WiFi... sí, gracias!

Publicado por Manuel Jimenez on martes, 1 de septiembre de 2015 Etiquetas: herramientas , wi-fi

¿Tienes Wi-Fi? - Claro. - ¿Cuál es la clave? pagarlo!

No sé si acaso es debido a mi timidez o que no suelo causar buena impresión a menos de 50m (y en foto). ~~Ahora que me pongo a pensar.!!!...quizás sea debido a mi problema con el alcohol o a mi natural vicio de ir en pelotas, o a mi animadversión a la autoridad... mis ojos blancos... o mi raro problema con las drogas y el Skateboarding no sé...., no pagar las multas, ver vikingos, jdt ...no sé,...~~ .

Los 50mtrs me parecen una medida perfecta para... casi cualquier cosa... las palabras... radiofrecuencia y... aburrimiento... hacen un cocktail perfecto. He de confesar que desde hace un año pago mi wifi...~~.pero por jugar al battlefield sin lag.~~ Por lo demás es una grandísima mi....rada hacia el pasado...

Se que a muchos de vosotros (como a mi) os gusta leer poesía, ir de entierro, conocer al padre de vuestra novia, y por su puesto odiáis a aquella gente que prefiere bajarse las fotos de la boda del vecino, o gorronearle el media center.. Sea como fuera, coñas a parte.....

Hoy os traigo un puñado de herramientas para auditar redes wifi *made in Spain* que después de probarlas me han dejado la boca como a una veinteañera después de comerse una pera ~~o era después de comerle las peras .. a una. vein .~~..jojojo como estoy hoy!

Perdón ahora si, sin tonterías..

Después de repasar unos vídeos reparé en la charla (brillante y sencilla, como

deben ser las cosas) de la gente de **Lallakk** que dieron en la Rooted, que dicho sea de paso hoy por hoy, estas herramientas se han hecho imprescindibles en mi *home*....

La primera que vamos a ver es una herramienta muy sencilla escrita en python de la cual ya no puedo pasar aunque quiera, se llama **lk_wifi_device_finder.py** y la podéis bajar directamente de la página de sus creadores http://www.layakk.com/ en la sección de lab.

La herramienta en sí, nos ayuda a determinar cual es la mejor posición para recibir una determinada señal y emite una serie de pitidos en base a la calidad ésta. Veamos como funciona...

```
usage: lk_wifi_device_finder.py [-h] -i INTERFACE [-r REFRESH_INTERVAL]
                                (-m MAC | -e ESSID) [-t] [-s] [-w]
```

Para hacerla operativa en nuestros sistemas tenemos una serie de pequeños requisitos:

```
python-scapy python-pyaudio libasound2
```

```
root@bigben:/home/manuel# ifconfig wlan1 down
root@bigben:/home/manuel# iwconfig wlan1 mode monitor
root@bigben:/home/manuel# ifconfig wlan1 up
root@bigben:/home/manuel# iwconfig wlan1 channel 1
root@bigben:/home/manuel#
```

Bajamos la interfaz, la ponemos en modo monitor, la levantamos y elegimos el canal a escuchar. Tras esto y después de darle permisos de ejecución arrancamos la aplicación pasándole los argumentos que deseemos.

```
root@bigben:/home/manuel/wifi# ./lk_wifi_device_finder.py -i wlan1 -m 00:00:00:00:00:0

Initializing PyAudio...
       (Warning messages about server socket and jack server are normal and may
 be discarded)
Cannot connect to server socket err = No such file or directory
Cannot connect to server request channel
jack server is not running or cannot be started

Starting to measure. Press Ctrl-C to finish.
__[      ]
__[  -51 ]_____________________________
__[  -51 ]_____________________________
__[  -51 ]_____________________________
__[  -50 ]_____________________________
__[  -50 ]
```

Aparte estamos recibiendo en todo momento una señal acústica la cual se hace mas notable conforme nos acercamos a la mejor posición para recibir la señal, esta característica hace a esta *tool* la mar de practica.

