Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 9: Configuración de seguridad y ataques en redes inalámbricas

1- Introducción

Una red inalámbrica de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a una red de datos, en lugar de los cables coaxiales, UTP o cables de fibra óptica que se utilizan en las LAN convencionales. Las principales diferencias entre una red cableada y una red inalámbrica son:

- ***Perímetro de la red:*** todo usuario que se encuentre en el área de cobertura de la red inalámbrica se convierte en un posible usuario (autorizado o malicioso)
- ***Movilidad:*** no es necesario que el ordenador esté conectado a una clavija.

Seguridad en redes inalámbricas

El objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas, enlazando los diferentes equipos o terminales móviles asociados a la red. Pero a la vez que obtenemos ventajas de facilidad de uso el uso de un medio "universal" y "accesible" como la ondas de radio hace que la red sea más vulnerable a posibles ataques, ya que elimina la necesidad de las redes convencionales de obtener un acceso físico a la red, que en muchos casos exigía un acceso físico a los edificios, donde se encuentran los puntos de conexión de la red.

Las principales amenazas de una red inalámbrica son:

- Escuchas ilegales
- Acceso no autorizado a la red
- Interferencias

Cómo se encuentra una red wireless

En redes que funcionan a través de un punto de acceso (AP), cada AP envía alrededor de 10 paquetes (llamados "beacon frames") por segundo. Estos "beacon frames" contienen la siguiente información:

- Nombre de la red (ESSID)
- Si usa encriptación y de qué tipo; a veces puede no ser legible.
- Qué velocidades soporta el AP.
- En qué canal (frecuencia) se encuentra la red.

Esta información aparecerá en la utilidad que use para conectarse a la red. Se muestra cuando ordena a su tarjeta que escanee o busque (scan) las redes que están a nuestro alcance con **iwlist <interface> scan** y también cuando ejecutamos un sniffer inalámbrico como airsnort o airodump-ng, o el clásico wireshark seleccionando la interfaz inalámbrica.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

2- Objetivos

- Conocer el funcionamiento básico de una red WiFi con un punto de acceso (Access Point) comercial y clientes WiFi PCs con sistema operativo Linux.
- Configuración de PCs como clientes de este AP conectados mediante el sistema de distribución cableado.
- Conocer las vulnerabilidades de una red inalámbrica abierta y una con protección WEP.

3- Configuración de equipos

El primer paso para preparar la práctica es utilizar los interfaces inalámbricos disponibles en los equipos del laboratorio y un punto de acceso Cisco Linksys que también se encuentra en cada uno de los armarios.

Clientes inalámbricos

Los equipos PC-A y PC-C de cada armario tienen un interfaz inalámbrico bajo el nombre de dispositivo ***ath0***. En primer lugar active el interfaz (***sudo ifconfig ath0 up***). Ahora puede localizar los puntos de acceso a su alrededor con:

```
% iwlist ath0 scan
```

Para gestionar la parte inalámbrica de un interfaz tenemos que utilizar el comando ***iwconfig*** (recuerde utilizar *sudo* para realizar cambios).

Mediante iwconfig podemos realizar las siguientes operaciones clásicas:

- Conectarnos a un punto de acceso según el essid (*sudo iwconfig ath0 essid nombre*).
- Definir la clave de encriptación de la red(contraseñaWEP)(*sudo iwconfig ath0 key clave*)
- Establecer parámetros de configuración del interfaz inalámbrico: ratio (rate) de transferencia, canal de escucha, etc.

Ejecuta *iwconfig* en un terminal para ver la información que nos muestra. Podemos ver qué interfaces de los disponibles tienen extensiones inalámbricas. Encontrará un interfaz llamado `wifi0`, propio del driver madwifi-ng, utilizado habitualmente en Linux por ser de código abierto y permitir configurar prácticamente cualquier parámetro del chipset Atheros que integra la tarjeta WiFi instalada en los PCs A y C. Este interfaz sólo indica la presencia física de una tarjeta con dicho chipset, no es un interfaz configurable, su correspondiente interfaz configurable es el `ath0`. Identifique los distintos parámetros asociados a dicho interfaz inalámbrico ***ath0***, en especial:

- ESSID (**E**xtended **S**ervice **S**et **Id**entifier)
- Mode
- Frequency(channel)
- Access Point(AP)

(Como ayuda consulte el manual del comando *iwconfig*)

¿Cuál es el nombre del protocolo que define el estándar WiFi?

