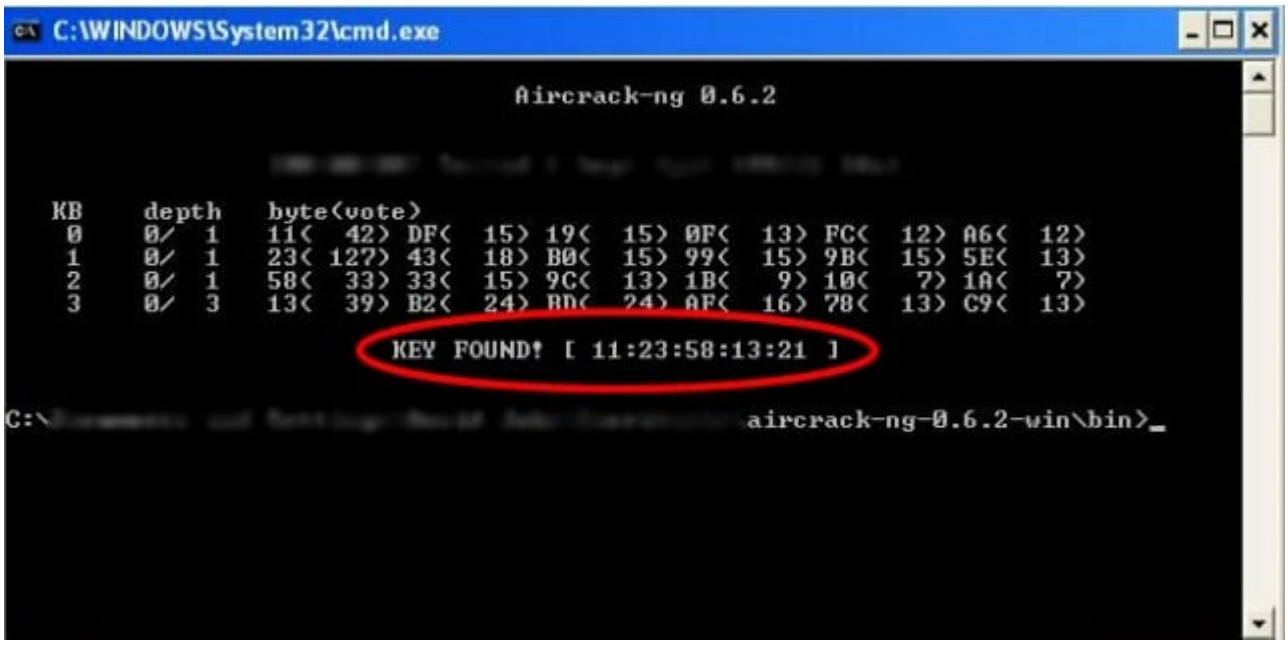
La Seguridad De Una Red Inalambrica

Como Un Atacante Podría Romper La Seguridad De Una Red Inalambrica

No es raro que a cualquier informatic@ se le haya preguntado al menos una vez si sabe como **sacar la clave de la red Wi-Fi**. Esta es una de las preguntas que se hacen, justo después de preguntar si se sabe como obtener las contraseñas de Facebook :S La seguridad de tu red inalámbrica es algo bastante importante, ya que cualquier persona podría tener acceso a tus datos, y mas aun, si eres un medio para llegar a algo mas importante como por ejemplo la empresa en la que trabajas. En el presente articulo no pretendemos dar una guía de como «**hackear la Wi-Fi de tu vecino**«, ó como «**robar contraseñas**» de redes inalámbricas. La finalidad es hacerte saber como es que un atacante podría comprometer la información que manejas.

Disclaimer

En el presente articulo mostraremos diferentes técnicas que usan los atacantes para vulnerar cualquier red Wi-Fi. El leer este articulo no te convertirá en un hacker de la noche a la mañana. **No nos hacemos responsables** por las contraseñas que de ahora en adelante los lectores puedan descifrar :D

