
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA


# Vulnerabilidades en redes WiFi

## ELO-323

## Redes de Computadores 2

**Profesor: Agustín Gózales**
**Ayudante: Jesús Márquez**

**Alumno:**
**Rodrigo Jiménez Castro (ROL: 201304292-9)**
**rodrigo.jimenez.13@sansano.usm.cl**

**Fecha de Entrega: Viernes 21 de Diciembre de 2018**

**Documento compuesto con LaTeX**

# Índice

# 1. Introducción

La seguridad inalámbrica es un tema para el mundo moderno, ya que tanto para empresas como para usuarios domésticos, es importante asegurar los principios de seguridad como son la confidencialidad, autenticidad e integridad de los mensajes.

El presente trabajo consiste en entender y comprobar como se llevan a cabo los distintos ataques a las redes WiFi, específicamente a mecanismos para lograr conectarse al respectivo Access Point de la red objetivo. Para ello se investigará los conceptos de ELO323 involucrados en el tema, luego, una vez entendidos se procederá a realizar dichos ataques a una red local de hogar, donde se configurara el Access Point para encriptar la conexión con distintos protocolos creados y se observara como vulnerar cada uno de ellos.

# 2. Conceptos Involucrados

El desarrollo del proyecto involucra principalmente los tópicos de Seguridad Inalámbrica de la asignatura y algunos investigados particularmente, como lo son los siguientes:

## 2.1. Protocolo WEP

Wired Equivalent Protocol, es el protocolo lanzado junto con el estándar de redes inalámbricas IEEE 802.11 en 1997. Entre sus principales características se encuentran el Vector de Inicialización IV, el mecanismo CGC-32 y la clave RC4. Más Información

### 2.1.1. Vulneravilidad WEP

La vulnerabilidad de este protocolo esta dada principalmente porque utiliza el mismo vector de inicialización IV para cada paquete de un mensaje. En base a esto, un intruso puede estimular el AccessPoint para generar respuestas, a modo de obtener vectores IV suficientes como para realizar un análisis estadístico y de esta forma encontrar la clave. Más Información

## 2.2. Protocolo WPA

WiFi Protected Access, es el siguiente protocolo de seguridad inalámbrica. Lanzado en 2001 junto con el estándar IEEE 802.11i, es similar a WE, pero con una marcada diferencia: este utiliza un mecanismo TKIP para cifrar los mensajes, que a diferencia de el vector IV, este genera un numero distinto para cada paquete de cada mensaje. Más Información

### 2.2.1. Contraseñas y Ataques por Fuerza Bruta

Con la evolución de la tecnología, se crearon interfaces bastante amigables para usuarios no expertos en el tema, las cuales permiten cambiar la contraseña de fabrica por una más fácil de recordar. Si bien es mas amigable para el usuario, también lo es para un atacante, ya que al usar palabras conocidas puede ejecutarse un ataque por fuerza bruta, es decir, probar distintas combinaciones de números y letras, hasta encontrar la correcta. Esto aumenta su eficiencia con el uso de diccionarios con palabras de un determinado idioma. Más Información

#### 2.2.2. WPS y ataque a WPS

Con la evolución de las redes, cada vez mas dispositivos requieren acceso a un Access Point mediante WiFi, algunos de estos con una interfaz de usuario básica, sin teclados por ejemplo. Para esto nace WPS (Wifi Protected Setup), un mecanismo pensado en estos casos, donde conectarse sea muy simple. Este mecanismo utiliza un pin de 8 dígitos que debe coincidir en ambos dispositivos. Es en este punto donde el mecanismo se vuelve inseguro, ya que se puede ejecutar un ataque por fuerza bruta sobre el WPS para intentar encontrar el pin, y en un peor caso, buscarlo en un diccionario esperando sea algun pin de fabrica conocido. Más Información

### 2.3. Protocolo WPA2

Es la versión certificada de WPA, actualmente es el mecanismo más seguro para encriptar contraseñas WiFi. Su principal característica es que cambia el mecanismo TKIP por AES, que es su versión mejorada. Este protocolo tiene las mismas vulnerabilidades de WPA antes mencionadas, además de las siguientes.Más Información

#### 2.3.1. Ataque por desconexión y falsa interfaz

Este método obedece la filosofía: *"Si no puedes encontrar la contraseña, has que te la den"*. Se trata de un método que busca desconectar a un usuario de su red y al mismo tiempo levantar otra red con el mismo nombre, en la cual al intentar conectarse el usuario se le pedirá su contraseña WPA2, el cual al ignorar que se trata de un formulario falso, la ingresara, obteniéndola instantáneamente el atacante. Más Información

