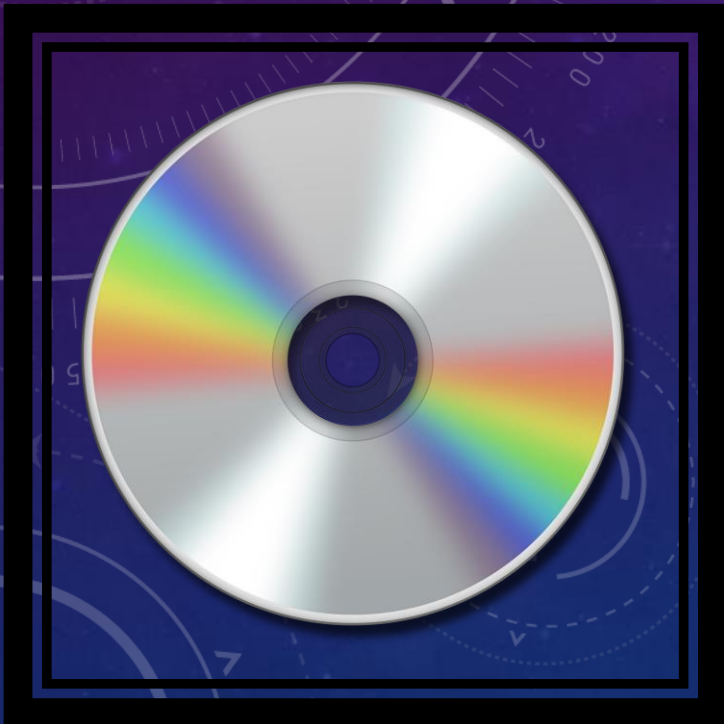






¿QUÉ ES WIFISLAX?

Es un Sistema Operativo Linux Live, que contiene herramientas para auditar redes Wi-Fi.
Se puede instalar en la mayoría de dispositivos:
discos duros, CD/DVD, Pen Drive...



¿QUÉ VENTAJA NOS OFRECE?

Nos permite comprobar la seguridad de una red ante posibles vulnerabilidades mediante el uso de sus herramientas.

WEP

WPA

WPA2

PRINCIPALES HERRAMIENTAS: WIFITE 2

Fácil de usar

Encriptación
WEP

WIFITE2

Obtiene
contraseñas

No necesita
diccionarios


```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

NUM  ESSID          BSSID          CH  ENCR  POWER  WPS?  CLIENT
-----
1    (00:23:        00:23:        3  WEP   99db   no    client
2    (CC:96:        CC:96:        3  WPA   99db   no    client
3    AP Galeria     A0:F3:        9  WPA2  58db   no
4    Mznlabsec      5C:33:        7  WPA2  49db   wps   client
5    WLAN_26        00:01:        6  WEP   44db   no    clients
6    WLAN_F912      F4:3E:        2  WPA   34db   wps   client
7    MOVISTAR_DD4D  E4:C1:        2  WPA   32db   wps
8    WLAN_86        40:4A:        3  WEP   32db   no
9    MOVISTAR_CF3E  F8:1B:        1  WPA   32db   wps   client
10   Orange-D3A3    9C:80:        11 WPA2  32db   wps
11   REAL MADRIT    00:C0:        11 WPA2  31db   no
12   WLAN_32        00:01:        9  WEP   31db   no
13   Monter        00:25:        6  WPA2  30db   no
14   WLAN_XX        38:72:        11 WPA2  30db   no
15   Familia        00:26:        11 WEP   30db   no
16   MOVISTAR_7716  E4:C1:        1  WPA   30db   wps
17   MOVISTAR_8008  F8:C3:        1  WPA   30db   wps   client
18   JAZZTEL_C3B8   F8:8E:        11 WPA   29db   no
19   BIBLIOTÉCA1    10:FE:        11 WPA2  29db   wps
20   JAZZTEL_4FAC   38:72:        6  WPA   29db   no

[0:01:53] scanning wireless networks. 20 targets and 11 clients found
```

WIFITE2

ESSID

Nombre de la red.

BSSID

MAC del Punto de Acceso.

