Hostbase guia completa

Hostbase : Herramienta de wifi para kali-linux y wifislax

P1 Instalacion sobre kali-linux.

Hostbase es un script ruby que usa muchas dependencias, en este caso vamos a instalar las dependencias.Abre un terminal y entra eso:

apt-get install -y build-essential upgrade-system subversion wget g++ iptables iptables-dev pavucontrol ffmpeg sqlite3 libsqlite3-dev libssl-dev libnl-3-dev libnl-genl-3-dev dsniff isc-dhcp-server pkg-config xterm freeradius apache2 php libapache2-mod-php php-cli tcpdump scapy vokoscreen wireshark python-twisted bridge-utils devscripts gengetopt autoconf libtool make

Ahora empezamos con las dependencias de ruby y la interfaz grafica (GUI).Se entra eso, cada linea es un comando a entrar:

gem install rake

gem install bundler

apt-get install ruby

apt-get install ruby-dev

gem install highline

apt-get install libgtk2.0-dev

gem install gtk2

Eso hecho, queda el mas importante, hostapd.Por no tener problemo en los ataques que usan mas de un falso AP se tiene que descargar hostapd y hacer la compilacion, vamos a empezar:

* si tienes hostapd instalado ya, quita lo para poner la nueva configuracion :
apt-get remove hostapd

P2

Instalacion y compilacion de hostapd :

wget http://hostap.epitest.fi/releases/hostapd-2.6.tar.gz

tar -zxf hostapd-2.6.tar.gz

cd /root/hostapd-2.6/hostapd

cp defconfig .config

nano .config

Ahora estas en el fichero de configuracion y de compilacion de hostapd.Aqui vamos a quitar este symbol '#' antes de las opciones que pongo aqui :

CONFIG_DRIVER_NL80211=y

CONFIG_LIBNL32=y

CONFIG_EAP_PWD=y

CONFIG_WPS=y

CONFIG_WPS_UPNP=y

CONFIG_WPS_NFC=y

CONFIG_RADIUS_SERVER=y

CONFIG_IEEE80211N=y

CONFIG_IEEE80211AC=y

CONFIG_DEBUG_FILE=y

CONFIG_FULL_DYNAMIC_VLAN=y

CONFIG_TLSV11=y

CONFIG_TAXONOMY=y

P3

Una vez hecho, podemos pasar a la instalacion final de hostapd:

sudo make

sudo make install

hostapd -v

* Se encontra algunas errores en la instalacion pero no molesta los pasos.

Ya se tiene todo instalado para que hostbase anda sin errores,Vamos a pasar a la configuracion de apache2 en la pagina siguiente (P4),

P4

Configurar bien el servidor web apache2 es una cosa muy importanta para que la pagina de phishing se ve bien.Hay que modifiar el camino por defecto de los ficheros de apache2 y eso se hace en este fichero : /etc/apache2/sites-available/000-default.conf

Aqui pongo el mio:

```
ServerAdmin webmaster@localhost

        DocumentRoot /var/www/

ServerName maboxadministration.cf

        <Directory />

                Options FollowSymLinks

                AllowOverride None

        </Directory>

        <Directory /var/www/>

                Options Indexes FollowSymLinks MultiViews

                AllowOverride None

                Order allow,deny

                allow from all

        </Directory>
```

No hay que tocar a ServerName: maboxadministracion.cf es una configuracion mia,Lo que hay que hacer es verificar que el DocumentRoot esta en /var/www/ y no /var/www/html y hacer igual con el Directory un poco mas a bajo.

P5

Tambien hay que modificar los derechos de ficheros por no tener problemo despuès, son esas lineas :

```
 AllowOverride None

 Order allow,deny

  allow from all
```

Una vez este fichero modificado vamos a ir en el fichero /etc/apache2/apache2.conf.

