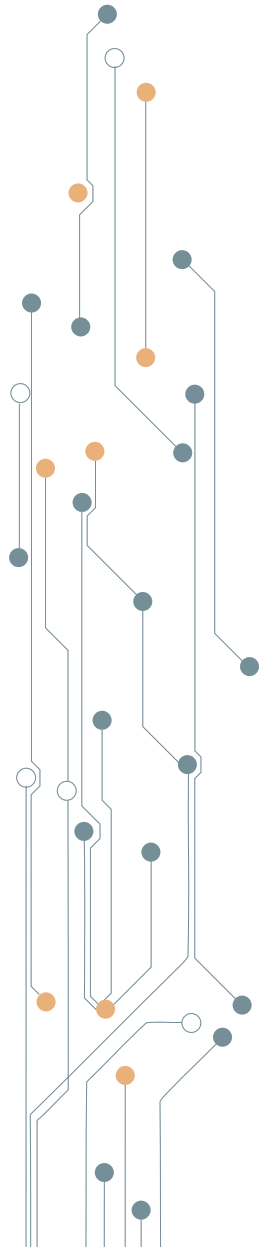
Conceptos básicos y cifrado Wireless

Telefónica EDUCACIÓN DIGITAL

Índice



1. Portales cautivos

Los portales cautivos son un método de aprobación de usuarios en nodos de redes inalámbricas. Se trata de un sistema frecuentemente utilizado para dotar de conexión a los usuarios que se encuentran en lugares públicos y grandes infraestructuras.

Podemos dividir el sistema en dos secciones diferentes: una pública, que está compuesta de nodos Wireless que puedan proporcionar una conexión, y otra privada que no permite la conexión a una red sin la previa autenticación de credenciales. Normalmente esta red privada es Internet.

En general, la base de los portales cautivos son varios puntos de acceso conectados a un Gateway que ha sido puesto previamente en la red privada, una base de datos y servidor de autenticación para poder guardar los datos de usuarios y poder validar su acceso, y un servidor web para el alojamiento del portal.