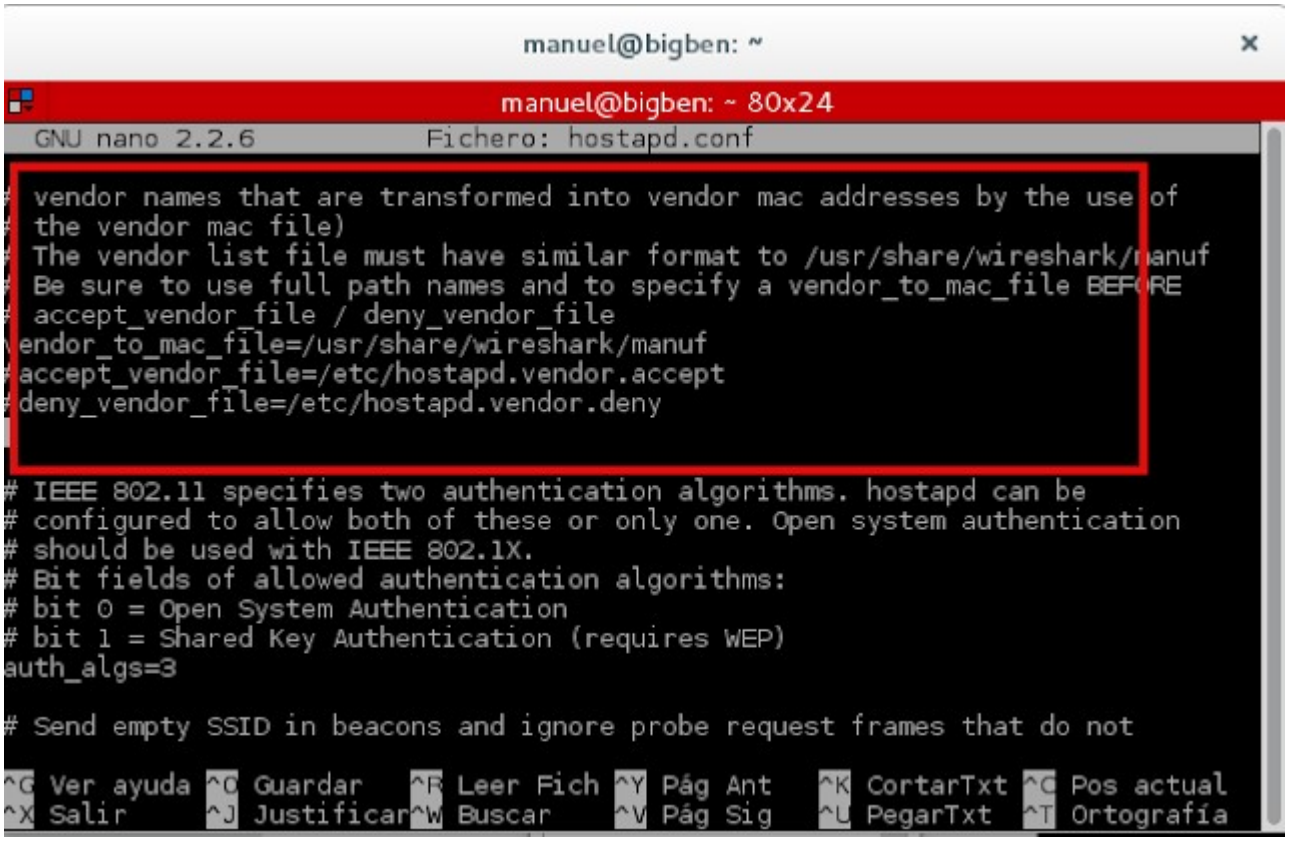
La siguiente utilidad que os quiero presentar son realmente unos parches para ***hostap*** (sabéis como me gusta esta herramienta que me esta siendo últimamente muy útil). Su nombre

El parche en cuestión dota a hostap de nuevas propiedades: La principal sería que podemos ser capaces de elegir a quien le damos servicio dependiendo del fabricante, y la otra da la capacidad de anonimizar las macs que salen por pantalla y en los logs.

