

## DISPOSITIVOS Y REDES INALÁMBRICOS

*Protección de las comunicaciones en WiFi mediante WPA-Personal y WPA2-Empresarial*

### OBJETIVO DE LA ACTIVIDAD

Los alumnos:

- comprenderán el funcionamiento del mecanismo WPA-Personal, y aprenderán a configurar una BSS con este sistema de encriptación; posteriormente, comprobarán como un agresor puede vulnerar esta medida de seguridad mediante un ataque por diccionario.
- comprenderán el funcionamiento del mecanismo WPA2-Personal; posteriormente, configurarán una BSS con este sistema de seguridad.
- comprenderán el funcionamiento del mecanismo WPA-Empresarial. Posteriormente aprenderán a configurar una BSS con este sistema de encriptación junto con un servidor RADIUS de autenticación de usuarios.

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: WPA PERSONAL

#### Pasos previos

- Identificar los diferentes mecanismos que implementan la integridad, seguridad y autenticación en WPA-Personal.
- Conocer el proceso de encriptación TKIP:
  - Parámetros que intervienen
  - Algoritmos implicados
  - Encapsulación requerida
- Conocer el proceso de autenticación usado por WPA basado en 4-way handshake.

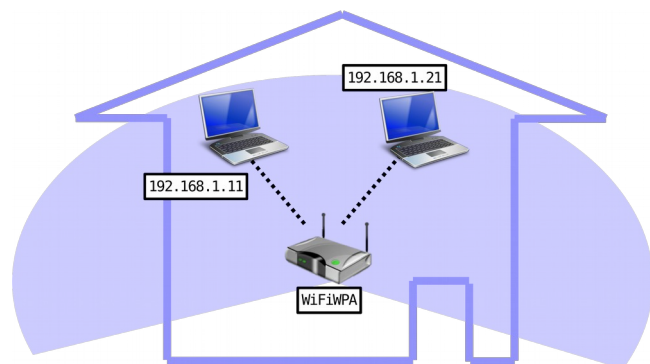
- Averiguar cómo configurar WPA-Personal en un punto de acceso WiFi.
- Averiguar cómo conectar una estación Windows, Linux, Android o iOS a un punto de acceso con seguridad WPA-Personal.

## Bibliografía

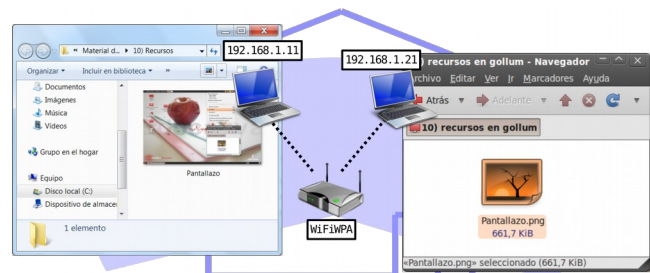
- Guillaume Lehenbre. "Wi-Fi security - WEP, WPA and WPA2". [http://tele1.dee.fct.unl.pt/rit2\\_2015\\_2016/files/hakin9\\_wifi\\_EN.pdf](http://tele1.dee.fct.unl.pt/rit2_2015_2016/files/hakin9_wifi_EN.pdf). Último acceso 24/01/17
- IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks—Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements. 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.
- Aplicación Aircrack-ng (Tutoriales). <http://www.aircrack-ng.org/doku.php?id=tutorial#spanish>. Último acceso 23/01/17
- Como crackear WPA/WPA2. [http://www.aircrack-ng.org/doku.php?id=es:cracking\\_wpa](http://www.aircrack-ng.org/doku.php?id=es:cracking_wpa). Último acceso 23/01/17

## Montajes a realizar

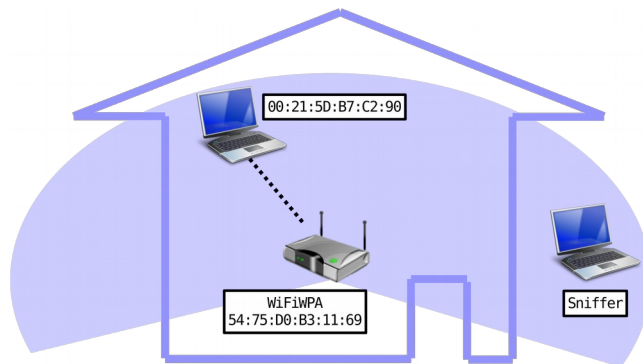
- Configurar un punto de acceso WiFi con WPA-Personal. Conectar al mismo una estación Windows y otra Linux.



