DISPOSITIVOS Y REDES INALÁMBRICOS

Acceso restringido en WiFi mediante SSID oculto y filtro MAC. Seguridad mediante encriptación WEP.

OBJETIVO DE LA ACTIVIDAD

Los alumnos:

- comprenderán la peligrosidad de los accesos no autorizados a la conexión WiFi. Posteriormente aprenderán a configurar un punto de acceso con un nivel de seguridad mínimo, consistente en ocultar su SSID; finalmente, comprobarán como esta medida de seguridad es fácilmente superable por un agresor malintencionado.
- aprenderán a configurar un filtro de acceso por dirección MAC en el punto de acceso y observarán como una estación no autorizada no puede asociarse a la red; posteriormente, comprobarán como esta medida de seguridad es fácilmente superable por un agresor malintencionado que accede a la red suplantando la identidad de una estación autorizada.
- comprenderán el funcionamiento del mecanismo WEP, y aprenderán a configurar una BSS con este sistema de encriptación. Posteriormente, comprobarán como esta medida de seguridad es fácilmente superable por un agresor malintencionado.

La actividad completa estima la siguiente dedicación por parte del alumno:

Actividad presencial	Actividad no presencial
4 horas	6 horas

ACTIVIDAD NO PRESENCIAL

La actividad no presencial que deberá realizar el alumno antes de realizar esta actividad es la realización, en casa y de manera autónoma de los “Pasos Previos” de cada una de las partes en que se divide esta práctica.

PARTE 1: OCULTACIÓN DE SSID

Pasos previos

- Enumerar los posibles objetivos de un acceso no autorizado a una red WiFi.
- Conocer el proceso por el cual las estaciones descubren los BSS que tienen en cobertura.
    1. Procesos de scanning, asociación, reasociación.

2. Describir las tramas de gestión implicacas en estos proceso.

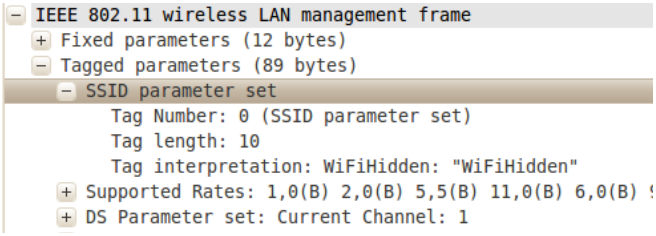
- Averiguar cómo configurar un punto de acceso con ocultación de SSID.
- Averiguar cómo conectar una estación Windows, Linux, iOS o Android a un punto de acceso oculto.
- Averiguar como utilizar la suite aircrack-ng para capturar todo el tráfico WiFi que hay en tu área de cobertura.

Bibliografía

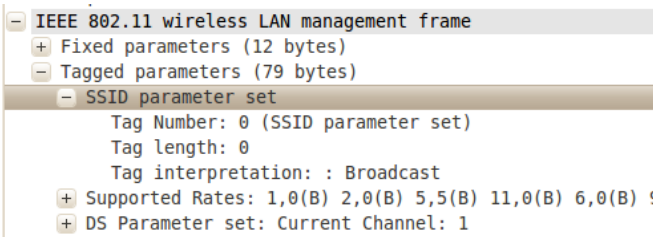
- Technet & Security, Up to secure. D-Link: Redes WiFi. Problemas y Soluciones. http://www.slideshare.net/chemai64/dlink-seguridad-wifi. Último acceso 23/01/17
- Estándar IEEE 802.11™-2007. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Secciones 11.1.3 (Scanning), 5.4.2.2 (Asociación y reasociación), 7.2.3 (Formato de mensajes de control). Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP4410n. Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP2000. Moodle de la asignatura.
- Analizador de red WireShark. http://www.wireshark.org. Último acceso 23/01/17
- Aplicación AirCrack-ng. http://www.aircrack-ng.org. Último acceso 23/01/17
- Guia para novatos de Aircrack-ng en Linux. http://www.aircrack-ng.org/doku.php?id=es:newbie_guide. Último acceso 23/01/17