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Nota-Importante: Para poder escuchar tráfico en la red, sin estar asociado a ella, es necesario poner la tarjeta inalámbrica en modo ***monitor*** mediante el comando `wlanconfig` (ver man wlanconfig), destinaremos el PC-C para este fin. El equipo PC-A debe estar en modo ***managed****(es el modo por defecto de la interfaz ath0)*. El cambio de modo de trabajo de una interfaz inalámbrica requiere la destrucción previa de la misma mediante el comando `wlanconfig`, que deberá ejecutar como root:

```
sudo wlanconfig ath0 destroy
```

Para posteriormente crearla en el modo deseado:

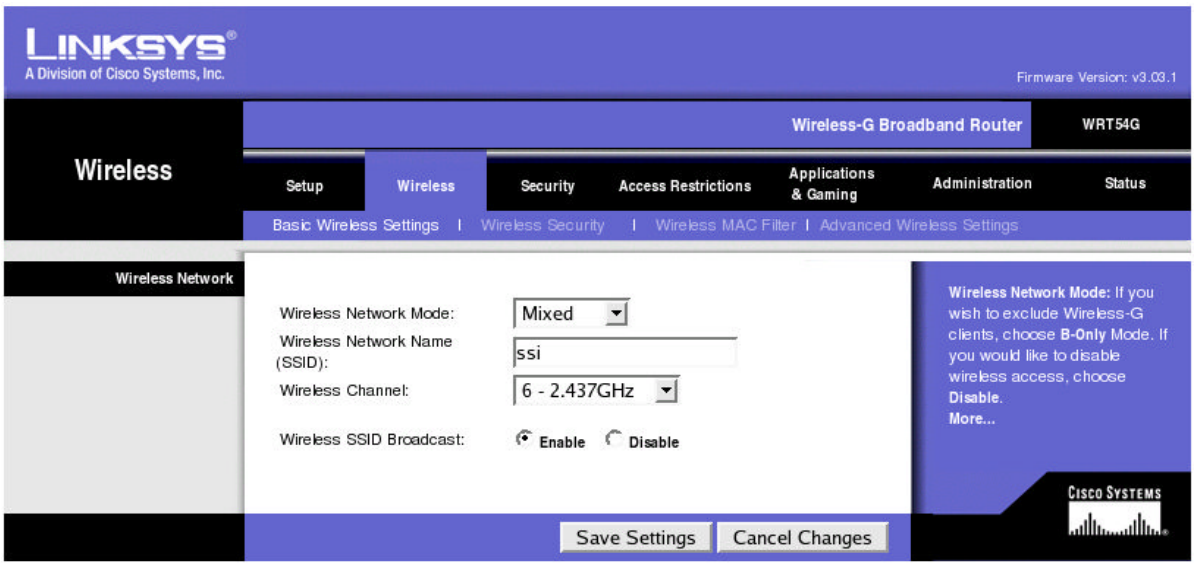
```
sudo wlanconfig ath0 create wlandev wifi0 wlanmode managed "o bien"
sudo wlanconfig ath1 create wlandev wifi0 wlanmode monitor
```

La etiqueta ath0 está reservada para el modo por defecto managed y ath1 para el modo monitor. Para esta práctica sólo necesitará activar una de ellas, destruya la otra si dispusiera de las dos. Una vez creada la interfaz, actívela con `ifconfig` y verifique su nuevo estado con `iwconfig`. Cambiar el modo de trabajo de la interfaz inalámbrica requiere la destrucción previa de la misma.