Verificamos que todo esta bien /var/www/ (lo tiene que ser por defecto).

```
<Directory />

        Options FollowSymLinks

        AllowOverride None

        Require all denied

</Directory>

<Directory /usr/share>

        AllowOverride None

        Require all granted

</Directory>

<Directory /var/www/>

        Options Indexes FollowSymLinks

        AllowOverride None

        Require all granted

</Directory>
```

Después de eso se entra en la carpeta paginaAQUI del archivo de hostbase y se copia todo lo que hay en el repertorio /etc

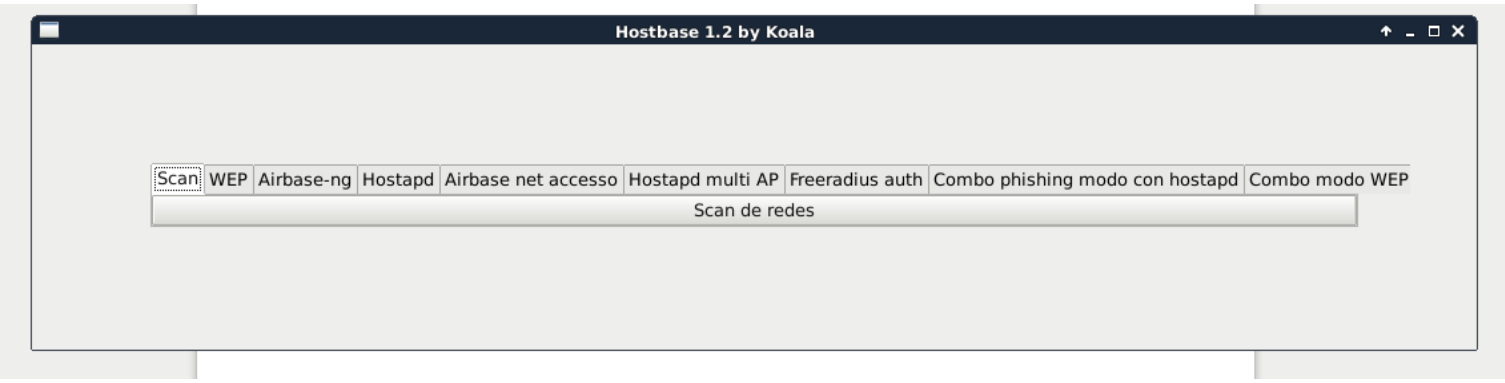
P6

Iniciar hostbase y empezar a elegir el attaque

Toda la instalacion y la configuracion esta hecha, vamos a poder ejecutar el script.Copia y pega la carpeta hostbase-1.1 a dentro el repertorio /tmp ponte a dentro la carpeta hostbase-1.1 y ejecuta lo :

ruby hostbase.rb

Y hasta,



En primero lugar es muy importante de empezar por el scan de redes,Asi apagamos network-manager que da problema con hostapd, y tomamos las informaciones sobre las redes (no cierras la ventana de airodump).

Y llegamos a el punto el mas importante, elegir un plano de ataque.El ataque depende de los usarios que estan conectado a la red y con cual dispositivo estan conectado.Una ves que el scan de redes esta terminado, hay que saber con la MAC del usario si es un dispositivo movil o si es une ordenador.Es facil de saber eso con este sitio dondé puedes entrar la direccion MAC: https://macvendors.com/

No te dira de que dispositivo es pero lo puedes saber facil, ejemplo con mi MAC: 0c:84:dc:70:80:c7 = Hon Hai Precision.co.ltd

Podemos ver que es un ordenador porqué si fuera un movil saldra cosas asi :