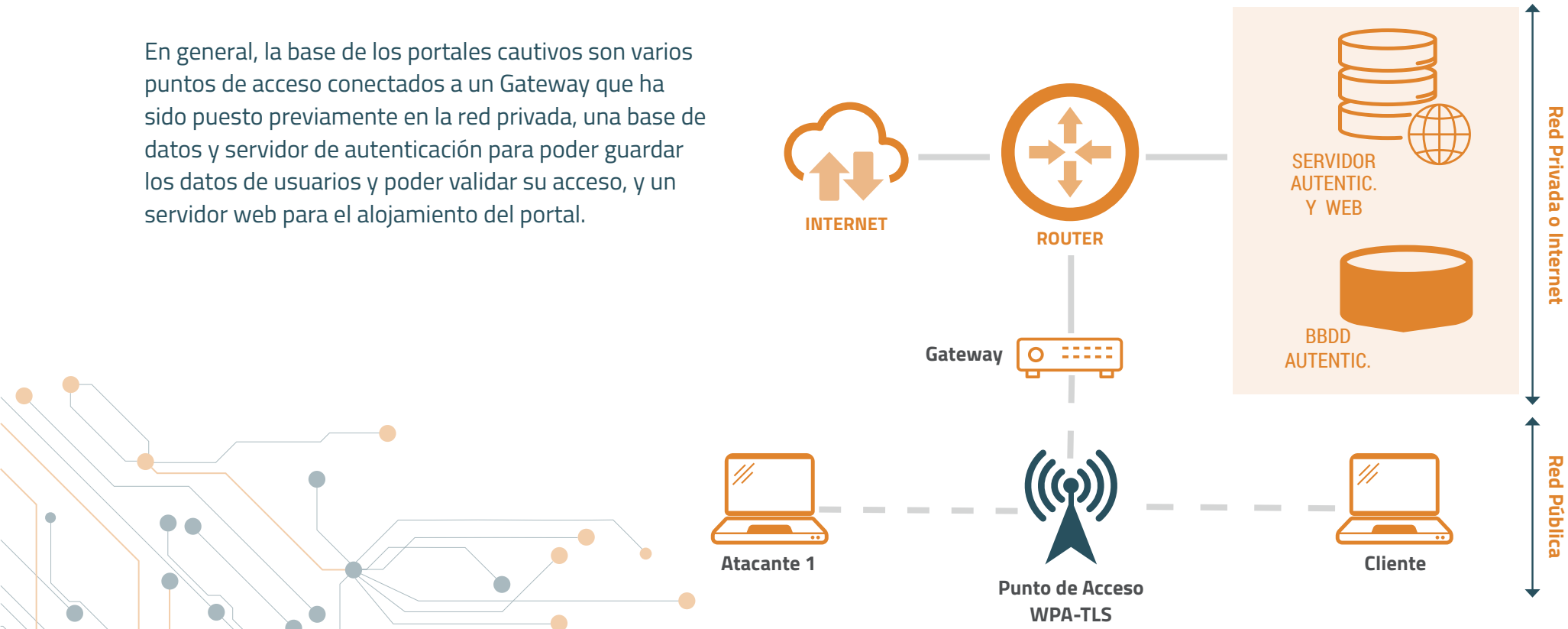


FIGURA 3. 1. PORTAL CAUTIVO

Cuando un usuario cuyas credenciales no han sido validadas quiere acceder a la red privada, el Gateway comprobará si hay una autenticación previa del usuario basándose en comprobar si tienen tokens temporales, que se gestionan por https. Si el usuario no tiene un token que se considere válido el Gateway redirige la petición al portal, que solicitará unas credenciales al usuario para poder proceder a la asignación de un token. Cuando consiga obtener un token el Gateway finalmente le concederá el derecho a acceder a la red privada.

Otro uso de los Portales Cautivos es la presentación de un sitio web antes de dar el acceso a la red privada informando simplemente de las normativas del sitio, mostrando anuncios patrocinadores, ...

Dadas las propiedades y el modo de funcionamiento de los Portales Cautivos, en los que se posibilita la asociación sin cifrar de cualquier usuario (y el tráfico que genera) con el punto de acceso, este tipo de estructuras es vulnerable a ataques en los que un intruso puede capturar el tráfico, o realizar ataques de tipo spoofing durante el tiempo de validez del token.

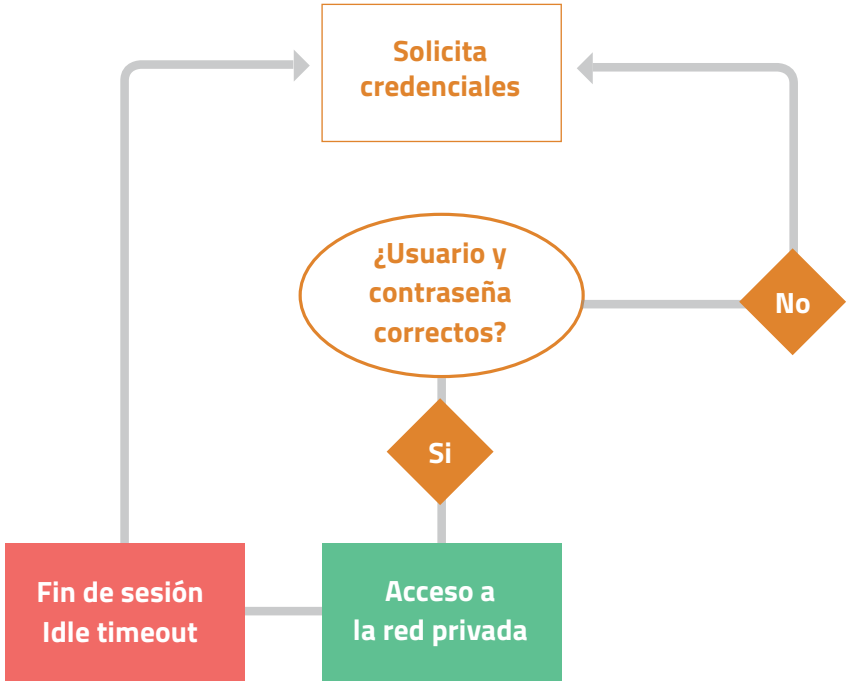


FIGURA 3. 2. ACCESO AL PORTAL CAUTIVO

1.1 | DNS Tunneling

Son muchas las ocasiones en las que el Gateway, que realizando un filtrado de los intentos de conexión y redirige dependiendo de la validez del token, admite el acceso de las solicitudes DNS a la red privada. Teniendo esto en cuenta, existe la posibilidad de que un atacante encapsule el tráfico TCP/IP en las solicitudes DNS, saltándose así los obstáculos del Portal Cautivo.