WPS

PIN de 8 dígitos para facilitar la conexión al Punto de Acceso.

```
[+] scanning (mon0), updates at 5 se

root : sh :

[0:10:00] preparing attack "Familia" (00:26:...)
[0:10:00] attempting fake authentication (1/5)... success!
[0:10:00] attacking "Familia" via arp-replay attack
[0:07:04] started cracking (over 10000 ivs)
[0:01:28] captured 50154 ivs @ 79 iv/sec

[0:01:28] cracked Familia (00:26:...)! key: "A52..."
```

PRINCIPALES HERRAMIENTAS: LINSET

Un poco más
complicado

Encriptación
WPA y WPA2

LINSET

Obtiene
contraseñas

Obtiene fácilmente el
handshake
(contraseña encriptada)

```
Internet Systems Consortium DHCP Server 4.3.4
Copyright 2004-2016 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/wlan0/9c:d3:6d:e[REDACTED] 192.168.1.0/24
Sending on LPF/wlan0/9c:d3:6d:e[REDACTED] 192.168.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.
DHCPREQUEST for 192.168.1.15 from 40:[REDACTED]:92 via wlan0: unknown lease 192.168.1.15
DHCPREQUEST for 192.168.1.15 from 40:[REDACTED]:92 via wlan0: unknown lease 192.168.1.15
DHCPREQUEST for 192.168.1.15 from 40:[REDACTED]:92 via wlan0: unknown lease 192.168.1.15
DHCPREQUEST for 192.168.1.15 from 40:[REDACTED]:92 via wlan0: unknown lease 192.168.1.15
█
```

```
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.1
█
```

```

PUNTO DE ACCESO:
Nombre.....: ONOD[REDACTED]
MAC.....: 9C:D3:[REDACTED]
Canal.....: 11
Fabricante.....: NETGEAR INC.,
Tiempo activo...: 00:00:04
Intentos.....: 0
Clientes.....: 0

CLIENTES ACTIVOS:
```

LINSET

```
Desautenticando con mdk3 a todos de ONOD[REDACTED]

Periodically re-reading blacklist/whitelist every 3 seconds

Disconnecting between: 40:[REDACTED]:A:92 and: 9C:D[REDACTED]:76
Disconnecting between: FF:[REDACTED]:F:FF and: 9C:D[REDACTED]:76 on channel: 11
Disconnecting between: BC:[REDACTED]:7:E6 and: 9C:D[REDACTED]:76 on channel: 11
Disconnecting between: FF:[REDACTED]:F:FF and: 9C:D[REDACTED]:76 on channel: 11
Disconnecting between: BC:[REDACTED]:7:E6 and: 9C:D[REDACTED]:76 on channel: 11
Packets sent: 145 - Speed: 8 packets/sec█
```

Iniciar sesión en red

Login Page

ESSID: ONOD [redacted]
BSSID: 9C:D3:[redacted]
Chan: 11

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

Introduzca su contraseña WPA:

Enviar

Capturando datos en el canal --> 11

CH 11][Elapsed: 18 s][2016-12-04 22:07][WPA handshake: 9C:D3:[redacted]

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
9C:D3:[redacted]	-86	44	102	475 0	11	54e	WPA2	CCMP	PSK	ONOD [redacted]

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
9C:D3:[redacted]	40:C6:[redacted]	-43	1e- 1e	0	410	
9C:D3:[redacted]	BC:8C:[redacted]	-76	1e- 1e	0	30	ONODF [redacted]
9C:D3:[redacted]	04:02:[redacted]	-78	0 - 1	0	7	ONODF [redacted]

LINSET

Esperando la pass

[00:00:00] 1/0 keys tested (78.08 k/s)

Time left: 0 seconds inf%

KEY FOUND! [540 [redacted]]

Master Key : FD 5B F8 86 2B 8E DC F3 49 C1 C8 18 DD 3B 98 17
97 F6 5C 2F CD A3 4E CD B1 5C 05 68 F7 87 4D 11

Transient Key : 9C 58 FD 57 E1 95 AE E2 D2 D1 1A 89 69 47 51 D2
77 10 CB D4 FD 45 85 0F AD 18 8E 35 2C BD 14 1E
5C 6F 01 AD 39 F1 85 2B 96 E3 91 7A BC 9F E2 75
BF E8 5B 67 22 B7 A5 48 CA D2 48 E7 B1 0F BF 52

EAPOL HMAC : 21 CF B7 E8 13 48 7A CD ED AE 59 43 78 B2 0C C3

Se ha guardado en /root/ONOD[redacted]-password.txt