#### 2.3.2. KRACK's

Se trata de un moderno ataque efectuado durante un paso del llamado *4 way handshake* entre el host y el Access Point. En este punto se negocia una llave que se utilizara para el cifrado de los mensajes entre estos, y específicamente en el paso 3 el AP envía una llave al host, pero cuando se desea efectuar este ataque, el host no avisa al AP que la recibió, por lo que el AP seguirá enviando llaves cíclicamente, llaves que se pueden utilizar para descifrar mensajes entre un host y un AP, lo que vulnera la confidencialidad e integridad de la comunicación.Más Información

## 3. Parte Práctica

### 3.1. Descripción e Implementación

Para comprobar las vulnerabilidades se utilizaran los siguientes elementos:

- Equipo Arris (Router + AP)
- Antena WiFi USB
- PC con LiveCD WifiSlax

La idea es configurar el Access Point del Equipo para encriptar una contraseñas en los distintos protocolos, para los cuales se proponen los siguientes ataques:

- Protocolo WEP: Se propone atacar mediante el Software GOY, el cual descifra la contraseña mediante la obtencion de muchos vectores de inicializacion IV.
- Protocolo WPA: Se propone atacar por WPS, por medio del Software Geminis.
- Protocolo WPA2: Se propone atacar por fuerza bruta, mediante los softwares Handsheaker y Brutus, con los cuales se obtiene el handshake y la contraseña respectivamente.

## 3.2. Resultados Obtenidos

### 3.2.1. Ataque a WEP

Se configura el Access Point con encriptacion WEP de 64 bits

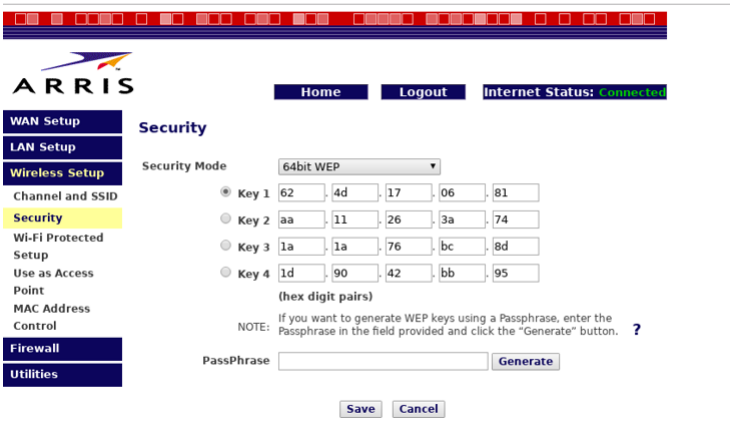


Figura 1: Access Point encriptado por WEP

En seguida se utiliza el software GOY WEP de WifiSlax para comenzar el ataque encontrando suficientes vectores IV:

