backtrack not recognizing a USB adapter.

Me personally, I run VMware Player with Backtrack 5 and Windows 7. If you are just starting out I would start by using a Boot DVD then move on to virtualization later, but this is a personal option and depends on your own experience and knowledge of using Operating Systems.

Creating a Backtrack 5 R3 Live CD

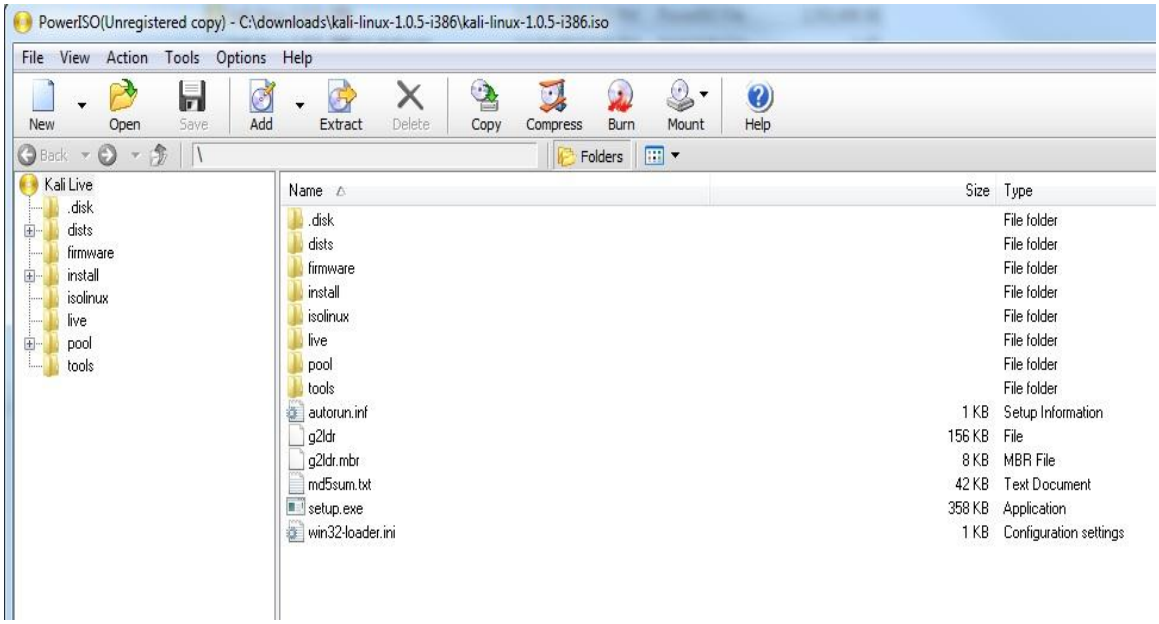
To boot off a DVD or Flash drive the Backtrack 5 ISO will be needed. The download can be found here http://www.wirelesshack.org/backtrack-5-download The download site has recently changed and will have to be downloaded by using a Torrent. If you have never downloaded a Torrent it is simple. First download and install a Torrent Client, the most popular is Utorrent but there are many. Then click the link to the torrent and the client will download the file.

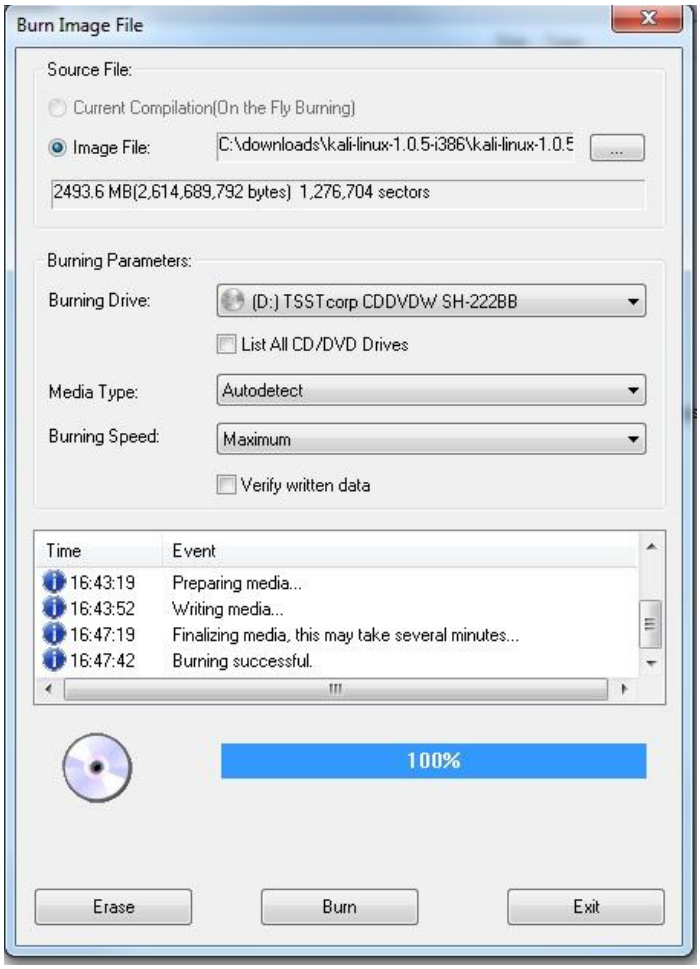
There are often spam links so be sure to click only the correct link. Such as this picture only click the link with the arrows.

ISO burning software will be needed. You most likely already have ISO burning software, such as certain version of Nero and so on, if in doubt use Power ISO.

(I have no connection with Power ISO it is simply what I use, so I will be using it for this example.)

Once the ISO is downloaded, load the Backtrack 5 ISO into your burning software and burn it to a DVD.


PowerISO(Unregistered copy) - C:\downloads\kali-linux-1.0.5-i386\kali-linux-1.0.5-i386.iso
File View Action Tools Options Help
New Open Save Add Extract Delete Copy Compress Burn Mount Help
Back Folders
Kali Live
.disk
dists
firmware
install
isolinux
live
pool
tools
Name Size Type
.disk File folder
dists File folder
firmware File folder
install File folder
isolinux File folder
live File folder
pool File folder
tools File folder
autorun.inf 1 KB Setup Information
g2ldr 156 KB File
g2ldr.mbr 8 KB MBR File
md5sum.txt 42 KB Text Document
setup.exe 358 KB Application
win32-loader.ini 1 KB Configuration settings


Burn Image File
Source File:
Current Compilation(On the Fly Burning)
Image File:
C:\downloads\kali-linux-1.0.5-i386\kali-linux-1.0.5
2493.6 MB(2,614,689,792 bytes) 1,276,704 sectors
Burning Parameters:
Burning Drive:
(D:) TSSTcorp CDDVDW SH-222BB
List All CD/DVD Drives
Media Type:
Autodetect
Burning Speed:
Maximum
Verify written data
Time Event
16:43:19 Preparing media...
16:43:52 Writing media...
16:47:19 Finalizing media, this may take several minutes...
16:47:42 Burning successful.
100%
Erase
Burn
Exit

After the ISO has been burned to a DVD it now can be used as a Live CD or used to install to the hard drive.

To boot from the DVD put it into the computer drive and check the computer settings to boot from the disk. Most computers have a boot option button to press or will automatically boot the disk.

Once it boots from the DVD it should come to the following menu.

Chose the first option which is "Default Boot Text Mode" and the computer will boot from the DVD and up to the login.

The default username and password for Backtrack is root then toor.

Once logged in and at the command prompt (pound symbol #) type "startx" and this will start the graphical user interface.

Quick steps to creating a Backtrack 5 Live CD

1. **Download the Backtrack ISO http://www.wirelesshack.org/backtrack-5-download**
2. **Download PowerISO or any ISO burning utility if you do not have one. http://www.poweriso.com/download.htm**
3. **Install PowerISO**
4. **Install a DVD into the DVD burner and open PowerISO.**
5. **Open the Backtrack image file in PowerISO then click burn and burn the Backtrack image file to DVD.**
6. **Use the DVD to boot which ever computer you like into Backtrack.**
7. **The username is root. The password is toor**
8. **At the command prompt type startx to enter the GUI.**

Installing to the Hard drive

Any existing Operating System will be wiped out and only Backtrack will be installed if this is done. For this reason I do not recommend installing to the hard drive unless you have done this before.

Backtrack can be setup to dual boot along with an existing Operating System, but explaining how to do a dual boot is more advanced. If something goes wrong the existing Operating System will be gone or damaged.

If you don't understand Operating Systems, use the other options, boot from the DVD but do not install Backtrack, or run Backtrack with VMware.

The ISO will be needed to be burned to a DVD to install to the hard drive. This is the same as the above booting off the DVD. Once Backtrack is in the GUI there is a file Backtrack.sh on the desktop. Double clicking this will install backtrack to the hard drive.

Quick Steps installing Backtrack 5 to the hard drive.