Montaje a realizar

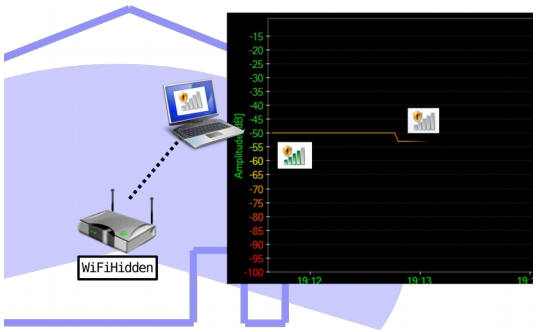
- Configurar un punto de acceso WiFi con SSID visible.
- Comprobar con un analizador de tráfico (como *WireShark*) la transmisión del SSID en las tramas *beacon*.



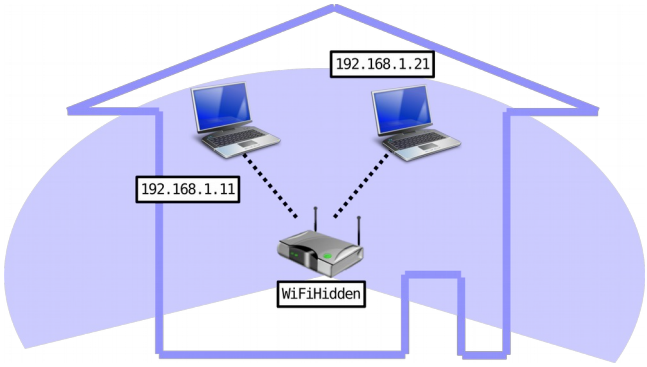
- Configurar un punto de acceso WiFi con SSID oculto.
- Comprobar con el analizador de tráfico la ausencia del SSID en las tramas *beacon*.



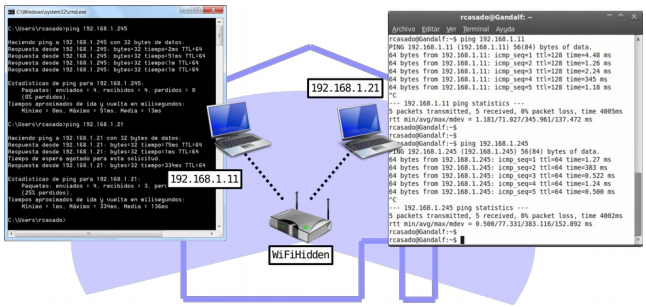
- Comprobar con inSSIDer, linSSIDer, o similar, que el punto de acceso oculto no es detectado por estaciones bajo cobertura.



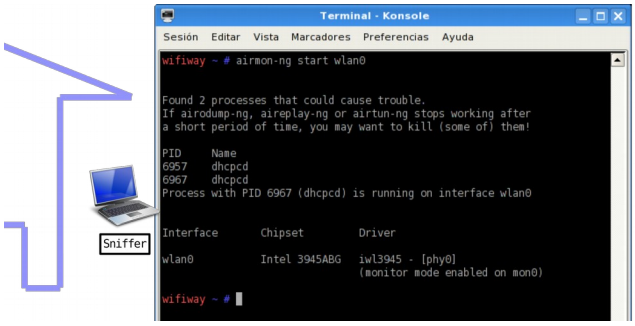
- Conectar al AP oculto una estación Windows y otra Linux.



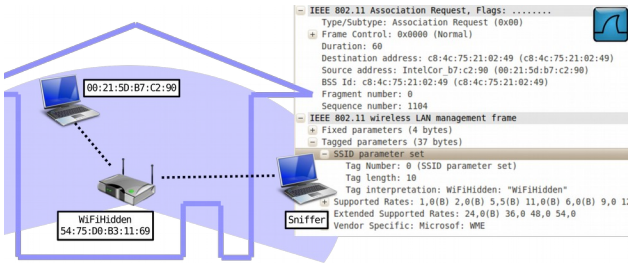
- Probar la conectividad entre las estaciones anteriores.