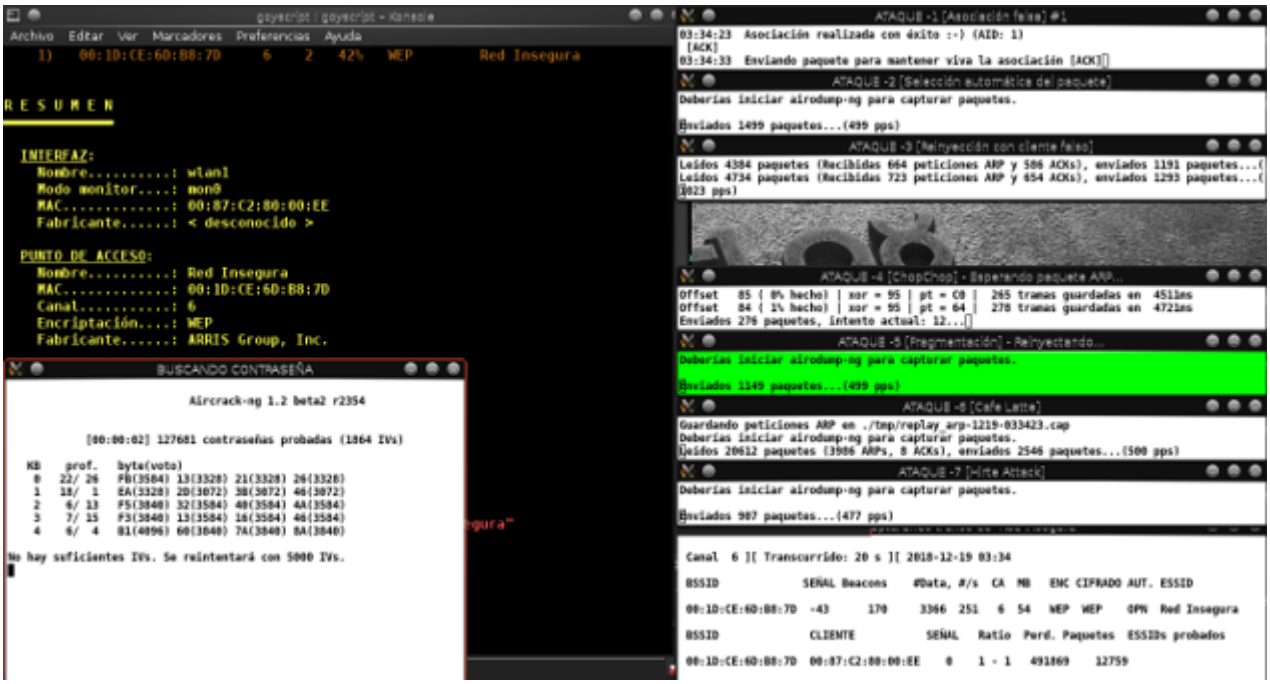


Figura 2: GOY Atacando

Finalmente luego de un tiempo la clave WEP es descifrada:

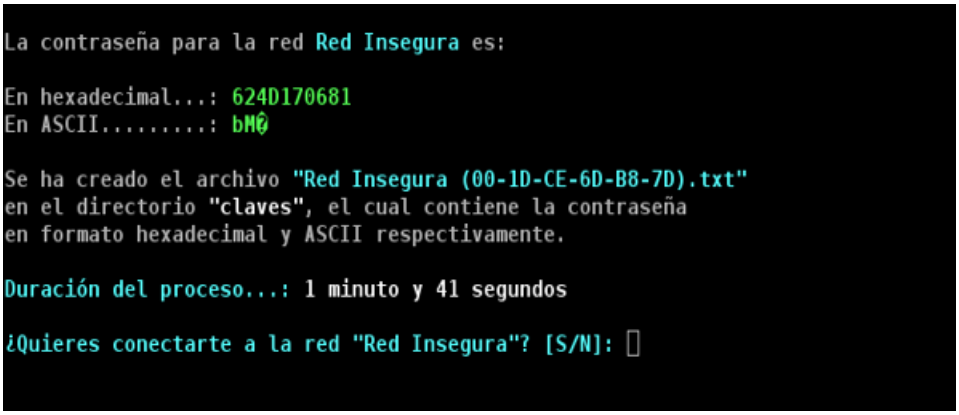


Figura 3: Clave WEP descifrada

La figura 3 muestra que el ataque fue exitoso.

### 3.2.2. Ataque a WPA

Se configura el Access Point para encriptacion WPA y se activa el WPS:


Figura 4: Access Point encriptado por WPA

La figura 4 muestra la clave por defecto 12345670 activada, la cual será vulnerada. En seguida se procede a atacar el WPS por medio del Software Geminis:

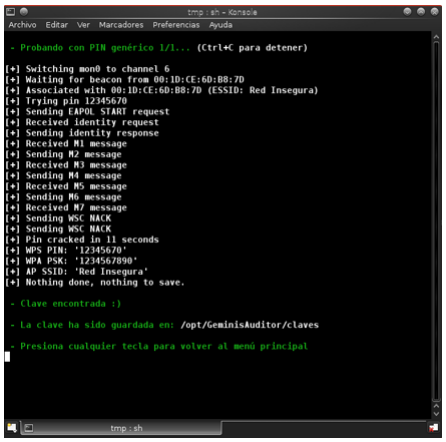


Figura 5: Software Geminis Atacando Satisfactoriamente

La figura 5 muestra que el ataque por WPS fue exitoso.

### 3.2.3. Ataque a WPA2

Se configura el Access Point con encriptacion WPA2 con clave 12345678

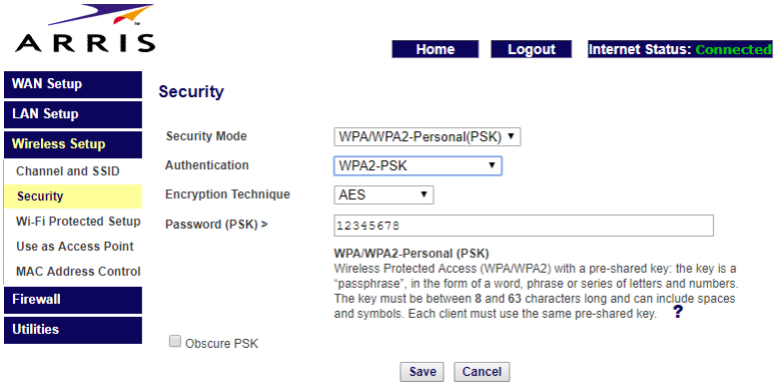


Figura 6: Access Point configurado para WPA2

En seguida se procede a capturar el handshake, para ello se utiliza el software Handshaker:

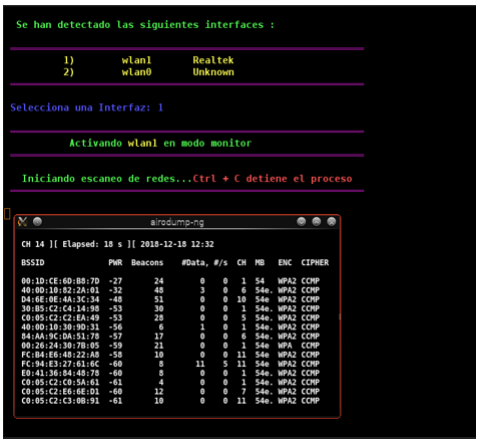


Figura 7: Software Handshaker esperando una conexion

Luego de que encuentra alguna conexión, captura el respectivo handshake a un archivo

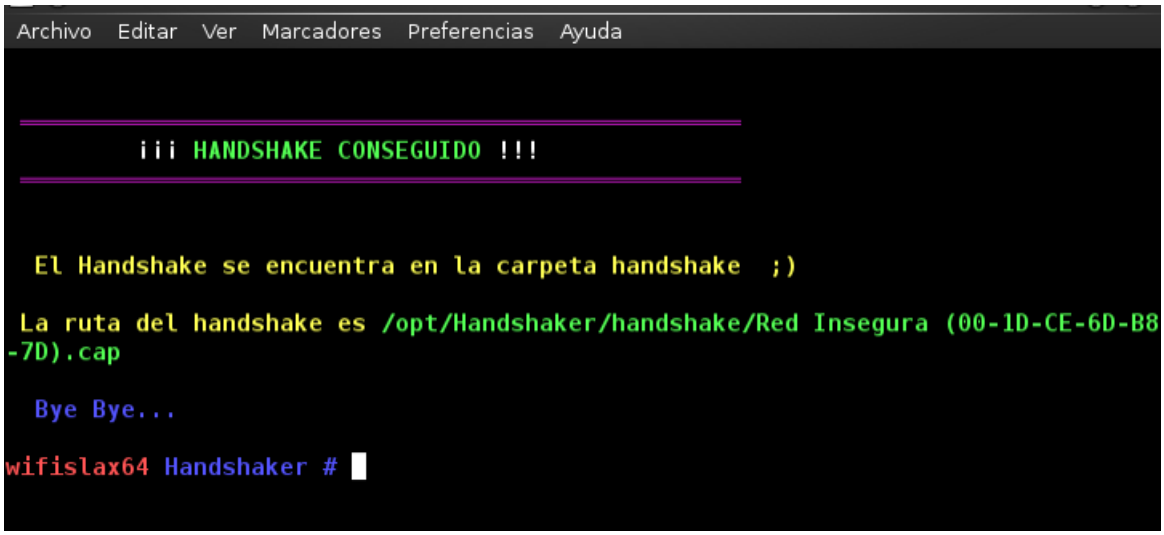


Figura 8: Software Handshaker capturando el handshake

Luego, se utiliza el archivo generado en la figura 8 como entrada al Software Brutus, el cual sera el encargado de encontrar la clave WPA2 por fuerza bruta. A modo de prueba se limita el rango de numeros a probar, haciendolo variar en un rango de 10000, hasta que encuentra la contraseña:

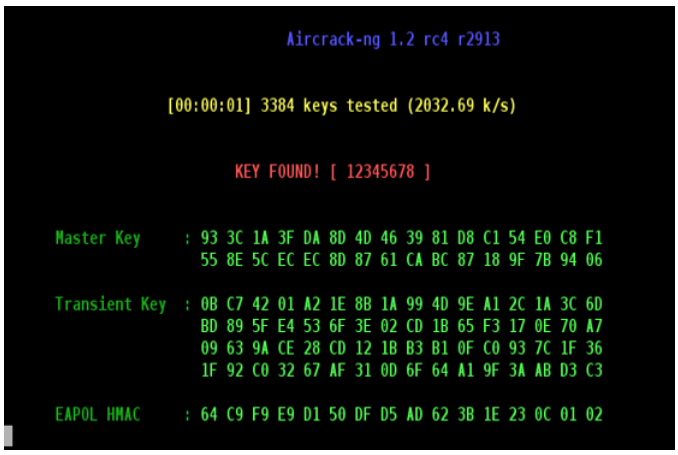


Figura 9: Software Brutus Atacando Satisfactoriamente

La figura 9 muestra el satisfactorio ataque por fuerza bruta.

# 4. Conclusiones

Del presente trabajo se puede concluir que a medida que las tecnologías de seguridad evolucionan, pasado un tiempo van apareciendo ciertas vulnerabilidades en ellas que no estaban previstas, dejando paso a que los atacantes puedan actuar en ellas. Es por esto que estudiar del tema y conocer como funcionan puede ayudarnos a aumentar la seguridad de nuestras redes simplemente tomando algunas precauciones, como es el caso de usar contraseñas difíciles de adivinar, o poniendo atención frente a redes con nombre duplicado, etc.