Si has contratado recientemente fibra óptica de Vodafone seguramente te hayan instalado el router **Sercomm Vox 2.5** y al acceder a su menú de configuración con el usuario **vodafone** y la contraseña que aparece detrás del router te habrás dado cuenta inmediatamente de que no tienes muchas opciones de configuración. Por ejemplo, no tienes cortafuegos ni forma de cambiar las bandas en las que opera el WiFi, entre otras. Para la mayoría de la gente eso no tiene por que ser un problema, pero en mi caso, lo fue dado que tengo un servidor con varias páginas webs desde el que también sirvo bastantes cosas por lo que el router empezó a darme problemas desde el vamos.
Por defecto, las opciones que aparecen en el router son tan pocas que incluso es hasta sospechoso. De hecho, así lo planteé en el grupo de Telegram del podcast SeguridadOverflow:

– Tiene que tener más opciones – les dije a los integrantes del grupo. – No me creo que sea tan básico.

Llamé entonces a Vodafone plantéandoles el principal problema que me daba el router y que no era otro que el no poder acceder desde casa, es decir, desde dentro de mi wifi, a las webs que estaban alojadas en el servidor conectado al Sercomm. El «técnico» empezó a hacer cambios en el router y al tiempo que me los iba comentando:

– A continuación lo que haré será deshabilitar el cortafuegos.
– ¡Un momento! ¿¡Cómo que deshabitar el cortafuegos!? – le pregunté.
– Si – me dijo. – Puede ser la causa del problema.
– ¡Pero si este router no tiene cortafuegos! – le dije mientras esbozaba una sonrisa sospechosa. – Yo no lo vi.
– Son unas opciones que no están disponibles para el cliente – Me aclaró en un tono muy cortante.

Me cabreé, lógicamente, pero no lo manifesté. La llamada concluyó con el resultado esperado: por un lado no me pudo decir por que demonios no podía acceder a mis páginas web desde dentro de casa y por otro descubrí que mis sospechas estaban bien fundadas. Y ya, teniendo la certeza de la existencia de un menú oculto lo primero que hice fue ponerme a ver cuales eran esas opciones para ver si valía la pena perder tiempo buscando métodos para hacerme con la contraseña del admin. El lector atento, en este punto estará pensando:

- Si no tiene la clave del admin ¿cómo demonios va a ver las opciones del admin?

Bueno, la observación es correcta. Pero ya he asistido varios años a la Euskal Encounter, y el haber conocido el HackIt, es decir, las pruebas de seguridad informática que tienes que pasar para coronarte como «el hacker definitivo», han despertado en mi (gracias @marcan42) una forma de pensar que antes no tenía. La verdad es que nunca he superado más que una o dos (suelen ser 6 o 7) pero si que me han ayudado a desarrollar esa mentalidad intrusiva, que si bien la mayoría del tiempo no sirve para un carajo, en casos como el que atañe a este artículo, ha dado resultado.

¿Cómo he «husmeado» en la cuenta admin sin ser admin»?

Bien, si usamos Chrome para acceder a la web del router (http://192.168.0.1) y metemos el usuario **vodafone** y la contraseña de administración que está en la pegatina de detrás acabaremos en su menú principal. Una vez en el menú principal vamos a la pestaña «Configuración». Vemos entonces, en el lado izquierdo, que se nos muestran las siguientes opciones:

- Idioma
- Contraseña
- Configuración de energía
- Compartir contenido

Luego, arriba a la derecha, en el desplegable cambiamos de «modo básico» a «modo experto» y podremos ver algunas opciones más:

- Idioma
- Contraseña
- Configuración de energía
- USB
- Compartir contenido

- Compartir impresora
- Configuración
- LAN
- Móvil

Aún con esas últimas vemos que son muy pocas opciones para un router tan «moderno». Entonces, en esa misma página hacemos click derecho en algún lado donde no haya nada y le damos a «Inspeccionar». Se nos abrirán las opciones de desarrollador en la parte derecha de la ventana. Allí vamos a la pestaña **Sources** para poder navegar por el contenido de las carpetas del código de la web del router. Ubicamos la carpeta **js** y la desplegamos haciendo click en la flechita hacia abajo. Una vez desplegada vemos varios archivos .js (JavaScript). Hacemos click sobre **mainFunctions.js** y podremos ver su código. Buscamos el siguiente código:

```
usermode = getUserData('usermode', data);
```