1 Boot the Backtrack Live Environment.

2 Login username root, Password toor.

3 At the prompt, type startx to enter the GUI.

4 Double click the Install Backtrack.sh on the desktop

5 Follow the on screen instructions such as time, date region and so on.

Installing and running with VMware

Running two operating systems at the same time is quite common now and done relatively easy. Two things will be needed the Backtrack 5 VMware Image, and VMware Player or Workstation.

For those who do not know VMware is a way to run another operating system virtually within another operating system. Basically if you are running Windows and want to run a Backtrack 5 install at the same time you can do this with VMware.

VMware works very well and as long as you have a fairly recent computer it should run fine. If you have an older laptop or older computer then the ISO may be better. Mainly because a ISO can be burned to a disk or any bootable device and booted from. When Backtrack 5 is booted off a ISO then it does not run Windows in the back ground.

VMware workstation is not exactly cheap although there is a free version. There is a 30 day free trial for VMware Workstation if you want to check it out.

VMware Workstation is not free but there is a free version called VMware Player. VMware Player doesn't come with all the options Workstation does but it does work, and runs Backtrack 5 fine.

VMware Player can be downloaded here http://www.vmware.com/products/player You will have to scroll down to find the free download of VMware Player.

Free for Personal Use

Player Plus is licensed for commercial use but if you simply want to learn about virtual machines or run virtual machines at home you can always use VMware® Player™ for free!
Download Player for personal use.

Are you ready for VMware Workstation?
Get access to powerful features with Workstation including snapshots, cloning, remote connections to VMware vSphere®, sharing VMs, advanced Virtual Machine settings and much more.
Try Now

Upgrade to VMware Workstation

Run multiple operating systems.

Purchase Upgrade

Upgrade to VMware Fusion Professional

Designed for advanced users and professionals.

Purchase Upgrade

Buy VMware Player Plus

Purchase a full license today.

Buy Now

Once you have VMware Player, you will need the VMware Image file from the Backtrack 5 site here http://www.wirelesshack.org/backtrack-5-download

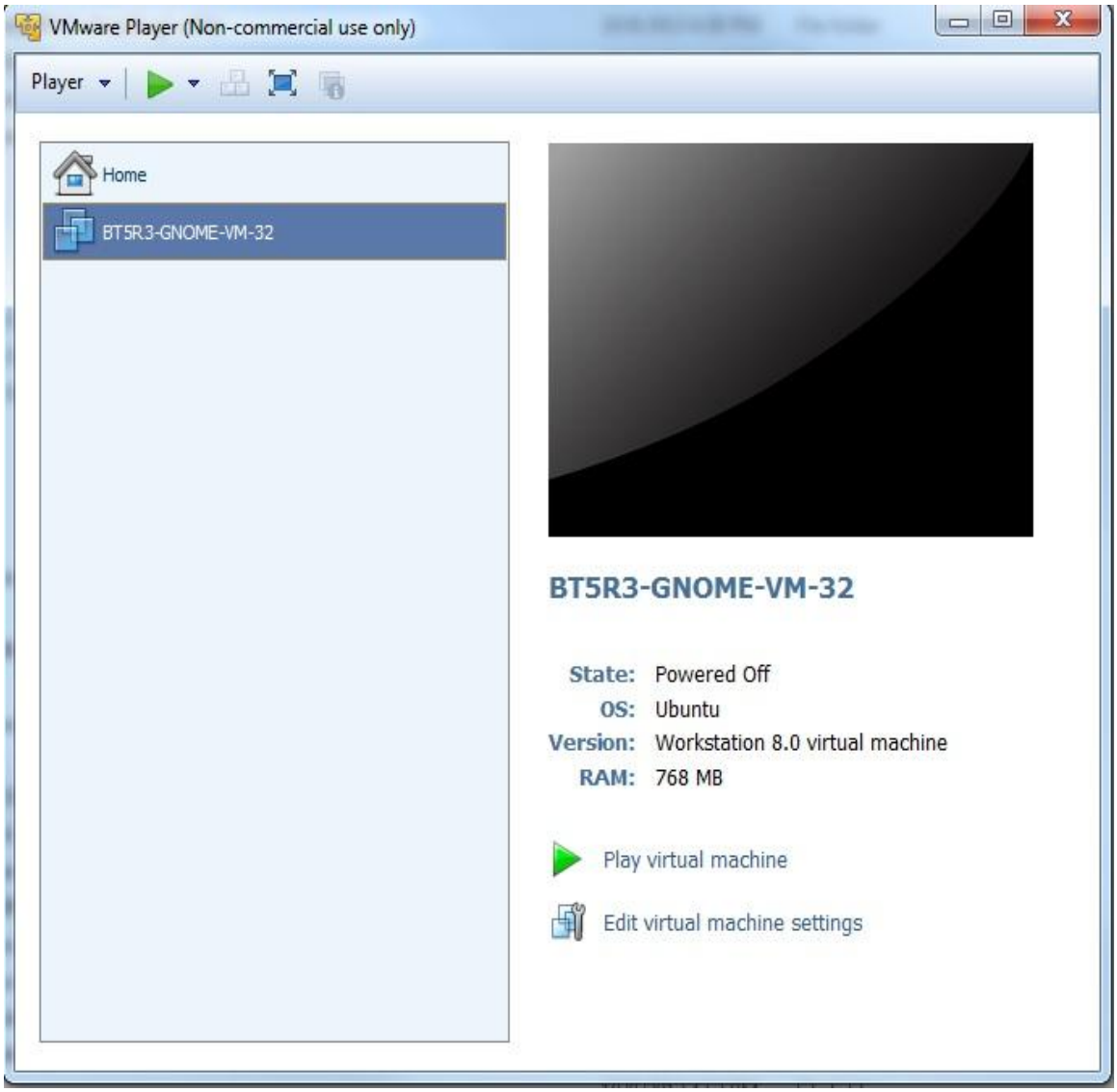
The VMware Image is a preset up install that can be loaded straight into VMware and be ready to use.

Once both VMware player and the Backtrack 5 VMware image is downloaded run and install VMware Player and follow the default options.

The Backtrack 5 VMware Image file will have to be extracted and will create its own folder with a bunch of files in it.

Once it is done extracting all the files, run VMware Player and on the right click "Open a Virtual Machine." A dialog box will come up simply direct it to the folder with the extracted Backtrack 5 VMware image.

Only one file will come up because of the .VMX extension click on it and you will be able to play virtual machine and run Backtrack 5.



Quick steps to installing Backtrack 5 and VMware player

1. **Download VMware www.vmware.com/products/player**
2. **Download the Backtrack VMware image file. http://www.wirelesshack.org/backtrack-5-download and extract the files.**
3. **Install VMware: follow the default options**

4. **Once VMware is installed go to Open a Virtual Machine, go to VMware Backtrack 5 Image file location and click on the file. Backtrack 5 will open and come up to a logon screen. The user name is root and the password is toor.**
5. **The user name is root and the password is toor. Once you are logged in type startx and Backtrack will open into a GUI.**

Reaver

Commands we will be using.

airmon-ng

airmon-ng start wlan0

wash -i mon0 -C

reaver -i mon0 -b (The BSSID) –vv

(The -vv is two V not a W)

Reaver is one of the best tools to come along in a long time. Before WPA was implemented and WEP ruled wireless encryption any network could be cracked easily. But when WPA became the standard it became much harder to do, using the dictionary attack method was the only real option. Then came Reaver.

Reaver works by a flaw found in routers called WPS or Wi-fi Protected Setup. WPS makes it easy for wireless devices to find and connect to a router. The problem with WPS is, it has a flaw in it that lets someone go around the encryption.

If a router has WPS enabled then cracking the encryption is no longer necessary. Think of it like a backdoor.

If a router has WPS enabled it can usually be cracked in two to ten hours.