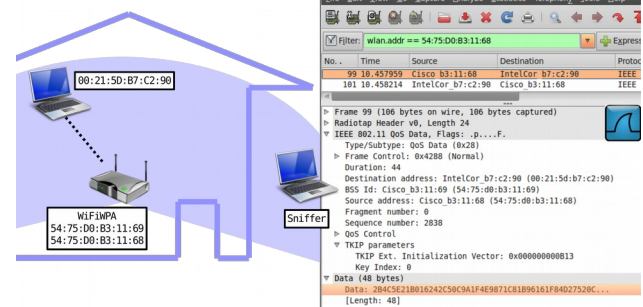
- Probar que la conectividad es efectiva.



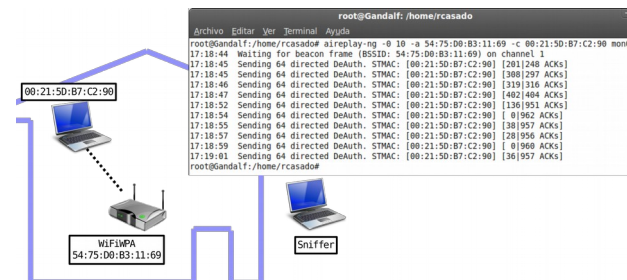
- Escuchar el tráfico desde una tercera estación ajena a la BSS.



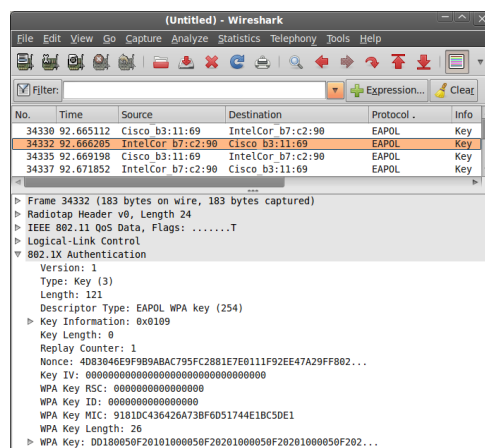
- Monitorizar el tráfico de la red con la herramienta *Wireshark*. Observar los paquetes encriptados.



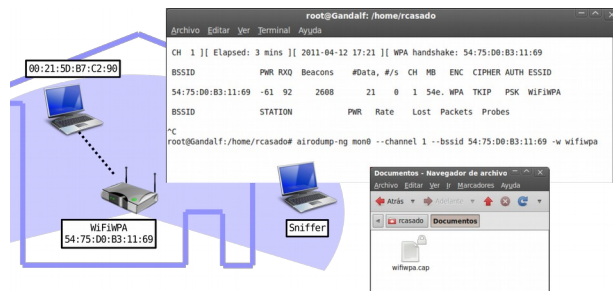
- Desautenticar al cliente mediante la herramienta *aireplay-ng*, con el fin de que vuelva a autenticarse.



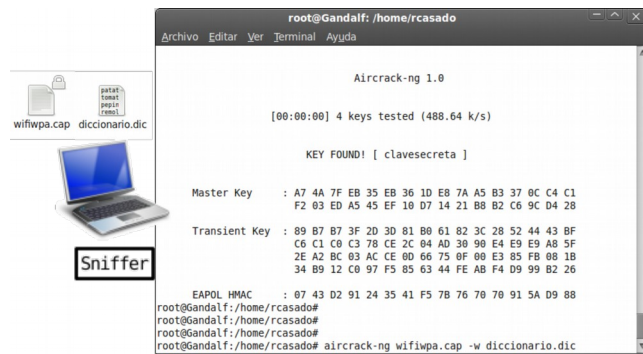
- Capturar, con *Wireshark*, el handshake realizado durante la autenticación.
- Comprobar que se ajusta a lo descrito anteriormente.



- Capturar, con la herramienta *airodump-ng*, el handshake realizado durante la autenticación.
- Almacenar los paquetes implicados.



- Usar un pequeño diccionario de claves, la clave de nuestra WiFi WPA debe estar incluida, para extraer la clave WPA con la herramienta *aircrack-ng*.