- Configurar en modo promiscuo una tercera estación (no conectada al AP).



- Utilizar un analizador de red que monitorice la conexión de una estación al AP oculto.
- Inspeccionar las tramas *beacon*, *probe y association* transmitidas y extraer el SSID de las mismas.



PARTE 2: ACCESO RESTRINGIDO MEDIANTE FILTRO MAC

Pasos previos

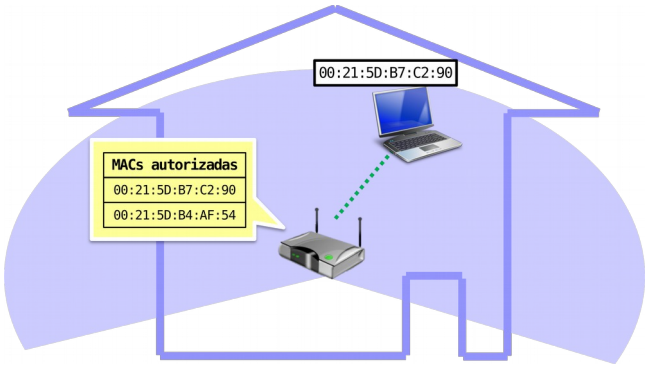
- Describir en que consiste el acceso restringido a WiFi mediante filtro de direcciones MAC.
- Averiguar cómo activar el filtro MAC en el punto de acceso y dar de alta a las estaciones autorizadas.
- Averiguar cómo consultar la dirección MAC en una estación Windows y Linux.
- Averiguar cómo captar la dirección MAC de una estación asociada a un AP, mediante aircrak-ng.
- Averiguar cómo cambiar la dirección MAC de una estación Linux.

Bibliografía

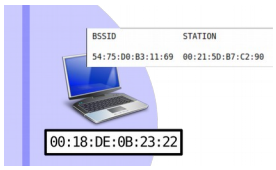
- Technet & Security, Up to secure. D-Link: Redes WiFi. Problemas y Soluciones. http://www.slideshare.net/chemai64/dlink-seguridad-wifi. Último acceso 23/01/17
- Manual del punto de acceso Cisco WAP4410n. Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP2000. Moodle de la asignatura.
- Analizador de red WireShark. http://www.wireshark.org. Último acceso 23/01/17
- Aplicación AirCrack-ng. http://www.aircrack-ng.org. Último acceso 23/01/17
- Guia para novatos de Aircrack-ng en Linux. http://www.aircrack-ng.org/doku.php?id=es:newbie_guide. Último acceso 23/01/17

Montaje a realizar

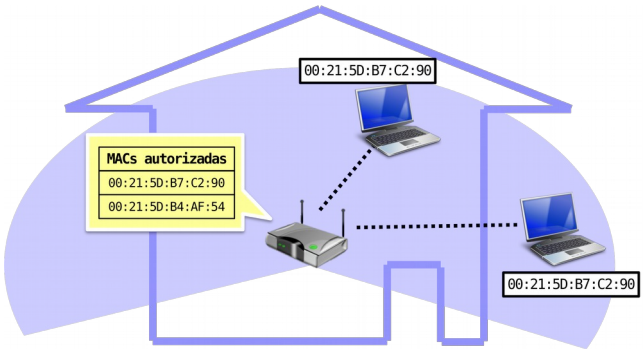
- Configurar un punto de acceso WiFi con filtro MAC. Conectar una estación (previamente autorizada) al mismo.