En mi caso está en la línea 38 pero dependiendo de la versión de firmware del router puede estar en cualquier otra línea. Esté en la posición que esté, hacemos click sobre el número de la línea siguiente (en mi caso la 39). El número de línea se resaltará y la línea quedará marcada. Volvemos a hacer click sobre la pestaña «Configuración» de la web y cuando el navegador empiece a re-cargar la sección se detendrá en la ejecución de la línea 39 dado que al haber hecho click sobre ella se lo hemos indicado expresamente.
Para ese entonces la carga de la web estará en pausa pero en la línea anterior ya se habrá cargado la variable «usermode». Lo bueno es que al interrumpir la carga de la web sólo una línea después, lo que haremos será volverla a pasar pero esta vez con el valor que nos interese. Entonces vez comprobado que la página detuvo su carga vamos a la pestaña **Console** y escribimos lo siguiente:

```
usermode="admin";
```

Y presionamos ENTER. Veremos entonces como la consola habrá inyectado el valor «admin» en la variable usermode, sobreescribiendo el valor anterior. Lo que haremos entonces será darle al botón azul de play (si no lo vemos tendremos que volver a hacer click en la pestaña sources) y si todo ha salido bien, deberíamos tener acceso visual del lado izquierdo a todas las opciones que antes no aparecían, cosa que nos permite comprobar que efectivamente el router es más avanzado de lo que los de Vodafone nos dejan ver.

Lógicamente y como bien indicaba el podcaster de SeguridadOverflow en su canal de Telegram el haber descubierto esto no me proporcionaría ninguna ventaja real dado que la autenticación se haría a nivel de servidor y no a nivel de usuario que es el JavaScript que yo estaba intentando manipular por lo que, al intentar guardar algún dato o modificar algún campo jamás iba a poder hacerlo permanente. Es cierto, pero al menos me permitiría ver si valía la pena perder el tiempo tratando de conseguir la clave del admin o no. Y la verdad es que el router es un router bastante decente. Dual band simultánea. AC. Compartición de archivos. En fin, un router moderno decente. Así que sí que valdría la pena ponerse a ver como demonios conseguir la clave del admin.

CONSIGUIENDO LA CLAVE DEL ADMIN

Leyendo un poco en los foros de Internet descubrí que los routers Sercomm suelen venir con una clave admin por defecto. Debería ser lo lógico si no, de no funcionar el botón de reset, estaría jodida la cosa. Después de unos días di con la contraseña por defecto de este router. En el caso de Vodafone España es:

Usuario: **admin**
Contraseña: **VF-ESvox2.5**

Pero mi gozo en un pozo. La clave no funcionaba. Se me ocurrió entonces resetear el router una última vez y casualmente esa vez no lo tenía conectado a la ONT. Intenté conectarme al router con la clave por defecto y entró. Entonces ahí me pasó algo en el cerebro. ¿Por qué o en qué momento se había cambiado la clave admin por defecto, por otra que no era esa? Y ahí me di cuenta que lo único que había cambiado es que el router no estaba conectado a la ONT. Lógicamente lo conecté, esperé unos minutos y en el proceso el router se reseteó porque vi que la WiFi ya no aparecía. ZAZ! Esa emoción del script kid... Sudando

estaba ya. La WiFi vuelve a aparecer, me conecto por WiFi, intento usar la clave por defecto y no me conecta. Y ahí lo vi todo claro: lo que ocurre realmente es que cuando el router se enciende por primera vez, o después de un reseteo, la clave admin por defecto si está operativa pero siempre y cuando no lo conectes a la ONT. Porque la primera vez que se conecta a la ONT ésta reconfigura el router cambiando la contraseña VF-ESvox2.5 que tenía por defecto por otra que le indica Vodafone. No se si lo hará por SSH. Seguramente si, porque la ONT tiene los datos de logueo por defecto del SSH de los Sercomm de Vodafone España y en la configuración vi (cuando me logueé con la clave admin por defecto) que el SSH esta activado. Así que debido a los cambios que la ONT realiza en el router a partir de ese momento, ya no podrás usar la cuenta admin por defecto y tendrás que llamar a Vodafone cada vez que quieras realizar un cambio importante en la configuración. Cosa que no es nada aceptable para un geek y mucho menos para alguien como yo que tiene montado un servidor con varias páginas webs y otros servicios varios. Plus, cuando llames, podrás comprobar que el «técnico» de Vodafone que se conecte a tu router podrá ver los dispositivos que tienes conectados a él, sus direcciones macs, y algunas otras cosas que sólo deberías ver tú.
¿Qué se puede hacer entonces? Pues obtener la clave de admin final, tener control de tu router y proteger la privacidad de tus conexiones.