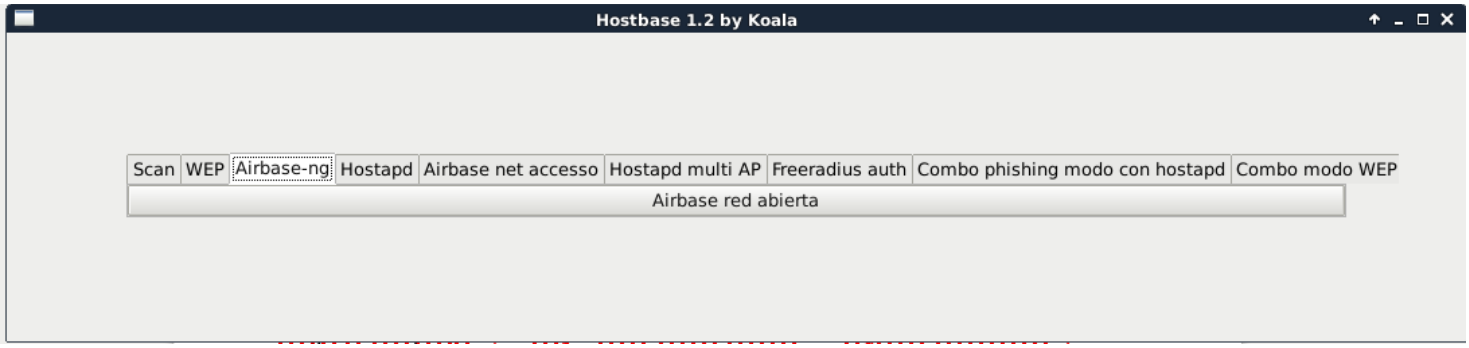
Samsung electronic, HUAWEI, Motorola.corp etc.

P7

Si se tiene duda se puede buscar mas informaciones en internet sobre la MAC del usario, con el movil si no tienes accesso a ninguna red.

Ahora que sabemos que dispositivo esta conectado a la red vamos a poder elegir el ataque.Lo que voy a decir ahora andara en algunas situaciones y en otras no, pero es lo que haria en este caso.Si hay solamente moviles de conectado consejo de usar el modo airbase-ng o el modo multi AP abierto.

Modo airbase-ng



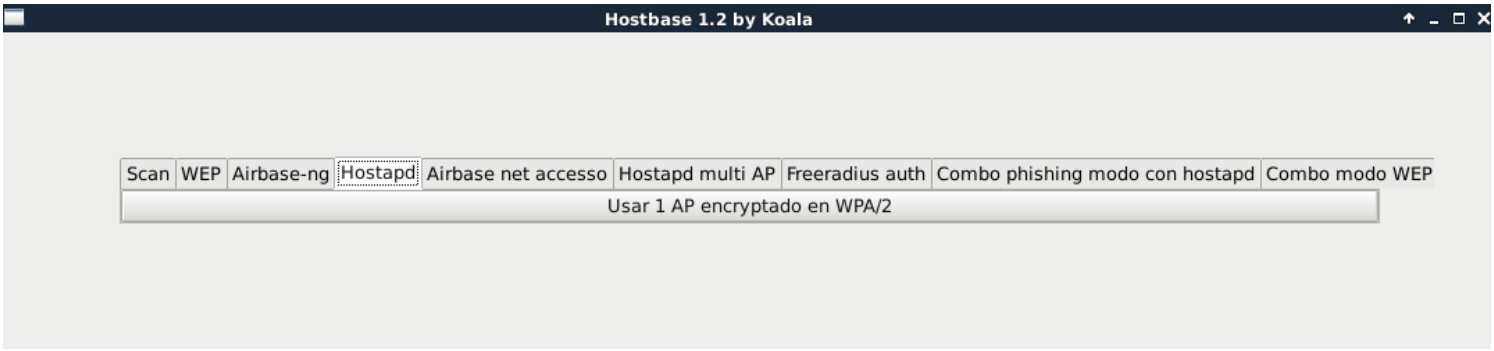
Hostbase puede hacer falsos AP en WPA o sea porqué usar airbase-ng ?

Porqué los android no pueden conectarse a las redes en WPA usando el WPS,Hay que ir en los parametros wifi del dispositivo android para que se conecta sobre el WPS y la mayoridad de los usarios no saben dondé es.Hostbase déjà el WPS activado cuando anda con redes en WPA, y los ordendores detectan en séguida ese typo de conexion, no los moviles.

