Aircrack ng windows tutorial

what am I going to learn? You'll learn how to install Aircrack-ng on your Windows computer. Requirements Difficulty Tutorial Content First Step: Download and unpack the Aircrack-ng file. Personally, I prefer to move the .rar file to my desktop to have a clearer work area. If your web browser doesn't ask you where to save the file, then just go to the Download section of your explorer file. Here's what it should look like: Step two: Determine if your Windows architecture is 64-bit or 32-bit. You should get something like this: The Third Step: Go to Your Local Drive (C:) and open the Program Files or Program Files (x86) folder depending on the window architecture. Since my Windows 64-bit I will choose the folder Files program. Then copy and paste the Aircrack-ng folder, which you haven't been pressed in front of in the program files folder. The Aircrack-ng folder should look like this in the program files folder. Once you've entered the Aircrack-ng folder into the Program Files or Files (x86) folder, you should go inside that folder. Once inside the folder you have to open the folder bin. Depending on the Architecture of Windows, you'll choose a folder according to Windows. In my case I chose a 64-bit folder because my Windows architecture is 64-bit. Once inside the relevant folder, you will have to copy the address of this folder as shown below: The Fourth Step: Now you have to go to this computer properties again. Once you get the box below, you'll have to leave a click on the Advanced Settings system as it is in the picture shown below. Now you have to press a button that says: Environment variables ... Once you get inside the Environmental Variables you have to get a screen just like this: Once you've got that box, you'll have to press the New Pointed button with an arrow. In this new window you have to write (the way) inside the Variable name window:. Then you will have to insert an address that you copied earlier in a step #4 in the Variable value field: All procedures are shown below. After that, just click the Good button on all the open windows. Also, click the Apply button if you see the option. Final step: Go to your desktop and press Ctrl and R to open the Run program. Inside Run type cmd, as shown below. Then click OK you have to get a box like this below Now that you have opened the cmd you will have to enter aireplay-ng inside the cmd. Then click enter. You should get a set of information just like this in the picture above. Now you're done and ready to use it. Training program Installation AirCrack-ng on Windows Setting AirCrack-ng No cap'tulo 3 comentei que, ao contr'rio do WEP, o WPA e WPA2 n'o possuem falhas conhecidas de seguran'a, que permitam descobrir a chave rapidamente. Apesar disso, ainda and poss'vel usar ataques de for'a bruta para descobrir passphrases f'ceis, baseadas em palavras do or simple sequences of numbers. Let's better see how this process works. The first step is to install the aircrack-ng package, the successor to the aircrack package that we used earlier, which contains the tools that we will use. To work, it needs a wireless map to support the monitoring mode, which is supported by default on dander and fewer drivers. In most cases, you first need to change the card drivers by downloading the source, installing the patch, and compiling the modified driver. To do this, you need to install kernel blanks and basic compilers. You can find detailed information on how to do this in conjunction with several boards in: . Another option is to use BackTrack, which already comes with patches installed. To apply the test, start by using Kismet to detect the SSID and the channel you want to test with, as well as access POINT MAC and MAC addresses of at least one customer who is connected to it. If you're testing your own network, just check the information in the hotspot configuration. The next step is to use airmon-ng to capture the authentication process of one of the network customers. It is based on the use of a four-century handshake where a series of four packages is used to negotiate a cryptographic key between the client and the access point, which is then used to encrypt the authentication process. Of course, capturing this sequence of packages doesn't detect the phrase of the network, but offers the ability to perform a brute force attack, testing multiple features until you find the right key. Start by putting the wireless card in monitor mode, using the Airmon-ng starter interface, as in: Airmon-ng start eth1 In the case of cards with Chipset Atheros, you need to disable the interface ath0 and recreate it in monitor mode, using commands: Airmon-ng stop ath0 airmon-ng to start Wi-Fi0 The next step is to capture the authentication process of one of the customers. Let's do this by opening two terminals. The first will be used to rotate the airodump-ng and thus capture the gears, and the second to rotate the aireplay-ng, disabling the customer and forcing him to reconnect with the hotspot so that the packages can be captured. At the first terminal activate airodump-ng, indicating where the file will be written with the captured packages, the channel used by the access point, and the interface as in: airodump-ng-w logrede --channel 2 ath0 With this, the file logrede.cap will be generated in the current catalog. At the other terminal, launch the aireplay-ng-deauth 1 team, by specifying the MAC address of the access point (-a) and the customer's MAC address to be disabled (-c) as in: -a 00:50:50:81:41:56 -c 00:19:7D:4C:CA:07 This command forces your computer to send a distorted package to the access point, simulating the process of disabling the customer Deceived by the package, the access point disables the customer, leading to its re-authentication, and then a process that works automatically by most operating systems. The authentication process will be recorded by a capture started at another terminal. To carry out a dictionary-based attack, you must use a text file containing a list of words that will be tested. There are several dictionary files widely available on the Internet (search for word lists on Google), such as a repository available on most distributions, you will also find a list of words, which can be used as a file /usr/share/dict/words, and you can also buy a CD with a collection of files containing lists with words from all languages in: word file in hand, use the command below to check the combinations, specifying the SSID network, file with words and file with capture packages (generated by airmon-ng) as in: $ aircrack-ng-ng-and network-w-wi-cap.txt. where the network points to the SSID network, dict.txt indicates the location of the dictionary, and logrede.cap indicates a capture file. You must specify the SSID network because it is one of the information included in the authentication process. The test is done offline using captured authentication packages to simulate the authentication process using each of the words included in the file. The amount of processing required for each of them makes the test take a long time. The Celeron-M 1.4 GHz, for example, can handle (even with all the optimizations included in aircrack-ng) only about 100 capabilities per second, bringing the pace to 360,000 combinations per hour, or 8.64 million combinations per day. It may seem like a lot, but at this rate it will take more than a million years to test all the possibilities of an 8-character phrase containing letters, numbers and special characters (and exponentially longer for longer phrases). That's why the attack focuses on word-testing rather than testing all possibilities. You can also use John the Ripper to test variations of dictionary words, which allows you to detect phrases based on variations or combinations of words such as paralep1ped0, which is quite common. You can download it in: use it, unpack the file, access the folder src (inside the created folder), and turn make the commands. This will create a program running in the running folder that can then be run like in ./john. John is a widely used tool for password testing because he can launch brute force attacks by checking all combinations or using a dictionary file in all kinds of password files. In our case, we will use John to process the dictionary file by directing the output to the aircrack-ng. The team will be: $./john-wordlist'dict.txt-rules--stdout aircrack-ng-and network-w logrede.cap As you can see, the WPA key hacking process takes quite a while and, despite this, it is ineffective against phrases built with random characters, especially in the case of long phrases. With the current generation of programs, you can secure your network using a good phrase. A long phrase, with 20 characters or more (except for a combination of two or more words), cannot be broken by brute force. The only way to access the network will be to convince one of the users to reveal it. One solution to this latest problem would be to use an easy-to-remember phrase (imagine a case of a phrase with 50 characters or more :). Then you can print the overflow on paper, enter it into the client to authorize the connection, and then destroy the printed copy. aircrack-ng windows tutorial pdf. aircrack ng gui windows tutorial. aircrack-ng tutorial windows 7. aircrack-ng 1.5.2 windows tutorial. aircrack-ng wpa2 tutorial windows. aircrack ng tutorial deutsch windows 10. aircrack-ng tutorial en español windows 7