## PARTE 2: WPA2 PERSONAL

### Pasos previos

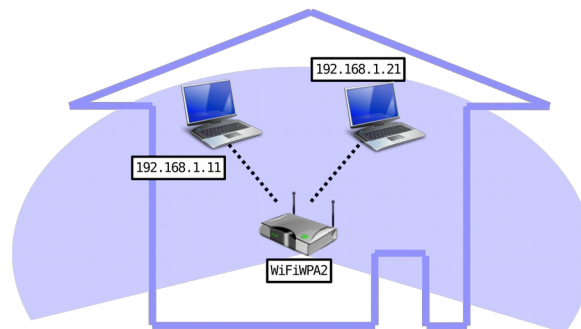
- Identificar las diferencias existentes entre WPA-Personal y WPA2-Personal en lo que respecta a los mecanismos que implementan la integridad, seguridad y autenticación.
- Conocer el proceso de encriptación CCMP-AES:
  - Parámetros que intervienen
  - Algoritmos implicados
  - Encapsulación requerida
- Averiguar cómo configurar WPA2-Personal en un punto de acceso WiFi.
- Averiguar cómo conectar una estación Windows a un punto de acceso con seguridad WPA2-Personal.
- Averiguar cómo conectar una estación Linux a un punto de acceso con seguridad WPA2-Personal.

### Bibliografía

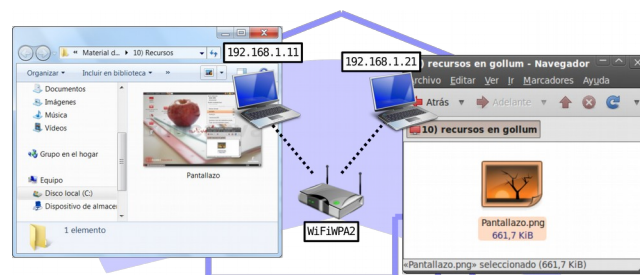
- Guillaume Lehenbre. "Wi-Fi security - WEP, WPA and WPA2". [http://tele1.dee.fct.unl.pt/rit2\\_2015\\_2016/files/hakin9\\_wifi\\_EN.pdf](http://tele1.dee.fct.unl.pt/rit2_2015_2016/files/hakin9_wifi_EN.pdf). Último acceso 24/01/17
- Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197. November 26, 2001. Moodle de la asignatura.
- The Rijndael Animation (animación Flash que explica el funcionamiento de AES). [http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael\\_Animation\\_v4\\_esp.zip](http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_esp.zip). Último acceso 24/01/17. También en Moodle de la asignatura.
- IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks—Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements. 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.
- Aplicación Aircrack-ng (Tutoriales). <http://www.aircrack-ng.org/doku.php?id=tutorial#spanish>. Último acceso 23/01/17
- Como crackear WPA/WPA2. [http://www.aircrack-ng.org/doku.php?id=es:cracking\\_wpa](http://www.aircrack-ng.org/doku.php?id=es:cracking_wpa). Último acceso 23/01/17

## Montajes a realizar

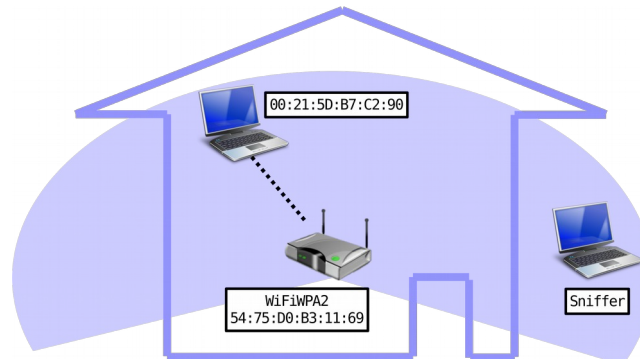
- Configurar un punto de acceso WiFi con WPA2-Personal. Conectar al mismo una estación Windows y otra Linux.



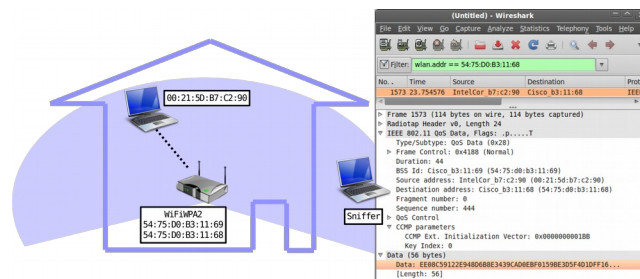
- Probar que la conectividad es efectiva.



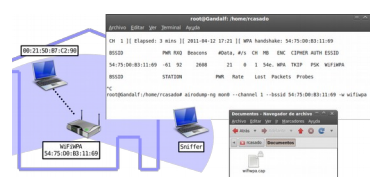
- Escuchar el tráfico desde una tercera estación.

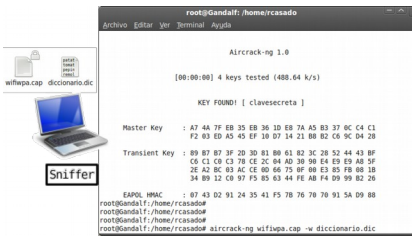


- Monitorizar el tráfico de la red con la herramienta Wireshark. Observar los paquetes encriptados.