"Wi-Fi Protected Setup, or WPS. It's a feature that exists on many routers, intended to provide an easy setup process, and it's tied to a PIN that's hard-coded into the device. Reaver

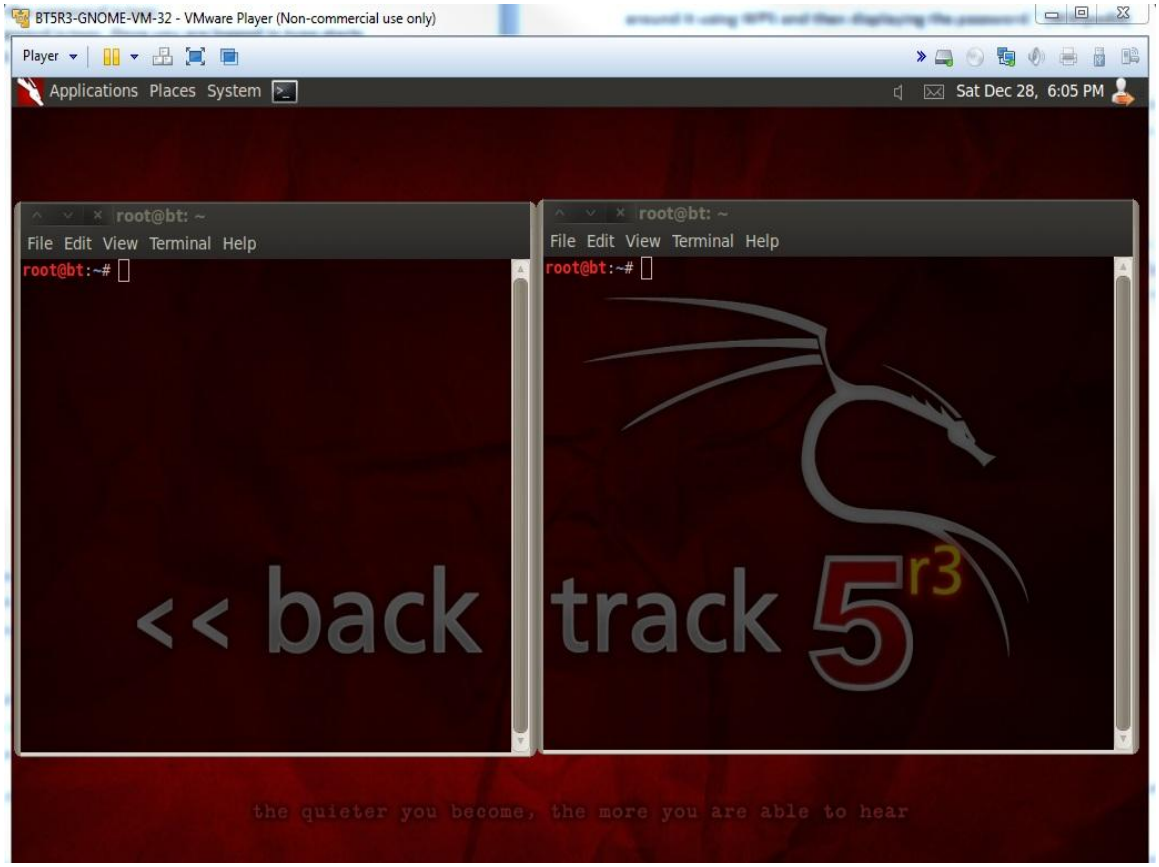
exploits a flaw in these PINs and the result is that, with enough time, it can reveal your WPA or WPA2 password. Reaver does not attempt to take on the WPA encryption itself but goes around it using WPS and then displaying the password." (Wikipedia)

As with other attacks there are some problems with this. Such as signal strength, a strong signal is almost a must. Also some routers can crash if too many pins get thrown at it to quickly much like a denial of service attack can crash a PC.

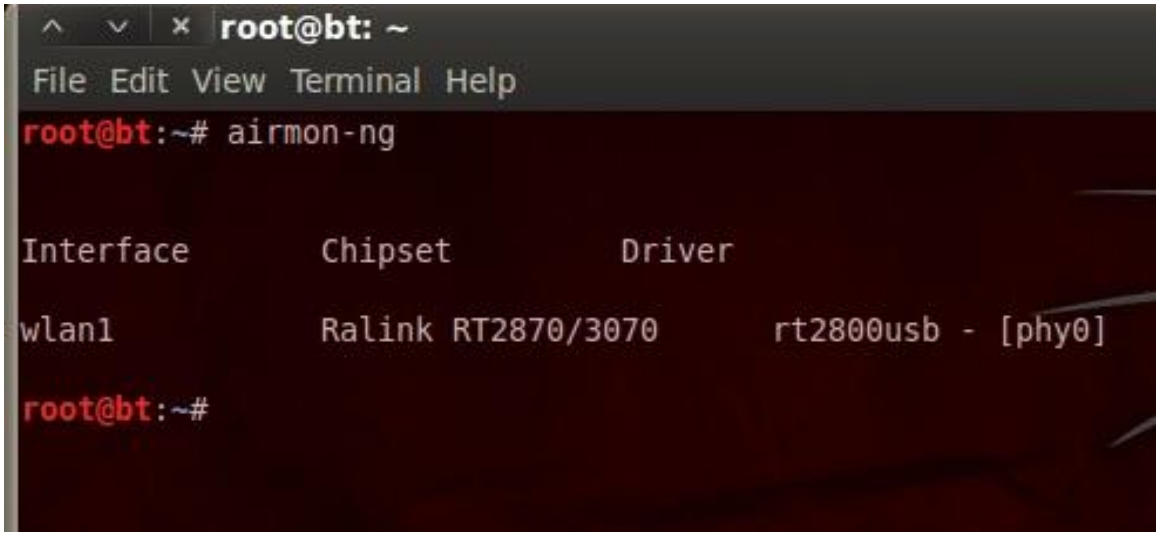
Reaver has many option or switches it can use to deal with these problems. The example I am using below is a basic one. There are many more commands to use with Reaver, you can see them all by typing "reaver /?", or In the Appendix there is a full list of the commands that can be used with Reaver.

The first thing we need to do is enable the wireless USB adapter.

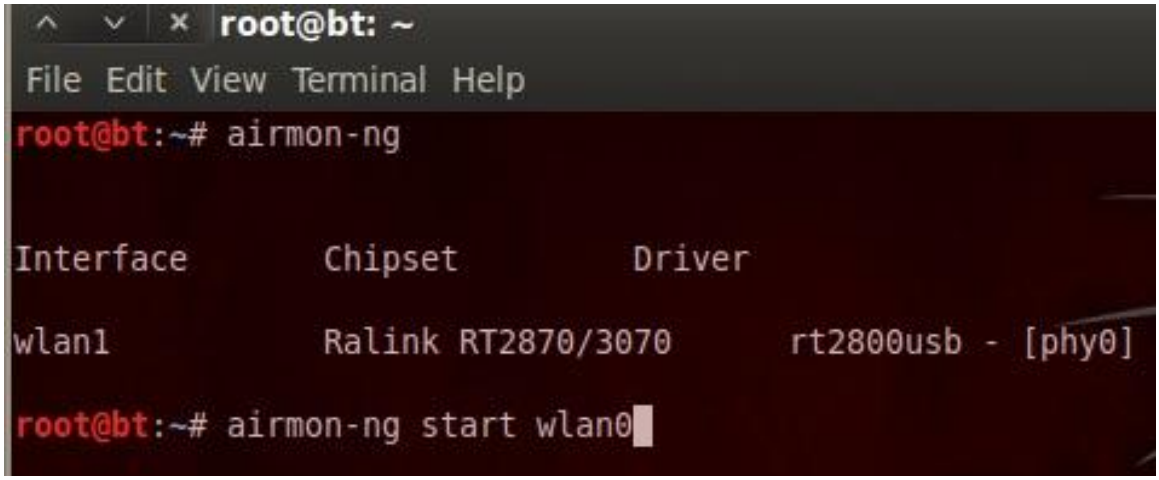
Start Backtrack 5 and open two terminal windows.



Run the command "airmon-ng" to see if Backtrack recognizes your wireless USB adapter. It should show "Wlan" along with the chipset, if it doesn't then some troubleshooting will have to be done until it does.



Once the wireless USB adapter is working, we need enable it. To do this run the following command "airmon-ng start wlan0"



If all goes well the screen will scroll by with some information then say enabled on mon0.

Finding a WPS enabled router is the next step this used to be hard to do until the "wash" command came along.

The “wash” command has been notorious for having problems and not working correctly. Basically the “wash” command goes out and tells you if a router has WPS enabled, so you don’t waste your time running Reaver. I believe I have found a fix that has been working for me on both Backtrack 5 and Kali Linux.

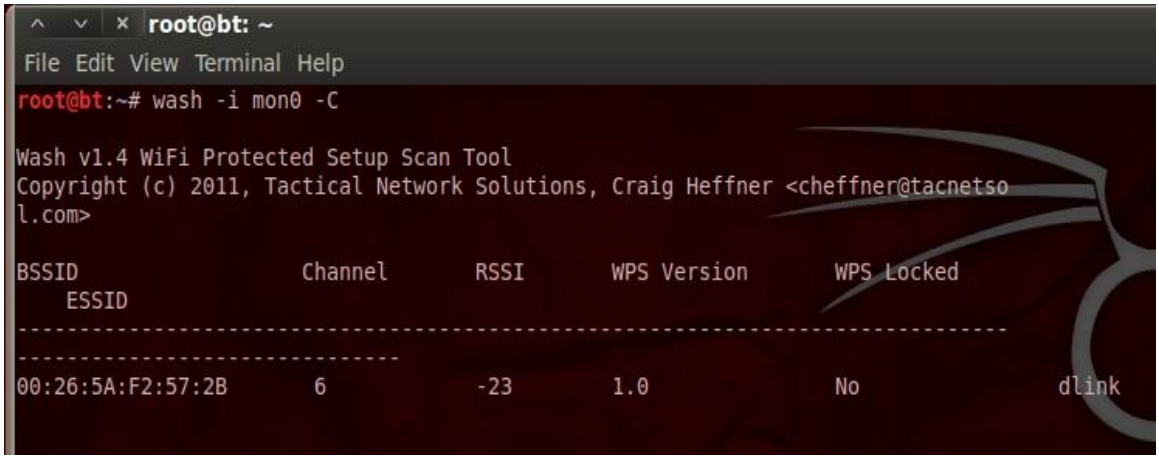
First make a directory like this.