Que hacer si son solamente ordenadores conectado ?

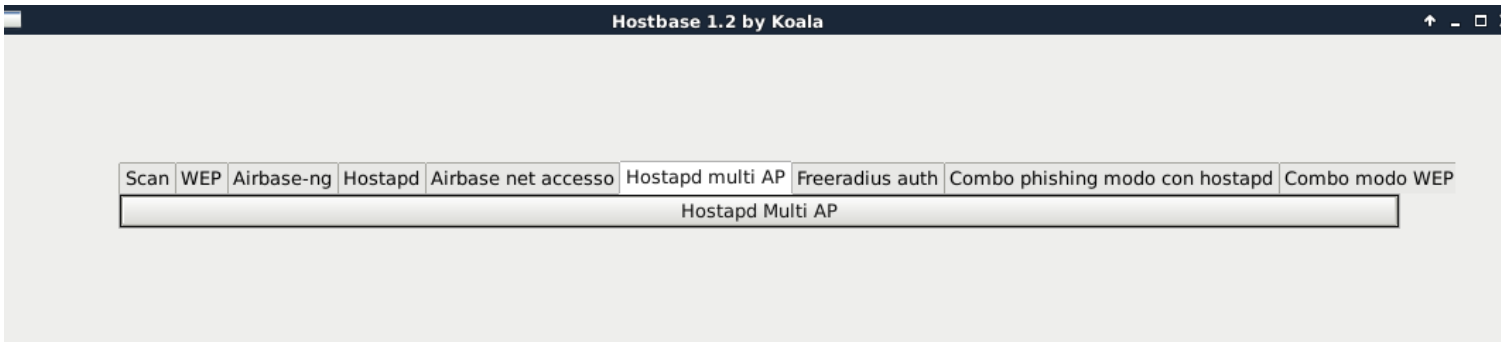
Se puede usar el modo hostapd con 1 red en WPA o el modo multi AP que hace hasta 3 redes (2 en WPA y la ultima abierta).

Modo hostapd



P8

Modo Hostapd multi AP



Que hacer si hay 1 movile y 1 ordenador connectado a la red o 2 moviles y 1 ordenador connectado a la red ?

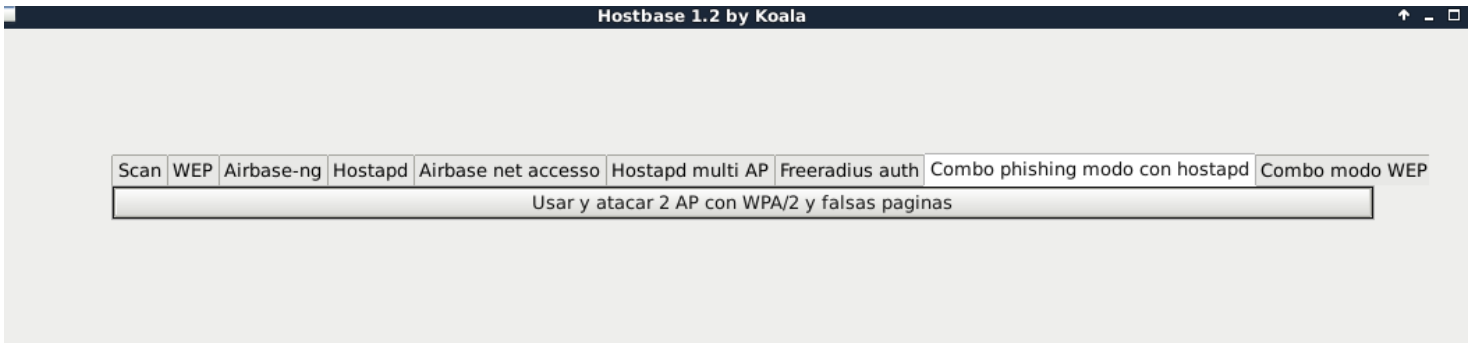
En este caso consejo de usar el modo hostapd, porqué ?

