HACKING Wi-Fi USING WINDOWS for WEP encrypted networks.

You could either see video or see the steps below.

VIDEO
http://www.youtube.com/watch?v=knMUDo5a_Xw#t=276

REQUIREMENTS :
A compatible wireless adapter:
This is by far the biggest requirement.The wireless card of your computer has to be compatible with the software CommVIew. This ensures that the wireless card can go into monitor mode which is essential for capturing packets.
CommView for Wi-Fi : http://tinyurl.com/pjue73q
This software will be used to capture the packets from the desired network adapter.
Aircrack-ng GUI : http://tinyurl.com/lgr4zu8
After capturing the packets this software does the actual cracking.

SETTING UP COMMVIEW FOR WI-FI
--Open Commview for Wi-Fi. When CommView opens for the first time it has a driver installation guide. Follow the prompts to install the driver for your wireless card.
--Run CommView for Wi-Fi.
--Click the play icon on the top left of the application window.
--Start scanning for wireless networks.
CommView now starts scanning for wireless networks channel by channel. After a few minutes you will have a long list of wireless networks with their security type and signal. Now it is time to choose your target network.

SELECTING THE TARGET NETWORK AND CAPTURING PACKETS
A FEW THINGS TO KEEP IN MIND BEFORE CHOOSING THE TARGET WIRELESS NETWORK :
This tutorial is only for WEP encrypted networks, so make sure you select a network with WEP next to its name.

Choose a network with the highest signal.
Each network will have its details in the right column.
Make sure the WEP network you are choosing has the lowest dB (decibel) value.
Once you have chosen your target network, select it and click Capture to start capturing packets from the desired channel.
Now you might notice that packets are being captured from all the networks in the particular channel. To capture packets only from the desired network follow the given steps.
Right click the desired network and click on copy MAC Address.
Switch to the Rules tab on the top.
On the left hand side choose MAC Addresses.
Enable MAC Address rules.
For 'Action' select 'capture' and for 'Add record' select 'both'.
Now paste the mac address copied earlier in the box below.
We need to capture only data packets for cracking. So, select D on the bar at the top of the window and

deselect M (Management packets) and C (Control packets).

Now you have to save the packets so that they can be cracked later. To do this:

Go to the logging tab on top and enable auto saving.

Set Maximum Directory Size to 2000.

Set Average Log File Size to 20.

Step 5: Waiting...

Now the boring part- WAITING!

NOTE: The amount of time taken to capture enough data packets depends on the signal and the networks usage.

The minimum number of packets you should capture should be 100,000 for a decent signal.

After you think you have enough packets (at least 100,000 packets), you'll need to export them.

Go to the log tab and click on concatenate logs.

Select all the logs that have been saved.

Do not close CommView for Wi-Fi.

Now navigate to the folder where the concatenated logs have been saved.

Open the log file.

Select File- Export -Wire shark tcpdump format and choose any suitable destination.

This will save the logs with a .cap extension to that location.

CRACKING

Run Aircrack-ng GUI.

Choose WEP.

Open your .cap file that you had saved earlier.

Click Launch.

In the command prompt type in the index number of your target wireless network.

Wait for a while. If everything goes fine, the wireless key will be shown.

You may also receive a request to try with more packets. In this case wait until more packets have been

captured and repeat the steps to be performed after capturing packets.

VIDEO (for those who can't understand the steps)

http://www.youtube.com/watch?v=knMUDo5a_Xw#t=276

SOURCE : http://mods-n-hacks.wonderhowto.com/