“MKdir /etc/reaver”

then run the wash command

"wash -i mon0 -C"

(That is a capitol C)



Copy the BSSID, to paste it when needed later, then press CTRL+C to stop the terminal window using the wireless USB adapter.

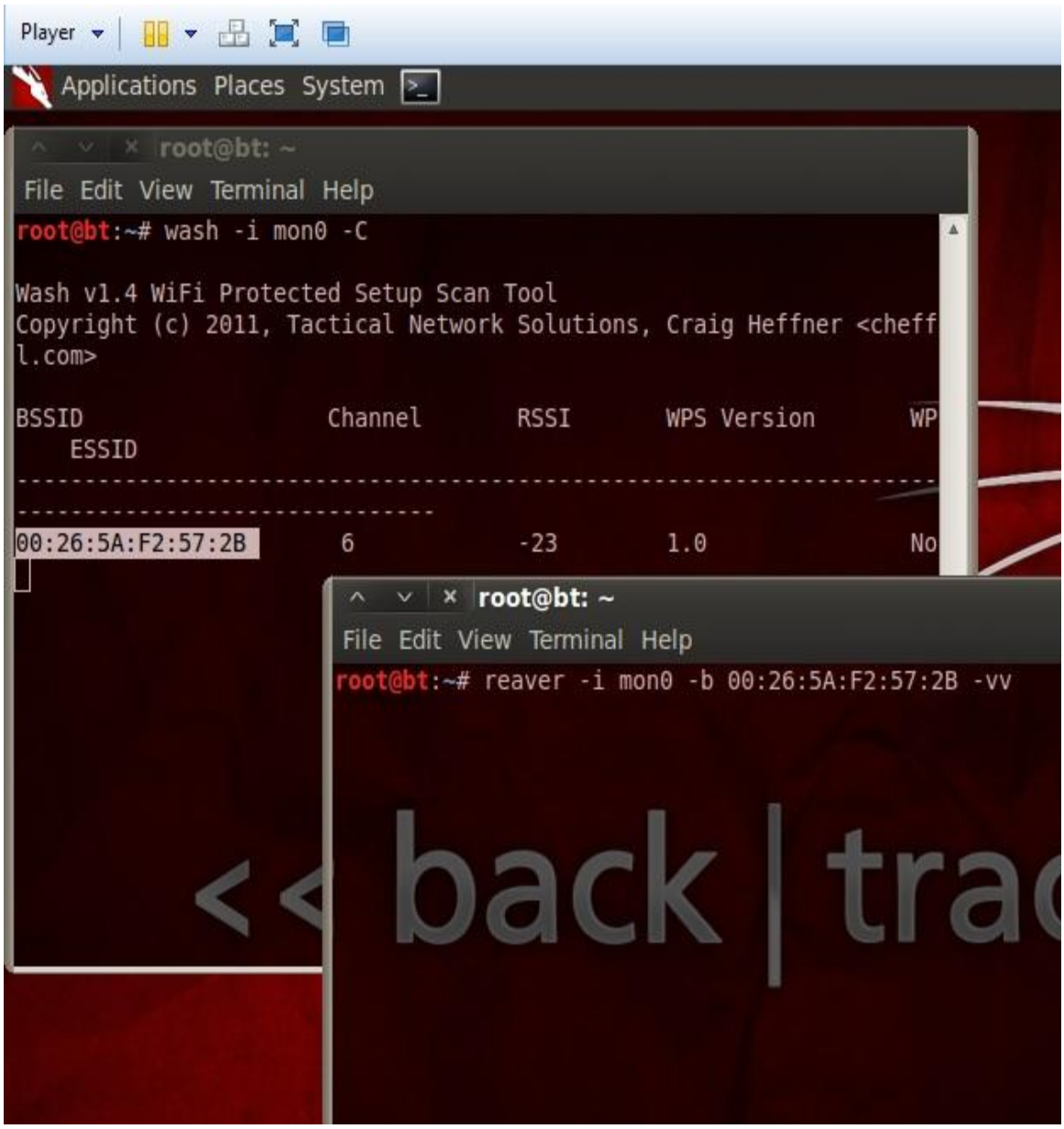
(If nothing comes up then no WPS enabled router is within reach. Run the following command to see all access point within your reach. "airodump-ng mon0". Only do this if the wash command finds nothing)

Now we can get to using Reaver. Be sure the terminal window running the "wash" command is not actively using the wireless USB adapter by pressing CTRL+C inside of it. You can copy and paste the BSSID.

In the second terminal window run the following command.

"reaver -i mon0 -b (Target BSSID) –vv"

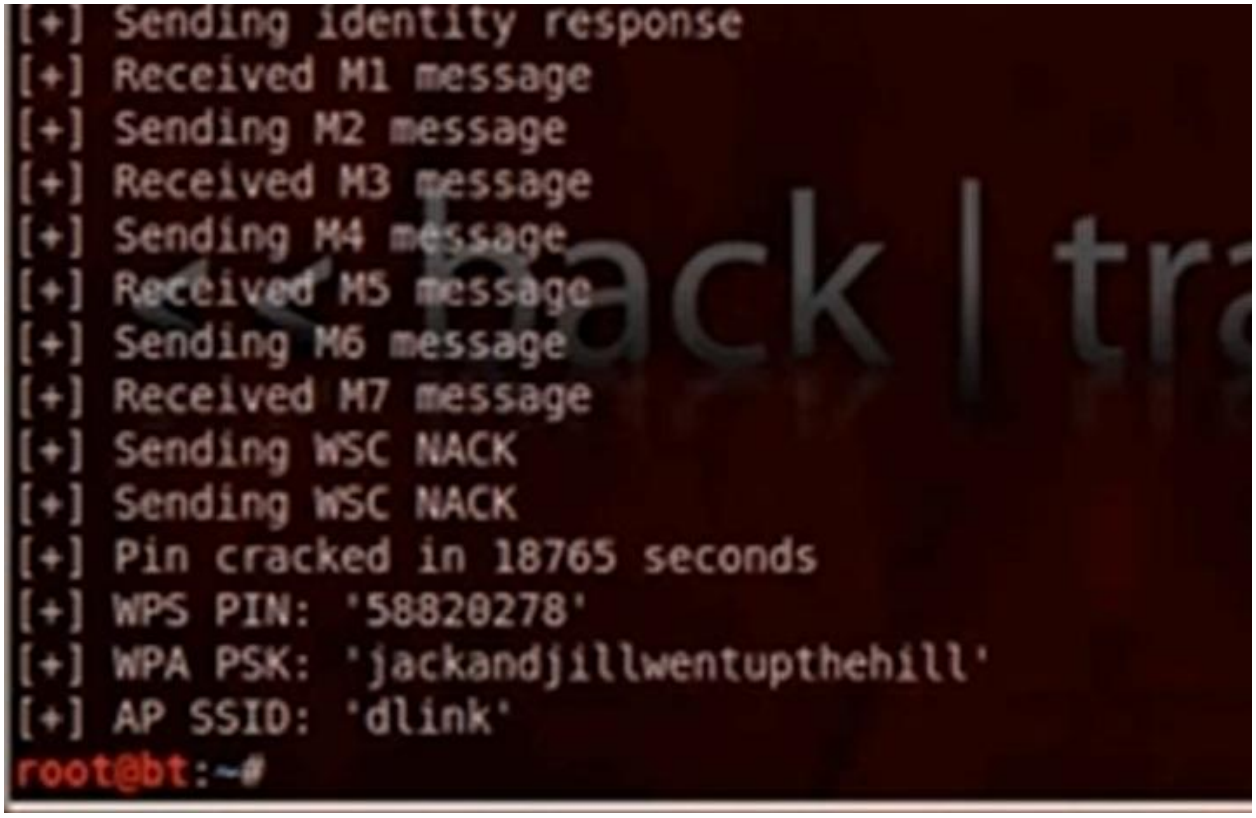
(The -vv is two V not a W)



Reaver should start to run.

Reaver will now run and start a brute force attack against the Pin number of the router. It will run until it finds the wireless password usually 2-10 hours.

Here is a screen shot of what it looks like when Reaver cracks the password.



The password is "jackandjillwentupthehill".

WPA dictionary attack

WPA and WPA 2 is the newest encryption for wireless devices, as far as cracking them they are the same so I will use WPA from here on.

A dictionary attack is one of the easiest to understand but the least likely to find a password. This is often the last resort because while it does work it depends on the dictionary used and the computing power.

Basically a data capture of the router is captured wirelessly when someone logs into the router. Then a dictionary file with a bunch of names and combination of names/numbers is used to throw at the data capture until the password is found.

