How to Crack a WEP Encrypted Wireless Network on Windows Vista

First you can only use this method to crack a WEP encrypted network. WEP has been replaced by WPA encryption which is stronger but can still be cracked, just not as easily. To find out if the network you want to crack is WEP encryption, simply view the wireless networks in the Connect to a network box and hold your mouse over the network of choice. A little box will tell you the encryption. If it say WEP - good we can proceed, if it says anything else this tutorial wont help.

First to understand what you will be doing. You will be using a program to capture packets and then use another program to analyze those packets and crack the key, thus allowing you to have access to their network. To capture packets (data from the network we are trying to crack) you must have the program running on your computer and you must capture about 200 000 or more IV packets (a special type of packet). I will show you how to capture the correct type of packets.

Also ONLY certain types of wireless cards can actually capture wireless packets. In order to capture packets your wireless card must be able to go into monitor mode, not every driver or every wireless card supports monitor mode. In most cases you will have to download a special driver designed for your wireless card to put it into monitor mode. I had to purchase a new wireless card because mine was not supported. The program you will be using has a list of supported wireless cards and comes with the drivers needed (Lucky you)

Ok, down to business. First the program you need to capture packets can be downloaded from this link http://www.tamos.com/download/main/ca.php

Next the program to analyze the packets and finger out the password can be downloaded from my own site. I got it to work for windows vista and then zipped it all into a folder for you. To get this to run all you have to do is extract it, open the aircrack folder, then open the bin folder, then double click on Aircrack-ng GUI.exe. Here is the download linkhttp://www.howtovideos.ca/images/aircrackVista.rar just click it and save the file.

Now for the dirty work, keep in mind this could take a few days to capture enough packets. First install the Commview for Wifi program. You do this by extracting the setup file from the file we downloaded earlier (ca6.zip) Then double click setup.exe and follow the prompts. When Commview opens for the first time it has a driver installations guide. This replaces the old driver with a newer, better, and more improved version! Hooray. Follow the prompts to install your new driver and now we are ready to capture. If everything has gone as planned when you open Commview for Wifi the little play button in the top left corner will be blue. If it is not blue the driver has not been installed properly. Moving on…

Click the blue button in the top left corner and then click Start Scanning. Commview for Wifi now starts scanning each channel looking for data that is being sent. It will list each network it finds. Now click each host until you find the name of the network key you are trying to find. Now select the appropriate channel (my network is broadcasting on channel 6 so I will start capturing all data on channel 6) Click capture.

Commview for Wifi is now capturing all the packets being sent over channel 6. Once Commview for Wifi collects enough packets aircrack can analyze them and crack the wireless key. The thing is, you only need certain packets, and if you collect too many unneeded packets aircrack may get confused. To help make things easier follow the next few steps.

First of all we only want packets from one host, not all of them. As you can see from my screenshot below I am collecting packets from 7 different network. (see screenshot below)A few are WPA encrypted so they and a few are WEP. I really only want to collect data being sent from one network, so in order to do this all you have to do is right click on the wireless network you want to crack and select copy mac address.

Now click on the rules tab. On the left side under simple rules click MAC Addresses. For action select Capture, and for Add Record select both. Now click inside the entry form box and hit ctrl+v (to paste the mac address) or right click and select paste. Now hit add MAC Address.
What we just did is make a rule so that Commview for Wifi will only capture packets coming from a certain MAC Address (the one we want) Great almost done.

Now to make things even easier for Aircrack you only want to capture DATA packets. There are 3 types to select from Management packets, Data Packets and Control Packets. We only want Data packets because that is where the information is that Aircrack needs to crack the wireless encryption passkey. Simply select the D, and unselect the M and the C.

Now Commview for Wifi is only capturing Data Packets. To be more specific Commview for Wifi is only capturing Data Packets to and from a specific MAC address. Now that everything is set up to capture the right types of packets we should start saving the logs.

You have to save all of the packets into a log for Aircrack to analyze them. You can set Commview for Wifi to save them automatically, or just save them yourself periodically. It is a good idea to have them auto save because it splits them into nicely sized logs, and if you accidentally close Commview for Wifi they will save and you wont lose all your packets! To do that just go to the logging tab and enable auto saving. You can change the settings if you would like (I recommend increasing the maximum directory size to something like 100000).

And now we wait… We have to capture over 15000 IV packets. Because we set up some rules most of the packets we capture will be IV packets (these are a certain type of Data packet with information used to crack the wireless key). It took me about 4 days to capture enough packets, but I was not running Commview for Wifi non stop. If you are close to the network and there is heavy traffic, it may only take you a few hours. Ok what do you do now?
Alright, so now 20000 packets (or more) later we are ready to crack the WEP wireless key. First lets converts all of the log files to .cap format (shown in screenshot below) When I cracked my first WEP key with this method I had 4 log files and about 220 000 packets.Go to wherever you have your log files saved and double click to open it. Now click on file -> Export Logs -> Tcpdump Format

Save it as 1.cap do the rest of your logs, saving them in sequential order 1.cap, 2.cap, 3.cap etc.

Now that you have all of your log files saved in .cap format lets open Aircrack. Open the aircrack folder (wherever you extracted it) then open the Bin folder, now double click Aircrack-ng GUI.exe. Aircrack will open, click the choose button and navigate to where you have your log files saved. To select all of your log files (saved in .cap format) Hold down CTRL and click each file, Then hit open.

Now click launch, Aircrack shows you all of the different BSSID's that it captured data from and assigns an index number to each one, then it asks you Index number of target network? You want to enter the number of the network you want to crack. Mine is called CrackMePlease so I am selecting 15.

Enter the index number and then press enter, if you have enough IV's then it should give you the WEP key. If not go back and capture more and try again.

That's all