Porqué la pagina de phishing esta mas bonita cuando se ve desde un ordenador, y el ordenador sera en la mayoridad del tiempo, el ordenador del admin de la red.

Que hacer si tienes 2 redes con un signal fuerte que tienen por lo menos 2 usarios conectado a cada una ?

En este caso puedes usar el modo combo phishing,

Modo combo phishing



P9

El modo combo phishing va atacar 2 redes al mismo tiempo pero hay que indicar los MAC de los usarios para que ponga la buena pagina de phising y que los usarios de la red1 no se encontra con la pagina de la red2… Ejemplo de configuracion.

Asi hemos visto un poco lo que hostbase puede hacer, y ese documento sirve para los usarios de wifislax tambien.Para salir del script y dejar todo bien se hace un ctrl+c en la consola. Ahora que hemos terminado con kali-linux vamos a pasar con la version de hostbase para wifislax.

P10

Wifislax hostbase

Hay 2 version de hostbase para wifislax, una facil y una mas avanzada.Para usar la version facil se descarga el archivo wifislaxairbase.

Instalacion :

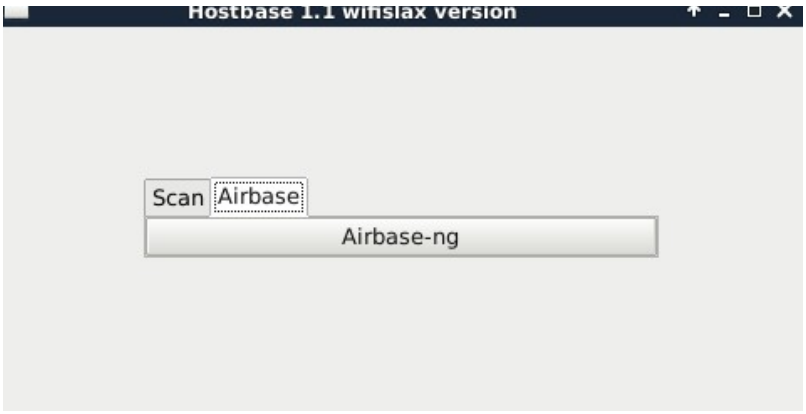
Se entra en la carpeta wifislaxairbase y se ejecuta el script de instalacion :
bash instalacion.sh

Este script te pondra las paginas en /etc y el fichero de configuracion de httpd.Tambien te dira si puedes usar el script o no.

Después se copia la carpeta wifislaxairbase en el repertorio /tmp y se entra a dentro la carpeta wifislaxairbase para ejecutar el script :
ruby airbase.rb

En primero lugar es muy importante de empezar por el scan de redes,Asi apagamos network-manager que dar problemo.No cierras la ventana de airodump después que el scan se ha terminado, te lo necesitara.

Una vez que has tomado los informaciones sobre la red puedes iniciar airbase-ng.



P11

Ejemplo de configuracion.

Después no tienes nada que hacer.Si se tiene problemos mira mi video en youtube para la configuracion : https://www.youtube.com/watch?v=WsFyYh8y9EQ
Tambien hay que dar la salida de consola del script de instalacion en los foros.Para salir del script y dejar todo bien se hace un ctrl+c en la consola.

Version avanzada de hostbase para wifislax

La version avanzada de hostbase para wifislax (nombre del archivo wifislax) puede hacer casi igual que la de kali-linux.Una vez descardo se inicia el script de instalacion a dentro la carpeta hostbase-1.1 y se copia la carpeta hostbase-1.1