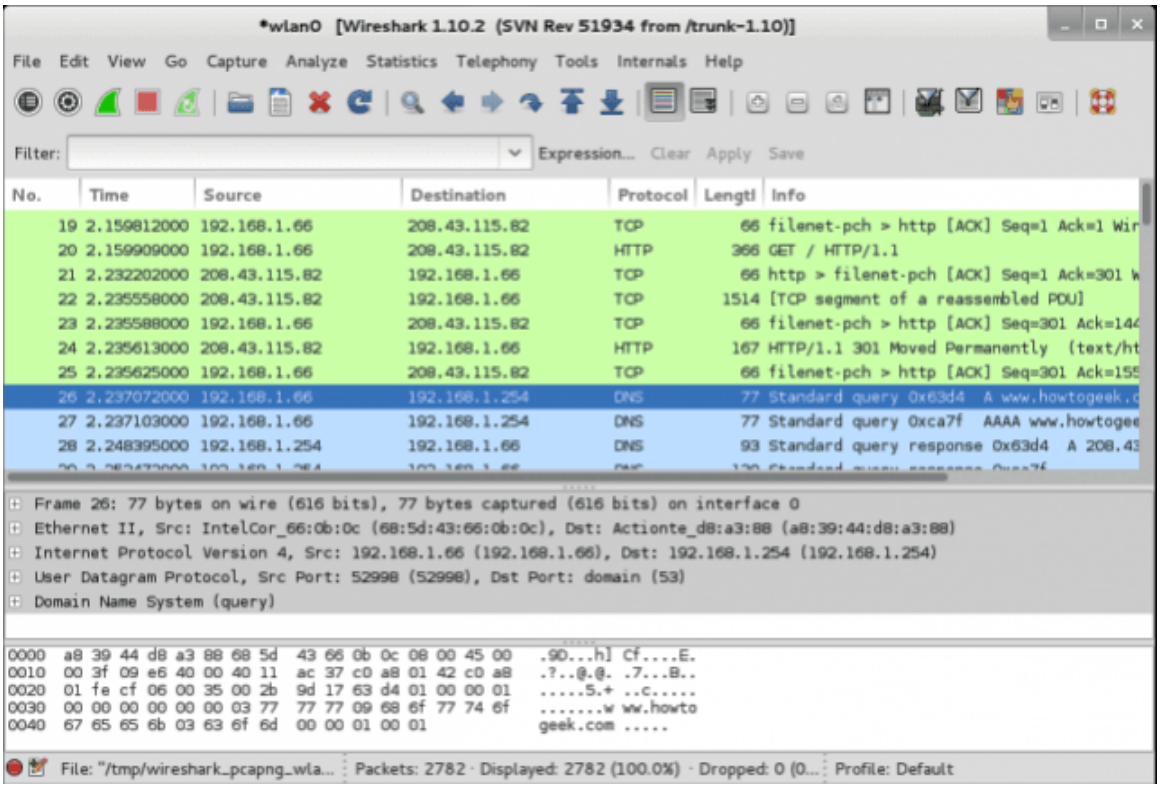


¿Como Se Espía Una Red Sin Protección?

En primer lugar, vamos a empezar con **la red menos segura posible**: Una red abierta sin contraseña. Cualquiera puede conectar obviamente a la red y utilizar su conexión a Internet sin proporcionar una contraseña. Cuando una red no esta protegida con una contraseña, todo su trafico será enviado de forma plana, y eso será lo suficiente como para que el atacante sea capaz de sniffear todos los datos que interactuan con esta red. Solo las conexiones HTTPS, como las que usan los certificados SSL, serán las únicas conexiones que protegerán los datos del usuario.

Una de las herramientas conocidas para realizar el rastreo de

datos es WireShark. ¿Sigues usando una red abierta?