If someone knows the person then they may be able to guess the password but otherwise this can take a long time and never find anything. If you are stuck using this method, thinking about how the password might be structured will be crucial along with computing power. The data capture could be copied between multiple computers to split the things up. A to F on one G to Z on another. Cloud computing might be a option to harness someone else computing power and so on.

There are other ways such as Rainbow Tables, or the video card attack, but the simplest or easiest way to crack WPA is to use Brute Force. The way this works basically is that there is a large dictionary that you use to throw as many combinations of words as possible at the WPA encryption until it cracks. If the password is easy then it will find it quick, if it is a long paraphrase with many different number letter combinations then it will be much harder.

Getting a handshake and getting a data capture

Commands used

airmon-ng

airmon-ng start wlan0

airodump-ng mon0

Backtrack should be up and running.

Open two terminal windows

Run the command "airmon-ng" to see if your USB adapter shows up, if it doesn't then some troubleshooting as to why it is not will have to be done. For this example I am using a Alfa AWUS036H which uses the RTL8187L chipset

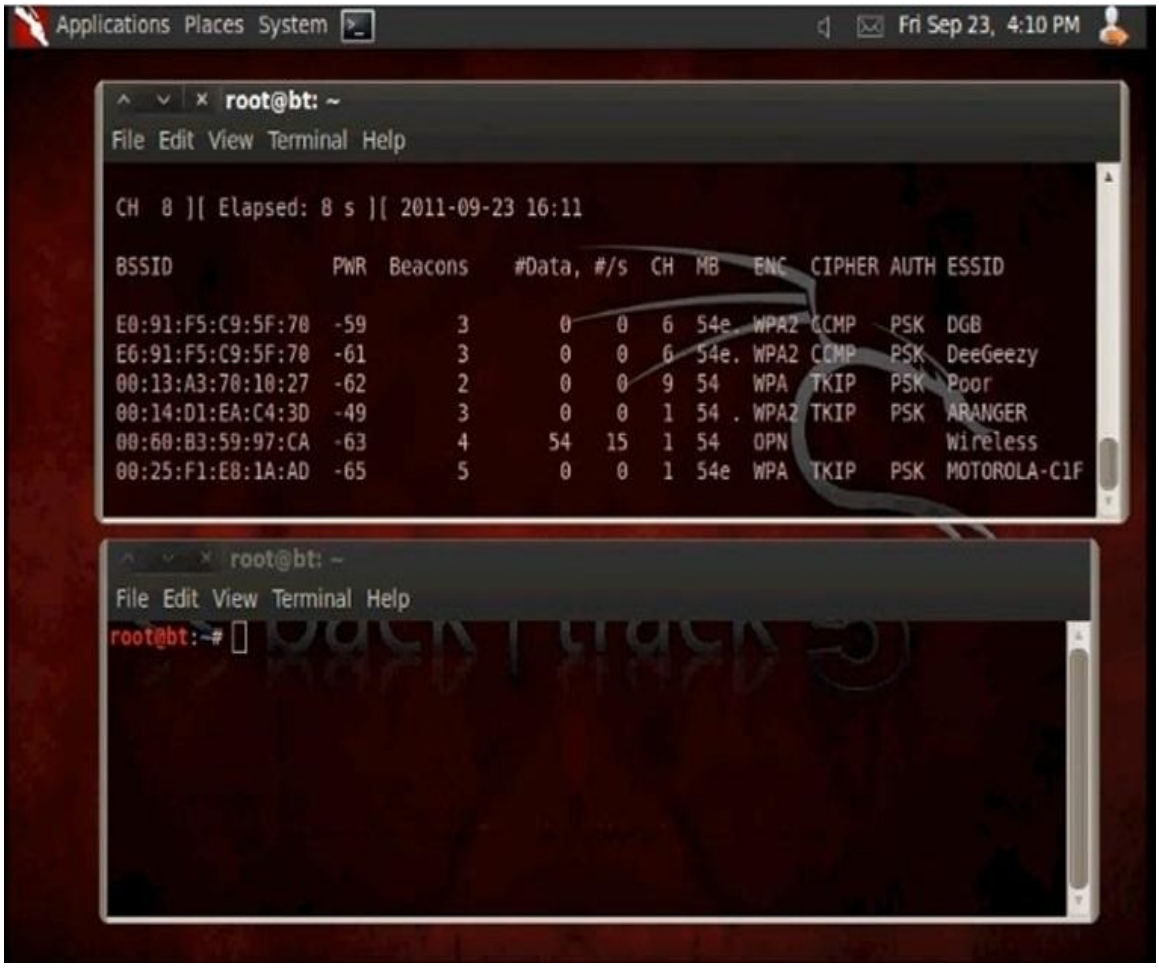
Once you know the adapter is connected and operating run this command to get the adapter into monitor mode.

airmon-ng start wlan0

if all goes well the screen will scroll by with some information then say enabled on mon0. sometime it will enable on mon1 or mon2 if it does use this.

Now we want to see what router or access point (AP) are out there so we run this command.

airodump-ng mon0



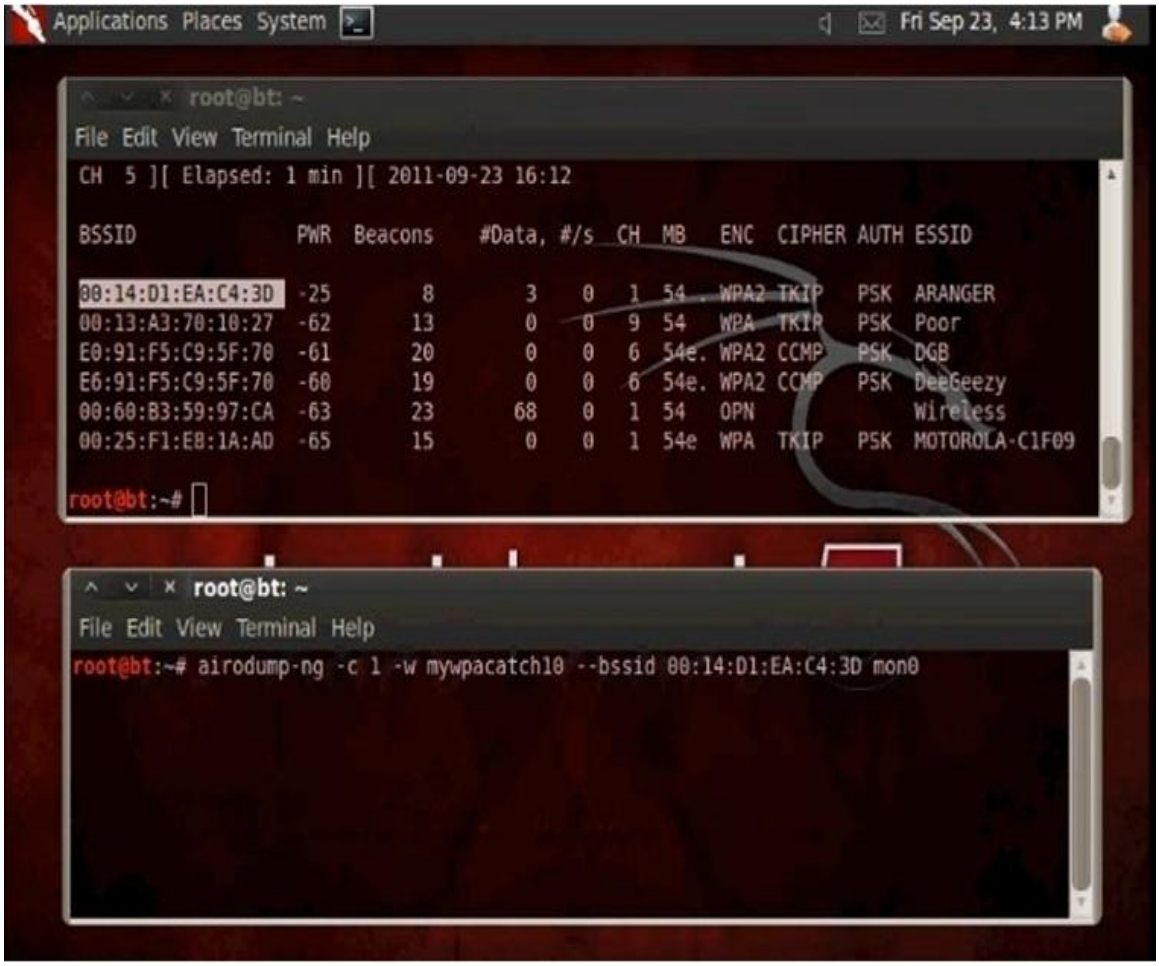
A picture like the above should come up and show all the AP out there. Here we want to target the AP we want and copy the BSSID. Use CTRL+C to stop the command and copy the BSSID.

Now we want to leave the original terminal alone and move to the second open terminal. Here we are going to setup the adapter to do a data capture on the AP point we selected. After we do this we will have to wait for a wireless device to connect to the router and it will do a data capture. To do this we do the following command.