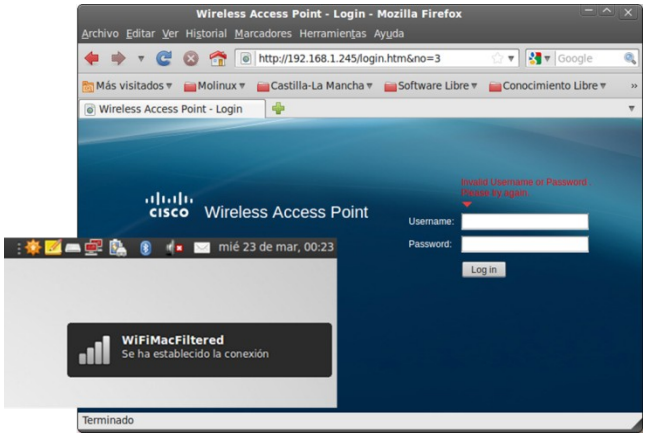
- Captar, desde una estación no autorizada, la dirección MAC de la estación autorizada.



- Suplantar la dirección MAC autorizada y conectar al AP.



- Probar que la conectividad es efectiva.



PARTE 3: SEGURIDAD MEDIANTE ENCRIPTACIÓN WEP

Pasos previos

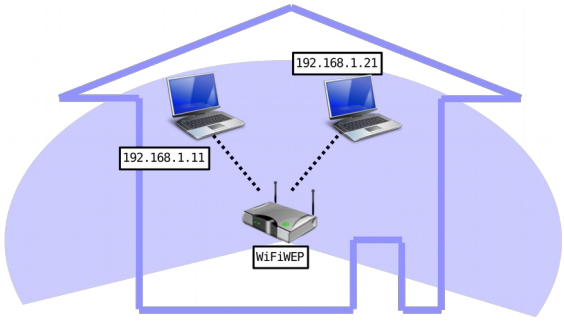
- Conocer los objetivos que se pretende alcanzar con la privacidad WEP.
- Describir en qué consiste la encriptación WEP.
- Presentar los diferentes tipos de autenticación de estaciones implementados en WEP.
- Describir como implementa el estándar IEEE 802,11 la encriptación WEP, y cual es el formato de las tramas de autenticación WEP.
- Averiguar cómo configurar WEP en un punto de acceso WiFi.
- Averiguar cómo conectar una estación Windows, Linux, Android o iOS a un punto de acceso con seguridad WEP.
- Conocer mecanismos de ataque para descubrir claves WEP utilizadas en redes inalámbricas.

Bibliografía

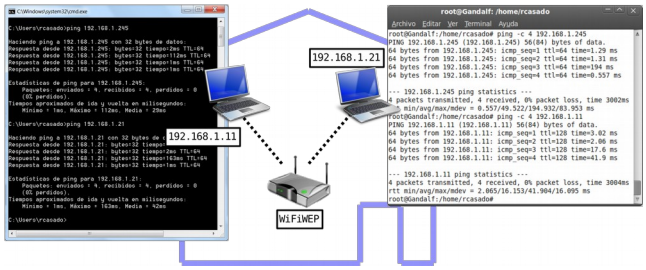
- Technet & Security, Up to secure. D-Link: Redes WiFi. Problemas y Soluciones. http://www.slideshare.net/chemai64/dlink-seguridad-wifi. Último acceso 23/01/17
- Javier Emilio Sierra, Leonardo Betancur Agudelo, Marcela Maya Gómez. "Protocolo de Seguridad WEP". http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml.Último acceso 23/01/17 También en el Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP4410n. Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP2000. Moodle de la asignatura.
- Analizador de red WireShark. http://www.wireshark.org. Último acceso 23/01/17
- Tutorial AirCrack-ng (Spanish). http://www.aircrack-ng.org/doku.php?id=tutorial#spanish. Último acceso 23/01/17