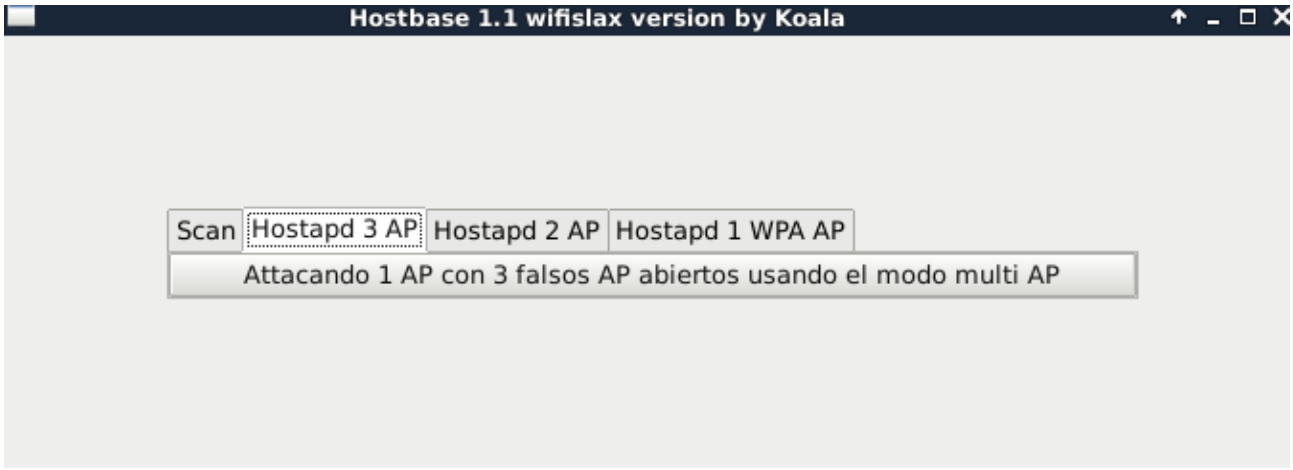
en /tmp, desde la carpeta hostbase-1.1 que esta en /tmp inicia el script :
ruby hostbase.rb

Igual que la version facil, se tiene que empezar por el scan de redes.

Asi apagamos networ-manager y podemos usar hostapd.