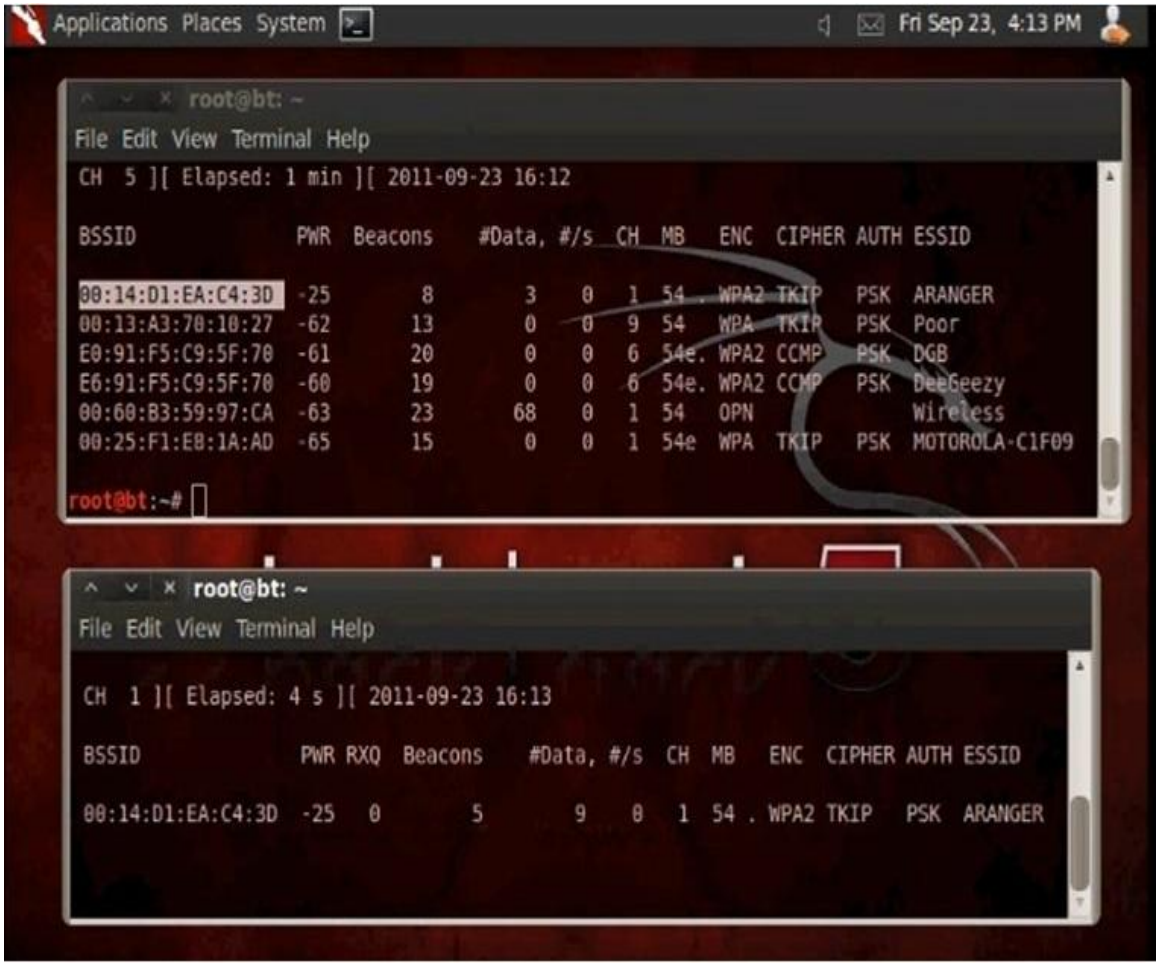
airodump-ng -c (channel) -w (Our file name) --bssid (bssid of AP) mon0

So for me it would be

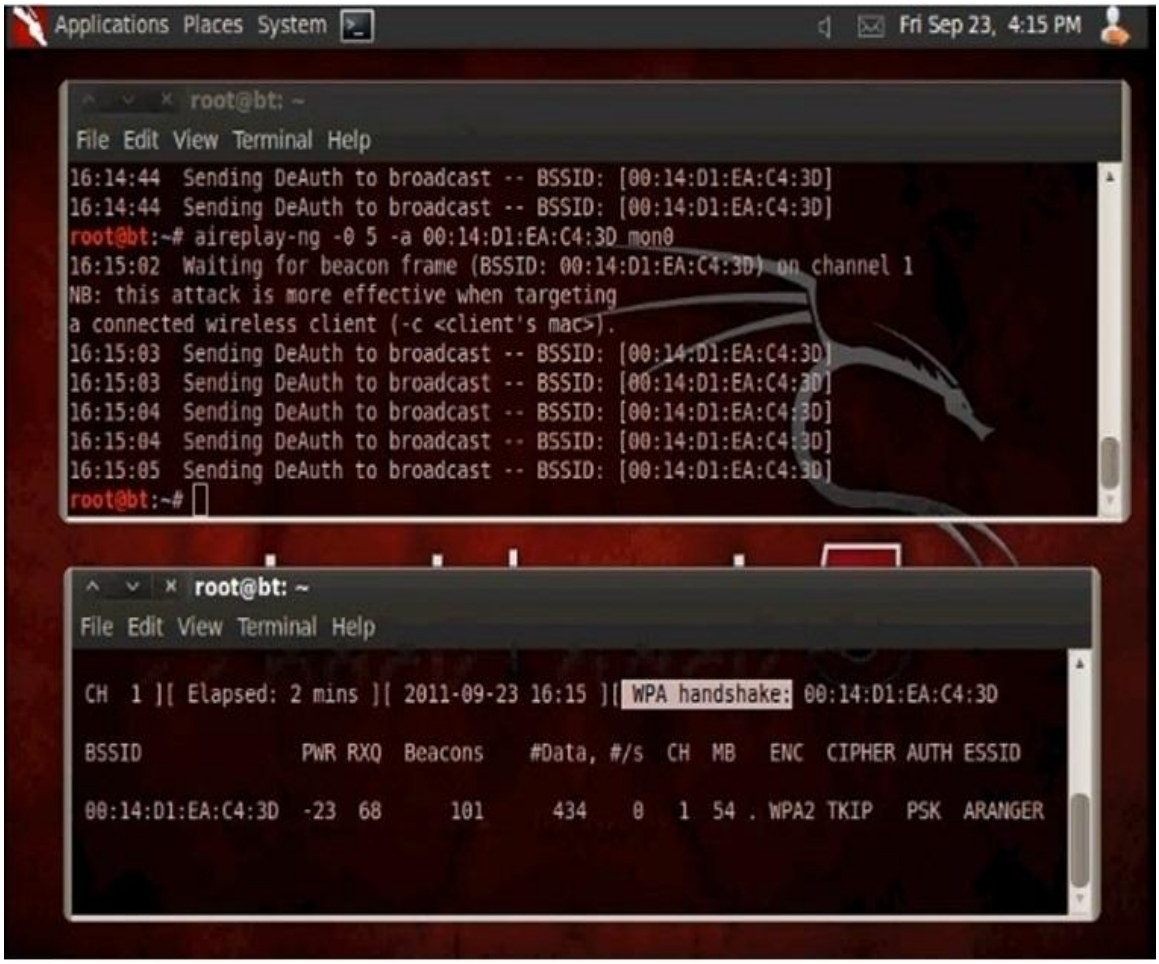
airodump -c 1 -w MyWpaCatch --bssid 00:14:D1:EA:C4:3d mon0



Then it should go into monitoring the AP for a data capture.



At this point we could simply wait for someone to connect wirelessly to the router. It can be any device their laptop, desktop or smart phone. If we wait then we stay in passive mode and no one can detect we are there. The bottom terminal (in this example) will pop up and say WPA Handshake in the upper right when this happens.