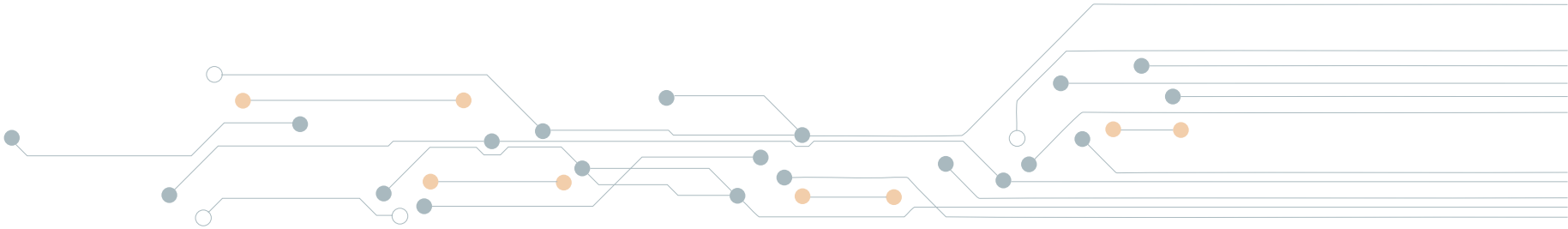
Este método tiene varios inconvenientes:

- El tráfico DNS usa UDP, que como se ha estudiado anteriormente, no es orientado a conexión, por lo que no asegura el ensamblado correcto de los paquetes.
- Las solicitudes DNS tienen una limitación máxima de 512 bytes en cada paquete (Este tamaño no es suficiente para encapsular TCP/IP).
- Sólo es posible recibir respuestas de los servidores DNS. Dichos servidores no pueden mandar paquetes sin haber recibido una solicitud previa.

Existen, sin embargo, métodos para superar las limitaciones anteriores. Es posible crear un servidor determinado con el que el atacante pueda evitar estos obstáculos y, con ayuda de una herramienta desarrollada para tal, posibilite la conexión mediante peticiones UDP por medio del puerto 53.

Otro requerimiento es el desarrollo de un protocolo específico que modifique la limitación del tamaño de los paquetes y proporcione algún sistema que no desordene los paquetes para poder re ensamblarlos. El problema es que tendríamos que utilizar el protocolo tanto en el servidor como en la aplicación.

Esta aplicación ya ha sido desarrollada, y recibe el nombre de Nstx, que utiliza el protocolo creado para tal, denominado **NSTC Protocol**.



2. Rogue AP

Rogue AP, también conocido como Fake AP, es un punto de acceso no autorizado que tiene la meta de que un determinado usuario se conecte a él para posteriormente poder capturar el tráfico.

Básicamente el funcionamiento de este tipo de ataque se basa en la colocación de un punto de acceso controlado por el atacante, de forma estratégica para que los usuarios se conecten al Rogue AP en lugar de la red de la víctima. La colocación estratégica suele traducirse en la cercanía geográfica y en emitir con mayor potencia para que la señal sea mayor que la de la víctima. Cuando finalmente el usuario se ha asociado al falso punto de acceso, el atacante tiene la posibilidad de realizar un ataque MITM, teniendo disponible todo el tráfico que circula entre el usuario y el Rogue AP.

A continuación, se muestra un esquema básico de este tipo de ataque:

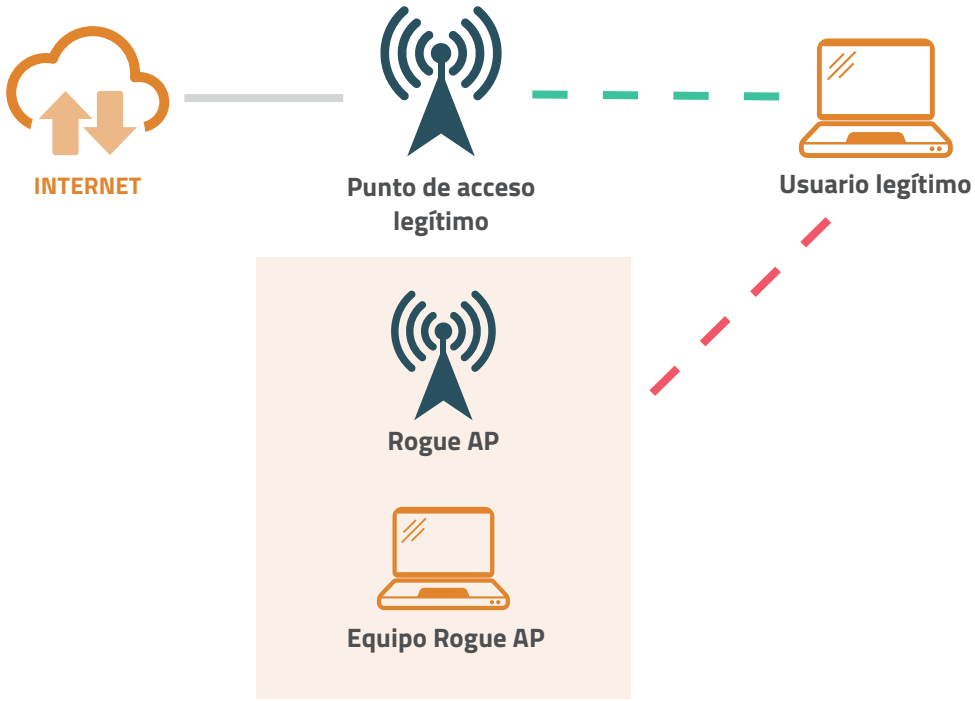


FIGURA 4. 1 ATAQUE ROGUE AP

Cuando el terminal de un usuario conectado a una red corporativa o Internet de forma inalámbrica se encuentra con un AP, supuestamente de la misma red, pero con una señal, cambia automáticamente de AP y se conecta al que ofrece mejor calidad de conexión. Si este AP resulta estar bajo el control de un usuario ilegítimo los datos confidenciales del usuario quedan comprometidos.

Realmente la simulación del Rogue AP es bastante sencilla, ya que puede implementarse instalando un determinado software en un ordenador portátil. Dicho software simularía los distintos servidores HTTP, DNS y DHCP así como un Portal Cautivo correctamente configurado para el desvío del tráfico. Además, existe una herramienta que puede hacer todo eso de forma mucho más sencilla: **Airsnarf**.

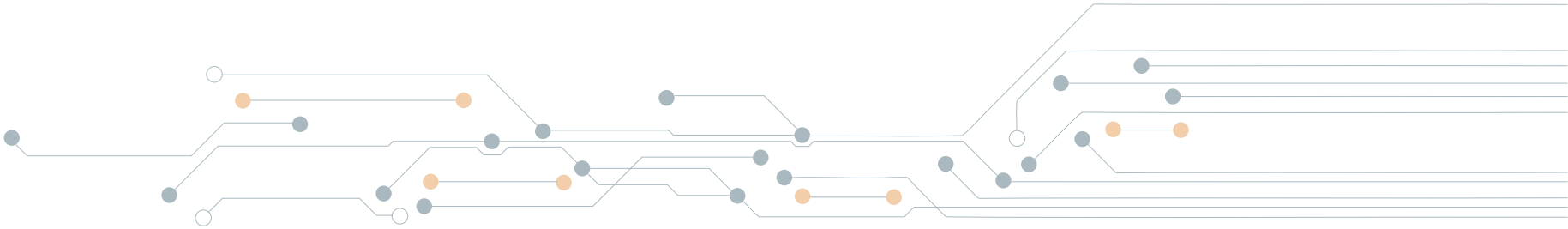
Además de esto, necesitamos una tarjeta Wireless compatible con HostAP, un software especial que posibilita poner la tarjeta en modo master, algo que necesitamos si queremos que el dispositivo que estamos utilizando simule comportarse como un Punto de Acceso. Por otra parte, si estamos utilizando el sistema operativo Windows necesitaremos que la tarjeta tenga compatibilidad con SoftAP.

El modo de funcionamiento de Airsnarf radica en la disposición del Rogue AP, para luego arrancar el servidor http y realizar la configuración del DHCP. El software solicitará diferentes datos del punto de acceso víctima, tales como la IP y el DNS para que la red que pretendemos simular sea similar a la víctima. De forma automática se realizará la configuración DNS, gracias a la que todas las peticiones hacia el punto de acceso original, podrán ser redirigidas hacia el Rogue AP.