Montajes a realizar

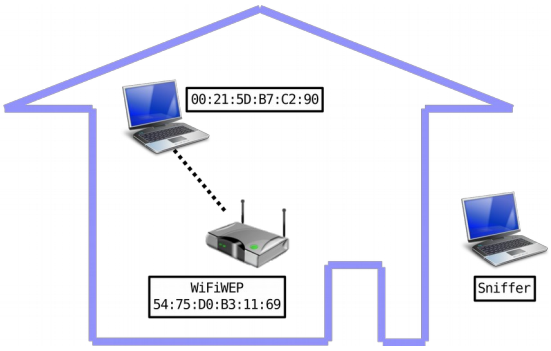
- Configurar un punto de acceso WiFi con WEP configurado con autenticación de sistema abierto y encriptación de 64 bits. Conectar al mismo una estación Windows y otra Linux.



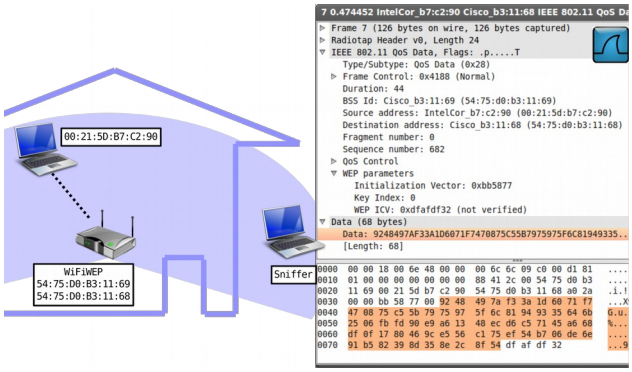
- Probar que la conectividad es efectiva.



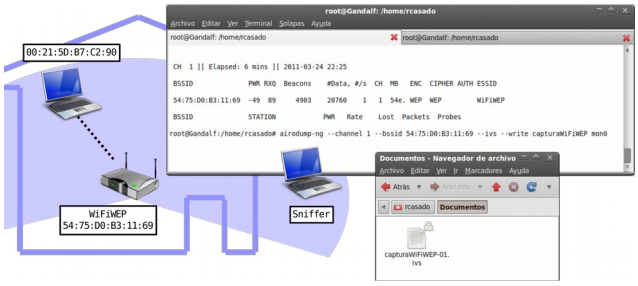
- Escuchar el tráfico desde una tercera estación.



- Monitorizar el tráfico de la red con la herramienta *WireShark*. Identificar los paquetes que contienen un campo vector de inicialización (IV).



- Capturar el tráfico de la red con la herramienta *airodump-ng*, almacenando los IVs.



- Extraer la clave WEP con la herramienta *aircrack-ng*.


```
root@Gandalf: /home/rcasado/Documentos
Archivo  Editar  Ver  Terminal  Ayuda
root@Gandalf:/home/rcasado/Documentos# aircrack-ng capturaWiFiWEP-01

Opening capturaWiFiWEP-01.ivs
Read 20761 packets.

   #  BSSID              ESSID                     Encryption

   1  54:75:D0:B3:11:69  WiFiWEP                   WEP (20760 IVs)

Choosing first network as target.

Opening capturaWiFiWEP-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 20760 ivs.

                              Aircrack-ng 1.0

            [00:00:00] Tested 18 keys (got 20760 IVs)

   KB    depth   byte(vote)
    0    0/  2   B7(26228) 34(25460) 78(25228) 97(25104)
    1    1/  3   5E(25832) C1(25684) B9(25424) 73(25352)
    2    0/  1   C5(28876) 6E(26928) 1B(26604) C5(26560)
    3    0/  4   EC(25676) 87(24812) A7(24804) 57(24736)
    4    0/  1   26(30728) AD(26588) CA(25416) DD(25356)

                         KEY FOUND! [ B7:0A:C5:EC:26 ]
      Decrypted correctly: 100%
```

ENTREGABLE

Fruto de esta actividad no se realizará ningún entregable, sino que cada vez que se obtenga una configuración se le deberá de enseñar al profesor, para que este compruebe su funcionamiento.