There is a way to speed this up if you know someone has a wireless device connected to the router by de-authenticating them or kicking them forcing them to reconnect. This will most likely be recorded by the router so this is not a passive method. To do this open another terminal window and type the following.

aireplay-ng -0 5 -a (Target AP BSSID) mon0

for me this would be

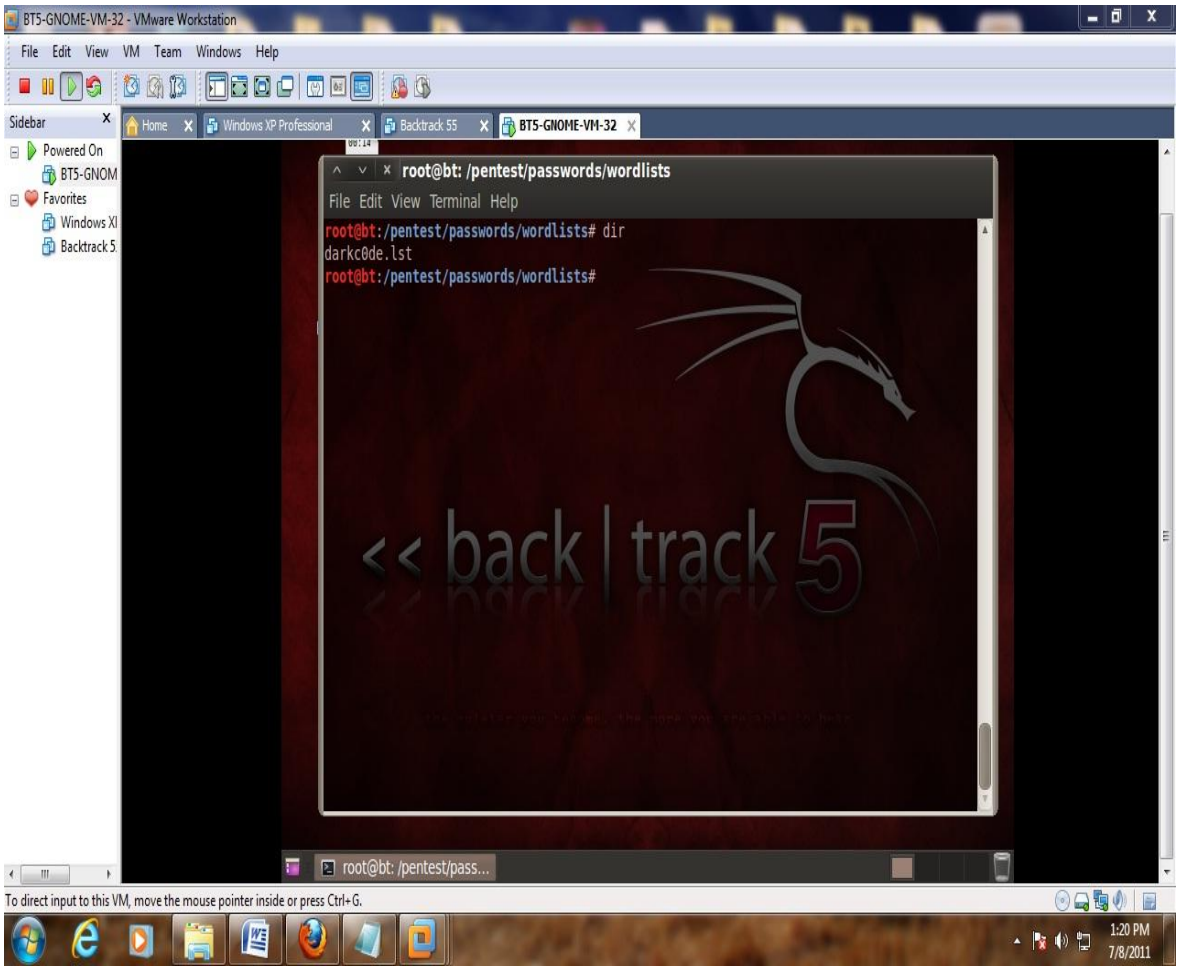
aireplay-ng -0 5 -a 00:14:D1:EA:C4:3D mon0

Using aircrack and a dictionary to crack a WPA data capture

You should already have a WPA handshake file and Backtrack 5 running.

The default storage for a WPA handshake is under /root and will be there under whatever name you called it. The dictionary that we will use is built into backtrack under the /pentest/passwords/wordlists and is called darkc0de.lst.

Getting a good dictionary can be hard there are some dictionaries within Backtrack 5 that I will use to explain the Brute Force method but there size is limited making them useless against all but the easiest passphrase.



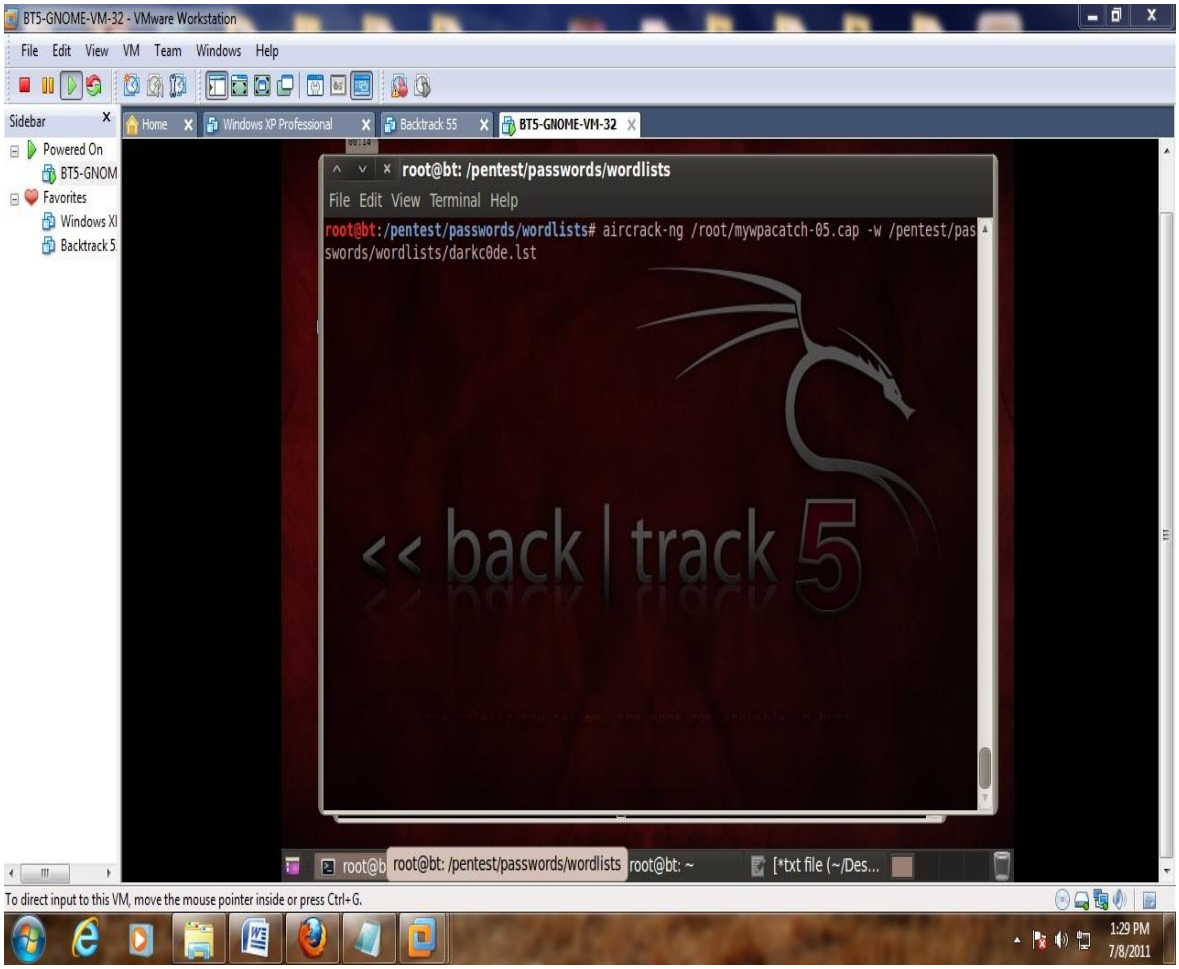
We will be using aircrack to do the cracking and the command to do this is:

aircrack-ng (file name) -w (dictionary location)