Punto de Acceso

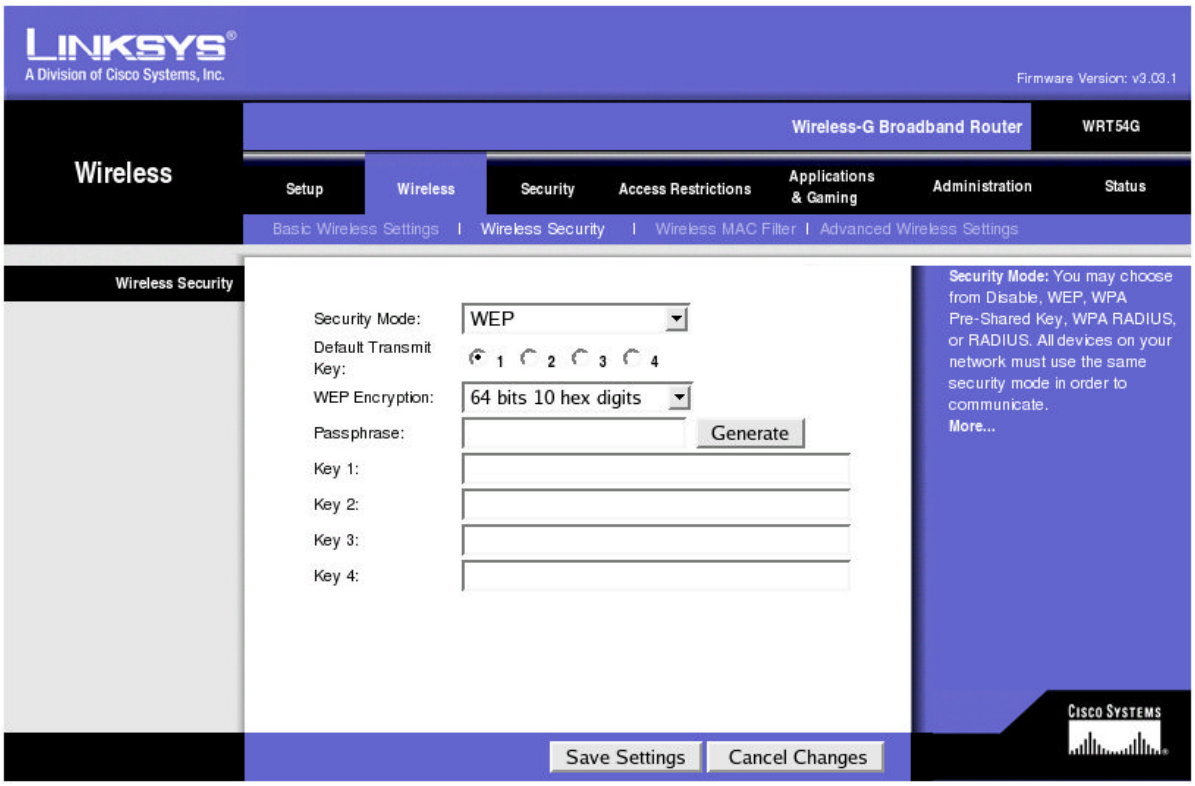
Se trata de un Cisco Linksys WRT54G que soporta el estándar 802.11g y ofrece ratios de transferencia de hasta 54Mbps. Realmente es un router que tiene dos interfaces de red, uno considerado LAN y otro WAN. Además integra un switch de 4 puertos LAN.

Para preparar el punto de acceso primero tenemos que **resetearlo** (para eliminar toda configuración de otras prácticas). Pulsamos el botón de ***reset*** que se encuentra en la parte posterior del equipo, hasta que veamos que la luz de Power parpadea. Una vez realizada esta operación, el equipo se reinicia según la configuración de fábrica y ya podemos conectarnos a él. El equipo ofrece un servidor Web con una página de administración y tiene configurada la dirección IP por defecto **192.168.1.1**. El usuario y contraseña para acceder son **admin/admin**. Podemos gestionar toda la parte inalámbrica, además de las configuraciones clásicas de un router. Para gestionar la parte inalámbrica tenemos que ir al apartado *WIRELESS,* desde el que accederemos a los subapartados, *Basic Wireless Settings* y *Wireless Security*, los únicos que configurar en esta práctica.



Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es



Nota-Importante: Tiene que salvar en cada pantalla y antes de abandonarla, los cambios realizados, de lo contrario los perderá.

4- Escenario inalámbrico abierto

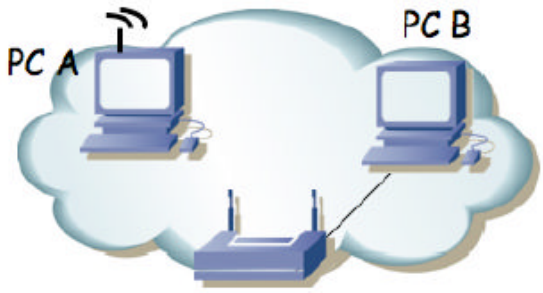


Figura 1.- Accesspoint y cliente

Configure el escenario inalámbrico de la figura 1:

1. Conecte el PC-B a la LAN cableada del punto del acceso.
2. Accespoint. Acceda a su página web de administración desde el PC B para configurar la parte inalámbrica del punto de acceso con los siguientes datos:

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

a. ESSID de la red: ssixx (xx *es su número de cuenta de prácticas. 01, 02, 03, etc.*)
b. Tipo de seguridad: *disabled*
c. Canal: x (x *es su número de armario*)

3. Conecte el PC-A mediante red inalámbrica a la red local a través del punto de acceso (utilice el comando *iwconfig*, debe indicar la red a la que quiere conectarse mediante la opción *essid*, así como el canal WiFi o su frecuencia).

Compruebe las comunicaciones entre los diferentes elementos (PC-B con Punto de Acceso y con PC-A).

Nota: Recuerde asignar una dirección IP a cada interfaz, para hacerlo sobre los interfaces inalámbricos tiene que utilizar igualmente el comando `ifconfig` (***`sudo ifconfig ath0`***)

Checkpoint 9.1: Verifique la asociación de PC-A con el AP, comprobando la dirección MAC de este y su ESSID. Para ello, utiliza el comando `iwconfig ath0`, e inspecciona la sección Status del AP.

El equipo PC-C será un equipo considerado externo que escuchará las comunicaciones entre PC-A y PC-B sin estar asociado a la red WiFi ssixx. Para ello, configure adecuadamente su interfaz inalámbrico ***ath0*** y seleccione un canal WiFi. ¿Cuál? ¿Por qué? ¿Necesitará configurar a ***ath0*** una dirección IP? ¿Por qué? (Recuerde las ocasiones en las que ha utilizado un PC conectado a una *red cableada compartida (hub)* para esnifar tráfico).

Desde el PC-C utilice tcpdump o wireshark para ver todas las tramas y estudie:

- Los beacons enviados por el AP.
- El proceso de asociación del PC-A (desactive y vuelva a activar su interfaz para verlo).
- El envío de paquetes entre un host en la red inalámbrica y otro en la LAN cableada (filtre adecuadamente la captura obtenida).

Establezca una comunicación entre PC-A y PC-B mediante un socket abierto (nc –l <puerto>) en uno de ellos (por ejemplo en PC-B) y una conexión (telnet o nc) desde el otro (PC-A).

Escuche desde el PC-C todo el tráfico que se genere en la comunicación entre PC-A y PC-B (no tenemos que conectar PC-C a la red WiFi, dejaría registro, en el punto de acceso, de que lo hemos hecho, y no queremos eso). Supongamos que la información que estamos transmitiendo es una información sensible o una contraseña; capturar con tcpdump o wireshark dichas transmisiones.

Nota-Importante: Recuerde que para poder escuchar tráfico en la red WiFi es necesario poner la tarjeta inalámbrica en modo ***monitor*** *mediante el comando* `wlanconfig` *(ver* `man wlanconfig`*). El equipo PC-A (conectado a la red WiFi) debe estar en modo* ***managed****. Recuerde que el cambio de modo de trabajo de la interfaz inalámbrica requiere la destrucción previa de la misma, para, a continuación, crearla en el modo deseado. Verifique, siempre, su nuevo estado con* `iwconfig`.

Checkpoint 9.2: Muestre al profesor los datos obtenidos desde el atacante y demuéstrele que éste no está asociado a la red WiFi ssixx.