CONSIGUIENDO LA CLAVE «FINAL» DEL ADMIN

Aquí empieza lo realmente técnico. No es que lo del código anterior no sea técnico, pero esto es un nivel más. Sabiendo lo anterior asumí que la ONT preguntaría al router, o vería si la clave SSH del admin es la que viene por defecto, y en el caso de ser positivo, iniciaría la re-configuración por SSH. Así que debería haber (si o si ya que se hace por ethernet) un intercambio de paquetes entre la ONT y el router. Así que llegó la hora de usar el WireShark. Y ahí vino el primer problema y la primera aclaración al lector:

Estimado lector, si usas Wireshark en macOS, y haz reinstalado macOS desde cero, no desde copia de TimeMachine o actualizando desde una versión anterior, asegúrate de instalar WireShark desde el instalador .pkg. No copies la App sin más porque nunca vas a poder entender por que demonios no tienes permisos para capturar paquetes si incluso llegas a ejecutar WireShark con sudo. Cuando lo instalas desde el .pkg oficial, el instalador ejecuta un script que establece los permisos para usar las interfaces para capturar.

Dicho lo anterior, el proceso es muy sencillo, al menos teóricamente:

1. Desconectar el router Sercomm de la ONT y resetearlo mediante el botón pequeñito de atrás.
2. Conectar el router al puerto de un switch que tenga la opción de «port mirroring» activada (en mi caso el TL-SG108E).
3. Conectar el ordenador al switch en el puerto que está siendo «espejado».
4. Lanzar WireShark en el ordenador y empezar a capturar la interfaz ethernet.
5. Conectar la ONT al switch y esperar hasta uno o dos minutos después de que el router Sercomm se reinicie.
6. Parar la captura y analizar los paquetes.

Como realizar una captura de paquetes en un puerto espejado no va a ser algo que voy a explicar en este artículo porque se haría más eterno de lo que ya es. Si os interesa me decís y hago un post o un video al respecto. Una vez que tenemos la captura, procedemos a guardarla (por las dudas) y posteriormente a analizarla.

Para obtener la contraseña del admin tenemos que buscar la línea:

```
InternetGatewayDevice.X_Management.LoginAccount.1.Password
```

Nos saldrá de la siguiente forma:

```
<ParameterValueStruct>
  <Name>
    InternetGatewayDevice.X_Management.LoginAccount.1.Password
  </Name>
  <Value xsi:type="xsd:string">
    XXXXXXXX
  </Value>
```

```
</ParameterValueStruct>
```

XXXXXXXX será la contraseña final del admin que nos dará acceso completo al router, como reza el título de este artículo. Si sabemos capturar paquetes es tan sencillo como eso. En mi caso todo el proceso hasta obtener la contraseña del admin me llevó semanas de mal dormir y horas de volver locos a **@nineain** y a **@segoverflow**. Espero que a vosotros no os lleve más que un par de horas. De todos modos guardaos la captura porque más adelante escribiré otro post donde explicaré que otras sacar de esa captura, porque me ha parecido ver cosas interesantes por ahí

Y si todavía os queda la duda de por qué no podía acceder a las webs que tengo montadas en mi servidor hogareño, es simplemente porque el router Sercomm que nos proporciona Vodafone no tiene la funcionalidad «NAT Loopback», necesaria para hacer exactamente eso.

ACTUALIZACIÓN 1: El problema del NAT loopback es historia pasada porque, si bien sigo teniendo vodafone, ya no uso el router Sercomm. En su lugar me he montado un router con Debian y he reemplazado el Sercomm por él.

ACTUALIZACIÓN 2: Hay una forma más fácil para capturar los paquetes que usando un switch. Se puede hacer directamente desde el router Sercomm. En este post se explica.