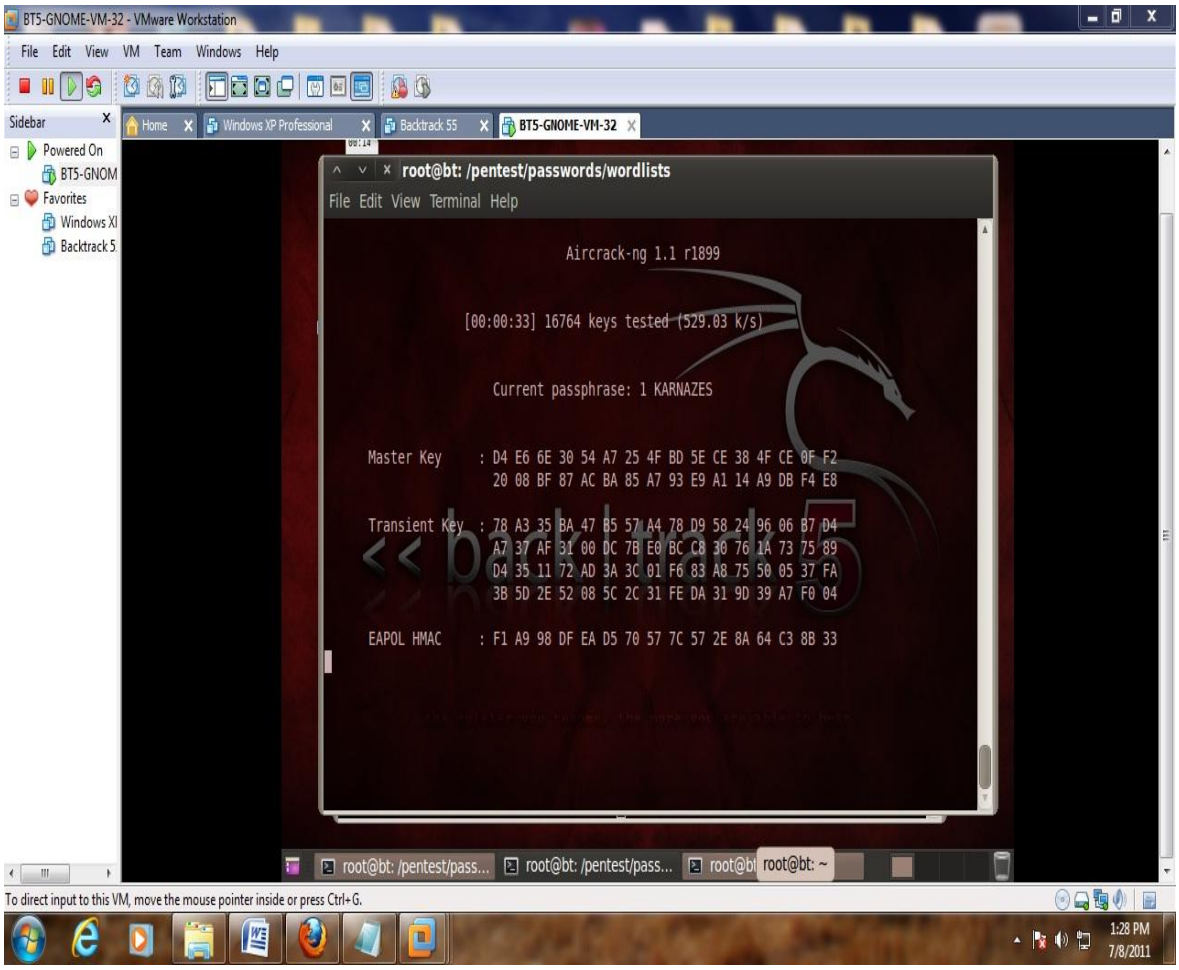
Where the file name is the handshake file you captured and the dictionary location is the path to your dictionary. The location of where this two files are and their names will be up to you. as I said above the usual default location of the handshake file is under /root and is whatever you called it. We will be using the darkc0de.lst dictionary for this example under the /pentest/passwords/wordlists directory.

So the command for me to do this would be:

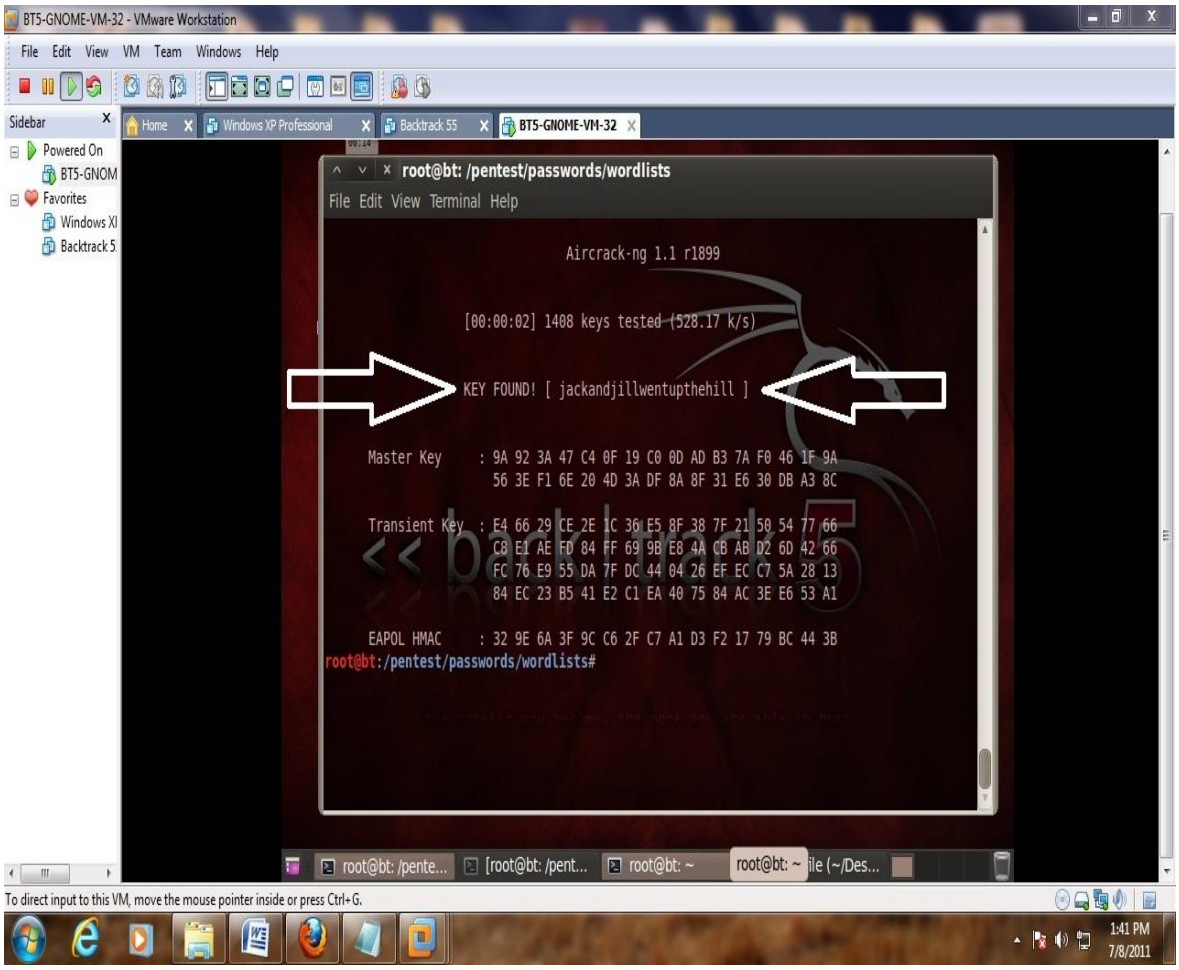
aircrack-ng /root/mywpacatch-05.cap -w /pentest/passwords/wordlists/darkc0de.lst



If done right aircrack should start and begin to try to crack the WPA handshake capture with the dictionary.



If the dictionary finds it, it will show as below if not then another dictionary will need to be used. For this example I edited the text dictionary file and put the password in to show what it looks like when it is found.



Conclusion

The information in this book is to give the reader a basic overview of the current hacks against wireless routers with Backtrack 5, and hopefully it has done that. There are many more options and switches that can be used with commands such as Reaver, simply type the command then "/?" to see the other options, such as "reaver /?". In the Appendix you can see these options.

www.wirelesshack.org

APPENDIX

Reaver v1.4 WiFi Protected Setup Attack Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:

-i, --interface=<wlan> Name of the monitor-mode interface to use

-b, --bssid=<mac> BSSID of the target AP

Optional Arguments:

-m, --mac=<mac> MAC of the host system

-e, --essid=<ssid> ESSID of the target AP

-c, --channel=<channel> Set the 802.11 channel for the interface (implies -f)

-o, --out-file=<file> Send output to a log file [stdout]

-s, --session=<file> Restore a previous session file

-C, --exec=<command> Execute the supplied command upon successful pin recovery

-D, --daemonize Daemonize reaver

-a, --auto Auto detect the best advanced options for the target AP

-f, --fixed Disable channel hopping

-5, --5ghz Use 5GHz 802.11 channels

-v, --verbose Display non-critical warnings (-vv for more)

-q, --quiet Only display critical messages

-h, --help Show help

Advanced Options:

-p, --pin=<wps pin> Use the specified 4 or 8 digit WPS pin

-d, --delay=<seconds> Set the delay between pin attempts [1]

-l, --lock-delay=<seconds> Set the time to wait if the AP locks WPS pin attempts [60]

-g, --max-attempts=<num> Quit after num pin attempts

-x, --fail-wait=<seconds> Set the time to sleep after 10 unexpected failures [0]

-r, --recurring-delay=<x:y> Sleep for y seconds every x pin attempts

-t, --timeout=<seconds> Set the receive timeout period [5]

-T, --m57-timeout=<seconds> Set the M5/M7 timeout period [0.20]

-A, --no-associate Do not associate with the AP (association must be done by another application)

-N, --no-nacks Do not send NACK messages when out of order packets are received

-S, --dh-small Use small DH keys to improve crack speed

-L, --ignore-locks Ignore locked state reported by the target AP

-E, --eap-terminate Terminate each WPS session with an EAP FAIL packet

-n, --nack Target AP always sends a NACK [Auto]

-w, --win7 Mimic a Windows 7 registrar [False]

Example:

reaver -i mon0 -b 00:90:4C:C1:AC:21 -vv