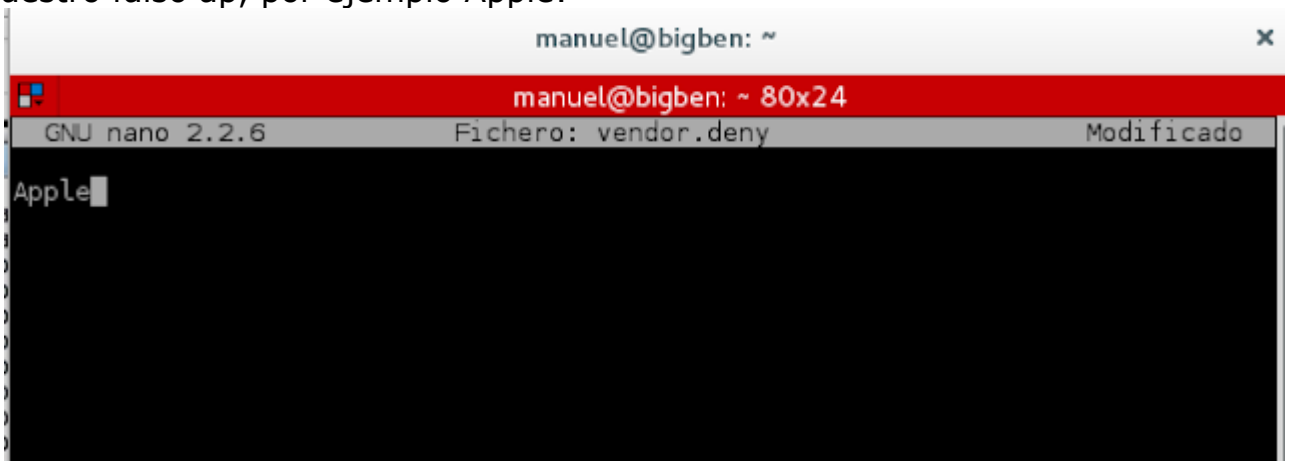
Para ello debemos compilar hostap desde las fuentes aplicando parches (aquí solamente aplico el parche de vendors).

```
root # git clone git://w1.fi/srv/git/hostap.git
root# cd hostap
root/hostap#patch                -p1</home/manuel/wifi/lk_hostap_patch-
v1.0/patch_layakk_hostap-Vendor_ACLs-
a60dbbce443d62c403492549a1353ed1a3eaefb4
root/hostap# cd src/
root/hostap/src#make & make install.
```

Para arrancar nuestro fake ap con su nueva funcionalidad necesitaremos generar y modificar un par de archivos; crearemos *vendor.deny* y modificaremos el fichero de configuración de hostap donde le diremos cuál es la ruta a este archivo (*vendor.deny*)..



En vendor.deny pondremos los fabricantes que no queremos que se conecten a nuestro falso ap, por ejemplo Apple:



y luego arrancamos hostap normalmente... http://www.hackplayers.com/2014/01/rogue-ap-sin-airbase.html

Por último el plato fuerte. Para quien se haya enfrentado a los resultados que arroja kismet en un ámbito wifi concurrido, puede llegar a ser una locura dar con los datos que te interesan.

A ésto, los chicos de Layakk han encontrado una solución bastante práctica: lk_k2db v1.0.

Cómo funciona: debemos coger el resultado de kismet (un .xml) lo pasamos por lk_2kdb.py el cual nos genera una base de datos. Luego tenemos una serie de scripts en la carpeta *scripts* para hacer consultas y cruzar datos de una manera muy pero que muy practica...

Tampoco tiene desperdicio su control de servos (el cual confieso que lo estoy utilizando en alguna cámara de vigilancia casera..),

lk_servo_system.py_v1.0 lk_servo_system.conf.example lk_pantilt.py v1.1
la cual se puede auto ajustar robóticamente con:
lk_beam_finder.py v1.0
Lo mejor es que si queréis mas detalles veáis la demo (esta en "fuentes").

Un saludo ...

Fuentes: David Perez y José Picó - Ampliando el arsenal de ataque Wi-Fi

2 comentarios :

1. *Profesor_xo*2 de septiembre de 2015, 19:00

   y como contrarestrar esos tipos de ataques fakeAP?

   Responder

2. 

   *Manuel Jimenez*5 de septiembre de 2015, 9:12

   la pura verdad es que la mejor contra medida es el puro sentido común...desabilitar la reconexión automatica, y tratar de verificar los puntos de acceso a los que te conectas, luego como deporte si localizar un falso ap siempre puedes dosearlo...