Si quisiera asociar PC-C a la red ssixx ¿Lo podría hacer? Verifíquelo.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

5- Escenario inalámbrico WEP

Para dotar de cifrado WEP (***Wired Equivalent Privacy*** o "Privacidad Equivalente a Cableado) al escenario inalámbrico de la figura 1 configure los equipos con los siguientes datos:

1. Punto de acceso (AP):
   a. ESSID de la red: ssixx (xx *es su número de cuenta de prácticas. 01, 02, 03, etc.*)
   b. Tipo de seguridad: *WEP*
   c. WEP Encryption: 64 bits
   d. Key 1: (diez caracteres hexadecimales)

2. Clietne WiFi (PC-A):

Para dotar a PC-A de acceso a la red inalámbrica protegida por WEP tienes que utilizar otra vez ***sudo iwconfig***, con los parámetros ***essid*** y ***key*** (ver man iwconfig). Recuerde que la clave será la clave hexadecimal introducida en el AP. Configure el interfaz ***ath0*** de PC-A en la misma red que el AP.

Compruebe que hay comunicación entre el PC-A y el AP.

Establezca una comunicación entre PC-A y PC-B, volviendo a escuchar desde PC-C (no tenemos que conectar PC-C a la red WiFi, dejaría registro, en el punto de acceso, de que lo hemos hecho, y no queremos eso). Supongamos que la información que estamos transmitiendo es una información sensible o una contraseña; capturar con tcpdump o wireshark dichas transmisiones.

Checkpoint 9.3: Muestre al profesor los datos obtenidos desde el atacante y demuéstrele que este no está asociado a la red WiFi ssixx

Intente asociar PC-C a la red ssixx ¿Qué tendrá que hacer? Verifíquelo.

6- Saltar la protección WEP de una red inalámbrica

Considerando el escenario inalámbrico WEP anterior realice sobre él alguno de los ataques descritos en clases de teoría.

Para ello dispone del grupo de programas `aircrack-ng`, consulte la siguiente referencia:

http://www.aircrack-ng.org/documentation.html

De entre los que necesitará básicamente `airodump-ng` y `aircrack-ng`. Consulte sus respectivos manuales para saber cómo indicarles las opciones necesarias según su escenario. Necesitará permisos de superusuario para lanzar cualquier programa de la suite aircrack-ng.

`airodump-ng` le va a permitir capturar tráfico que deberá guardar, mientras que paralelamente `aircrack-ng` estará analizando dichas capturas con el objetivo de descifrar la clave WEP.

Estas dos herramientas software le serán suficientes para un determinado tipo de ataques. Para otros tipos de ataques necesitará emplear además `aireplay-ng` (consulte su manual).

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Herramientas adicionales:

Generación de tráfico

Para generar una cantidad importante de tráfico puede utilizar el programa `iperf`, muy empleado para medir la capacidad de una conexión entre dos PCs.

A la hora de trabajar con `iperf`, tenga en cuenta la capacidad del enlace inalámbrico que le ofrece su AP. Averígüelo y téngalo en cuenta en las opciones de configuración de iperf.

Puede llegar a generar más tráfico, mediante distintas conexiones cliente-servidor con `iperf`, de menor capacidad, que con una sola de mayor tasa. Realice su propia configuración.

Un cliente-servidor típicos podrían ser:

Cliente: `$iperf -c <ipservidor> -u -P 5 -i 1 -p 5005 -l 1470 -f m -b 1M -t 600 -L 5001 -T 1`

Servidor: `$iperf -s -u -P 0 -i 1 -p 5005 -l 1470 -f m -t 600`

Si realiza correctamente su ataque, verá que puede descifrar fácilmente claves WEP de 64 bits. Considere aumentar la longitud de dicha clave hasta 128 bits. ¿Qué conseguirá con una clave de más bits? ¿Seguirá siendo vulnerable a sus ataques?

Checkpoint 9.4: Muestre al profesor los resultados obtenidos; paquetes necesarios y tiempo invertido en obtener la clave WEP de 64 bits.