P12

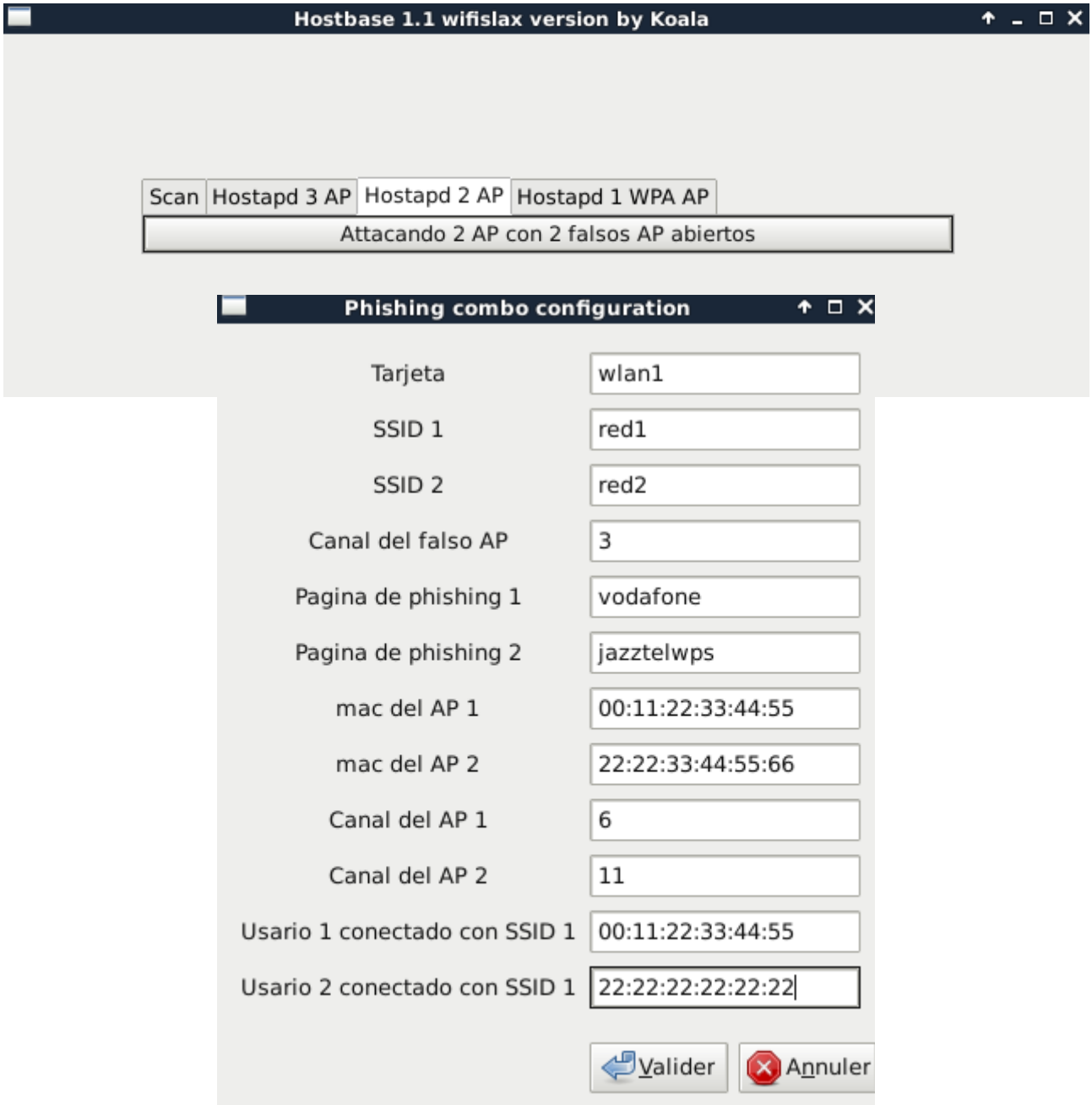
Ejemplo con el modo multi AP



Como podeis ver se pide la MAC de los usarios, eso es porqué hacemos 3 redes abiertas y para que no nos molesta alguien que no esta de la red a piratear, ponemos un filtrado MAC.Como puedes ver, no hace falta tener 3 usarios conectado a la red, si hay solamente 2 se entra los 2 y hasta.Se sale sel script con ctrl+c en la consola.

P13

Ejemplo con el modo que ataca 2 redes al mismo tiempo

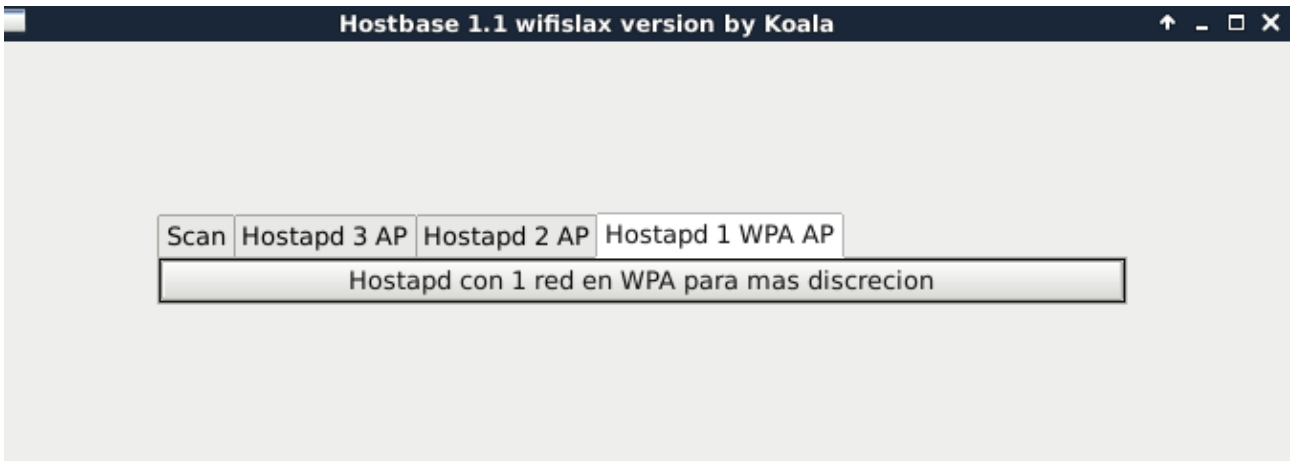


P14

Como podeis ver, aqui hay que entrar las 2 MAC de los usarios conectado a la red1.