- Intentar obtener la clave WPA2 de manera similar al caso anterior.





```
root@Gandalf: /home/rcasado
Aircrack-ng 1.0

[00:00:00] 4 keys tested (488.64 k/s)

KEY FOUND! [ clavescreta ]

Master Key   : A7 4A 7F E8 35 E8 36 1D E8 7A A5 B3 37 0C C4 C1
              F2 03 E9 A5 A5 EF 18 D7 14 21 B0 02 C6 9C D4 26

Transient Key : 89 87 87 3F 20 20 31 B8 61 82 3C 28 52 44 43 8F
              C6 C1 C9 C3 78 CE 2C 04 AD 38 98 E4 E9 E9 A8 5F
              2E A2 0C 03 AC CE 00 00 75 8F 08 E3 85 F8 08 18
              34 89 12 C8 97 F5 85 63 44 FE A8 F4 09 99 82 26

EAPOL HMAC   : 07 43 02 91 24 35 41 F5 78 78 78 91 5A 09 88

root@Gandalf: /home/rcasado#
root@Gandalf: /home/rcasado#
root@Gandalf: /home/rcasado#
root@Gandalf: /home/rcasado# aircrack-ng wifupa.cap -w diccionario.dic
```

## PARTE 3: WPA2-EMPRESARIAL

### Pasos previos

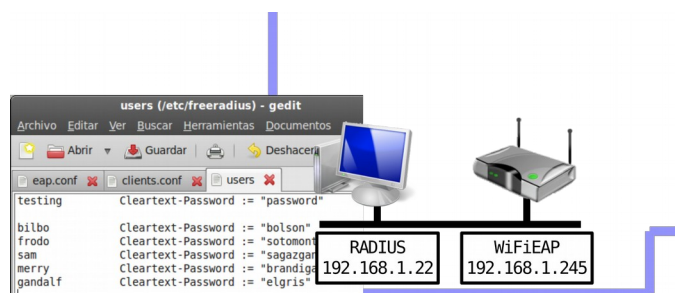
- Identificar las diferencias que incorpora WPA-Empresarial frente a WPA-Personal, en lo que respecta a la autenticación de usuarios.
  - Conocer el protocolo EAP, incluyendo los tipos de autenticación MD5, TLS, TTLS, LEAP y PEAP.
  - Conocer los métodos de autenticación MS-CHAP y MS-CHAPv2.
- Averiguar cómo instalar y configurar un servidor RADIUS. Elegir plataforma (Linux/Windows) y servidor (FreeRADIUS, IAS,...).
- Averiguar cómo configurar WPA-Empresarial en un punto de acceso WiFi.
- Averiguar cómo conectar una estación Windows, Linux, Android e iOS a un punto de acceso con seguridad WPA-Empresarial.

### Bibliografía.

- Understanding the updated WPA and WPA2 standards. <http://www.zdnet.com/article/understanding-the-updated-wpa-and-wpa2-standards/>. Último acceso 24/01/17
- Extensible Authentication Protocol (EAP). [https://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol). Último acceso 24/01/17
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). <http://www.thenetworkencyclopedia.com/entry/microsoft-challenge-handshake-authentication-protocol-ms-chap/>. Último acceso 24/01/17
- MS-CHAPv2. <https://technet.microsoft.com/es-es/library/cc957983.aspx>. Último acceso 24/01/17
- Proyecto FreeRADIUS. Servidor RADIUS de código abierto. <http://www.freeradius.org>
- HOWTO: FreeRADIUS+EAP/PEAP. UbuntuForums. <http://ubuntuforums.org/showthread.php?t=478804&highlight=freeradius%2BEAP%2FPEAP>

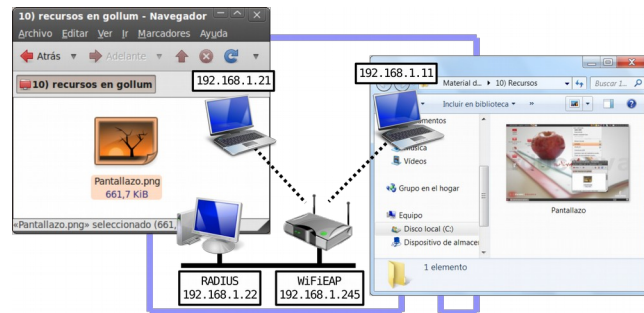
### Montajes a realizar

- Configurar un punto de acceso WiFi con WPA-Empresarial, enlazado con un servidor RADIUS de autenticación de usuarios mediante PEAP+MS-CHAPv2.





- Conectar a la BSS una estación Windows y otra Linux.
- Probar que la conectividad entre ambas es efectiva.



## 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.