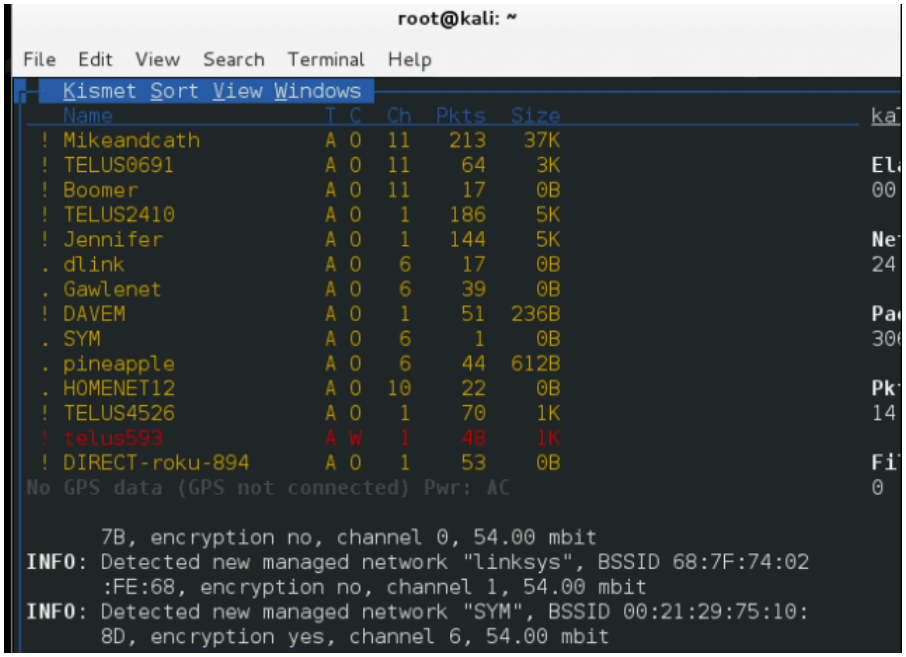
Encontrando Una Red Wi-Fi Oculta

Ocultar una red no es un método eficiente para protegerla. Es posible encontrar redes inalámbricas «ocultas» con herramientas como Kismet, que muestran las redes inalámbricas cercanas. El SSID del red inalámbrica, o un nombre, se mostrarán en blanco en muchas de estas herramientas.

Esto no ayudará demasiado. Los atacantes pueden **enviar una**

trama deauth a un dispositivo, la cual es la señal de un punto de acceso **enviaría si estuviera cerrando**. El **dispositivo** intentará conectarse a la red de nuevo, y **lo hará utilizando el SSID de la red**. El SSID **puede ser capturado en este momento**. Asi es, aunque ocultes tu red, el dispositivo que use esta red terminaria revelando el SSID que has ocultado.

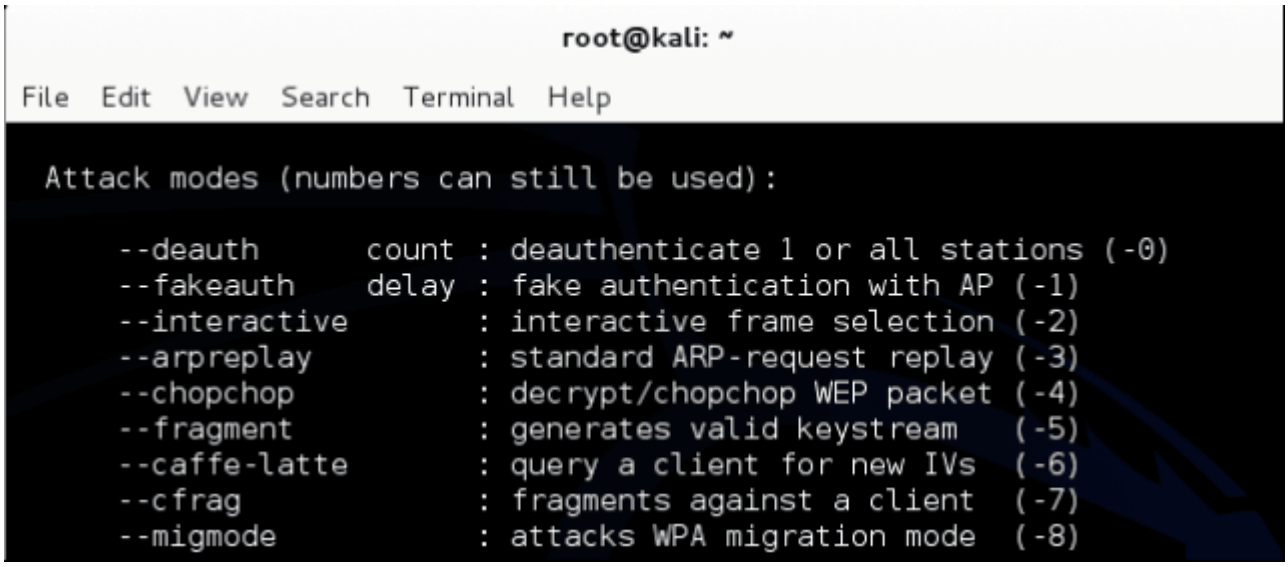
De hecho, un atacante cercano podría ver estas peticiones y pretender ser el punto de acceso oculto, obligando a su dispositivo conectarse a un punto de acceso comprometido.



Cambio De Una

Dirección MAC

Las herramientas de análisis de red, también mostrara el tráfico los dispositivos conectados a un punto de acceso junto con su **dirección MAC**, algo que es visible en los paquetes que viajan de ida y vuelta. Si un dispositivo está conectado al punto de acceso, y el atacante conoce la dirección MAC del dispositivo, créeme que este suplantara la «identidad» de tu dispositivo. Los atacantes esperarían a que el usuario desconecte o lo obligarían a hacerlo, luego, se conectarian a la red Wi-Fi con su propio dispositivo.