Eso es para que podemos bien hacer un filtrado entre la red1 y la red2 y para que los usarios de la red1 no se encontran con la pagina de phishing de la red2…

Si hay ordenadores de conaectado y que quieres hacer solamente 1 red en WPA, usa la opcion : hostapd 1 WPA AP (ver P7 y P8 para saber cuando usar eso).



Ahora hemos terminado de ver lo que hostbase pueda hacer.La pagina sigiente sirve para los que tienen errores.Se sale sel script con ctrl+c en la consola.

P15

Tengo un error que hacer ?

La primera cosa a hacer es de copiar la salida de consola cuando se produce el error, véo un monton usarios que se creen que soy jesus… no puedo ayudar si no sé nada del problemo.

- Errores que llegan muchas veces y solucion.

```
nl80211: Could not configure driver mode
nl80211 driver initialization failed.
hostapd_free_hapd_data: Interface wlan0 wasn't started
```

Eso es que tu tarejata no esta compatible con hostapd, o que network-manager esta iniciado.Entre 2 pruebas hay que apagar network-manager antes de volver a ejecutar el script.Por defecto network-manager se inicia a cada fin de ataque.

Kali comando :

systemctl stop NetworkManager.service

systemctl disable NetworkManager.service

Wifislax comando : service stop networkmanager

Error cuando se inicia hostap:

Too many open files in system

Eso es que hay hostapd iniciado ya o mal apagado, solucion : killall hostapd && airmon-ng check kill

Error : could'nt load gtk2

La interfaz grafica no esta instalado… no estas usando el ultimo ISO de desarollo de wifislax.Que se queda bien claro, Hostbase anda solamente con el nuevo ISO de desarollo y no version antiguas.

P16

Error : no encuentro la clave wifi.

La clave wifi esta en la carpeta /var/www/msftconnecttest/cle.txt

Lo puedes ver directamenter con el comando :

cat /var/www/msftconnecttest/cle.txt

Ver pagina siguiente para usar el tchat,

P17

Desde la ultima revision hostbase include un shoutbox (tchat) para hacer sse pasar por el servicio tecnico, el usario tiene un url que se llama ayuda en linea en la falsa pagina.

Para poder responder a el usario pongo a bajo las url que hay que copiar y pegar

a dentro el navegador web que tienes.
Orange : http://127.0.0.1/msftconnecttest/orangeshout/orangechat.php
Vodafone : http://127.0.0.1/msftconnecttest/vodashout/vodatchat.php
Ono : http://127.0.0.1/msftconnecttest/onoshout/onotchat.php
Movistar : http:127.0.0.1/msftconnecttest/movistarshout/movitchat.php
Jazztel : http://127.0.0.1/msftconnecttest/vjazzshout/jazztchat.php

Descargar version para kali-linux :
https://github.com/Koala633/hostbase/blob/master/hostbase-1.1.tar.gz

Descargar la version de wifislax facil :
https://github.com/Koala633/hostbase/blob/master/wifislaxairbase.tar.gz

Descargar la version de wifislax avanzada :
https://github.com/Koala633/hostbase/blob/master/wifislax.tar.gz

HostbaseByKoala

Official facebook page :
https://www.facebook.com/koala633hostbase/

Soporte en wifi-libre :
https://www.wifi-libre.com/topic-1011-hostbase-12-

esta-aqui-page-3.html#p10304

Guia completa : https://www.wifi-libre.com/topic-756-una-historia-de-rogue-ap-el-pdf-de-koala-traducido-al-espanol.html

Y lampiweb : http://lampiweb.com/foro/index.php?topic=15974.msg127842;topicseen#new