Cuando un usuario que quiere conectarse a la red original introduce sus credenciales en el Rogue AP el atacante ya dispondrá de ellas.

Generalmente se cambia el aspecto del portal cautivo para que el usuario no se dé cuenta de que ha accedido a un sitio diferente.

Además de robar información y monitorizar el tráfico, el atacante también podrá redirigir algunas peticiones de la víctima, enviando dichas peticiones a sitios diferentes al que el atacante quiere que la víctima acceda.



3. Recomendaciones de seguridad

Para evitar incidentes relacionados con la seguridad de nuestra red inalámbrica, en este caso, nuestra red WiFi, debemos tener en cuenta algunas consideraciones:

- En primer lugar, es recomendable cambiar el nombre que nuestra compañía de Internet ha generado para nuestra red(SSID). Este nombre viene por defecto en el router y también debemos cambiar la contraseña de administración del mismo.

- En segundo lugar, es importante que modifiquemos la clave por defecto del router para hacer nuestra red más segura. Existen muchas aplicaciones que podemos descargar incluso gratuitamente que pueden proporcionar la clave por defecto de muchas redes, incluso con WPA o WPA2. Algunas de estas aplicaciones, incluso dan la posibilidad de hacer ataques Dos.

- Una buena opción es controlar el número de dispositivos que se conectan a nuestra red, y para ello tenemos limitar el número de IP's asignables de nuestro router. Generalmente, el router viene configurado de forma que las IP's a los clientes sean asignadas dinámicamente (DHC).

- Por otra parte, es muy recomendable actualizar los controladores WiFi, el firmware del router y nuestro sistema operativo.

- Además, deberíamos deshabilitar la interfaz WiFi cuando no estemos haciendo uso de ella, así como desactivar las tecnologías que no estemos usando del router. Un posible ejemplo de esto es WPS.

En cuanto al cifrado, en este curso hemos aprendido que existen diversas técnicas de cifrado (WPA, WEP, WPA2). La más recomendada es WPA2 y dentro de esta opción, debemos tener en cuenta dos casos diferenciados:

- **WPA2 Personal o PSK con cifrado AES (Advanced Encryption Standard).** La opción más utilizada en espacios pequeños privados, ya sean casas familiares o locales destinados a empresas pequeñas. La contraseña debe ser robusta y contar con más de 20 caracteres.
- **WPA2 – Enterprise.** La opción recomendada para medianas y grandes empresas, ya que, además de cifrar con AES (Advanced Encryption Estándar), genera contraseñas robustas mediante RADIUS (Remote Authentication Dial In User Service), los protocolos 802.1S y EAP (Extensible Authentication Protocol). El protocolo utilizado dependerá de la infraestructura, será necesario estudiar las condiciones de cada escenario.

En cuanto a la seguridad de redes ajenas a la nuestra, resumiremos los consejos y recomendaciones en dos aspectos clave:

- **No utilizar redes privadas ajenas a la nuestra.** Además de que es una práctica ilegal, no conocemos quién puede estar detrás de esa red y qué puede estar averiguando sobre nosotros. Además, debemos desconfiar. Si el cifrado es WEB, posiblemente sea una "trampa" y aunque inicialmente podamos pensar que somos los intrusos de la red, es probable que acabemos siendo los "atacados".

- **No utilizar redes públicas.** Existen numerosos establecimientos e instituciones que proporcionan de forma gratuita (o de pago) acceso a internet mediante una red pública.

  Este tipo de redes son muy sensibles y perfectas para los atacantes ya que normalmente van a utilizar una seguridad muy limitada, o incluso van a carecer de ella.
  Cualquier persona puede hacer sniffing, hacer ataques de ARP Poison o cualquier otro tipo de ataque de forma sencilla.
  El acceso a una VPN (Virtual Private Network) a través de una red de este tipo tampoco es seguro, ya que el único tráfico protegido en las redes privadas virtuales es el correspondiente al de la capa 3 (IPSec) o nivel 5 (SSL).
  Numerosos ataques, como ataques de caché de ARP están a nivel 2, y, por tanto, no quedan protegidos con la VPN.

Telefónica EDUCACIÓN DIGITAL