Obteniendo

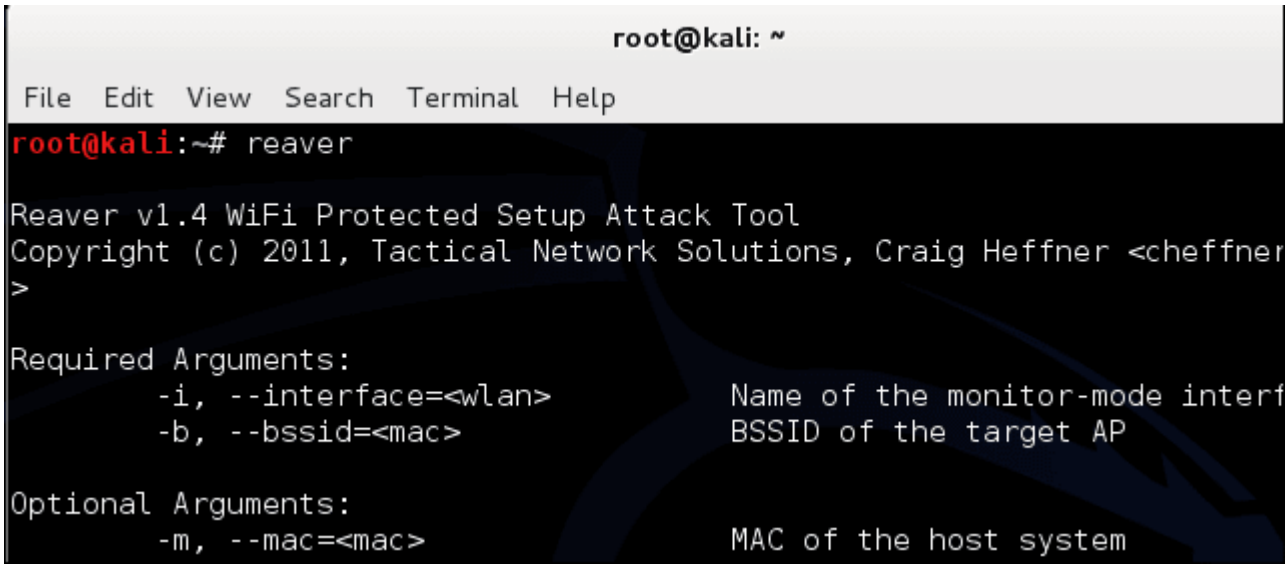
Claves Con Encriptacion WEP ó WPA1

Existen ataques conocidos que pueden romper el **cifrado WEP ó WPA1** (WPA1 se refiere a menudo simplemente como encriptación «WPA», pero que utilizan WPA1 aquí hacer hincapié en que estamos hablando de la versión anterior de WPA y WPA2 que es más seguro).

El propio sistema de cifrado es vulnerable y, con bastante tráfico capturado, el cifrado puede ser analizado y roto. Después de monitorear un punto de acceso durante aproximadamente un día y capturar sobre todo un día de tráfico, un atacante puede ejecutar un programa de software que rompe el cifrado WPA1, en el caso del cifrado WEP, es menor el tiempo de vulnerabilidad. El cifrado WEP es bastante inseguro y hay otras maneras de romper más rápidamente engañando al punto de acceso. WPA1 es más seguro, pero **sigue siendo vulnerable**.

La Explotación De Vulnerabilidades WPS

Un atacante también podría entrar en la red mediante la explotación del Wi-Fi Protected Setup o WPS. Con WPS, **el router tiene un número PIN** de 8 dígitos que un dispositivo puede utilizar para conectar en lugar de proporcionar la contraseña codificada. El PIN se comprueba en dos grupos, en primer lugar, el router comprueba los cuatro primeros dígitos, y le dice al dispositivo si es correcto, y luego el router comprueba los últimos cuatro dígitos y le dice al dispositivo si es correcto. Hay un número bastante reducido de posibles números de cuatro dígitos, por lo que un atacante puede usar «fuerza bruta» para vulnerar la seguridad WPS, tratando cada número de cuatro dígitos hasta que el router les dice que ha adivinado la correcta.



Fuerza Bruta En Contraseña De WPA2

Este tipo de ataque, lo que hace es usar un diccionario, en el cual se tendrán palabras que se han agregado, para luego automáticamente revisar una por una al intentar conectar con un **encriptado WPA2**. La mayoría de usuarios no hacen una **gestión segura de la configuración de su red Wi-Fi**, por lo que tendrán contraseñas simples y fáciles de descifrar. Supongamos, un usuario podría usar «**password**«; aunque este en ingles, la palabra es insegura. Para evitar esto, el usuario debe usar una combinación de letras minúsculas y mayúsculas en su contraseña, junto con una combinación de números y uno que otro símbolo.

Conoces algun otro metodo con el cual se pueda realizar un

ataque exitoso a una red Wi-Fi. Animate y compártela en un comentario, seria de gran ayuda que también compartieras como poder evitar el ataque ;)