Seguridad en Redes y Telecomunicaciones

Grado en Criminología

Curso 2017-18

Guía de Prácticas

Práctica 1.- Herramientas básicas de Seguridad
Sesión 3. Herramientas de seguridad

Objetivo: En esta sesión abordaremos como:
- Gestionar las contraseñas de nuestros equipos y servicios en Internet.
- Determinar que esta pasando en nuestro equipos y en la red.

1.- Las contraseñas y su gestión

Hoy en día, el acceso a nuestros equipos y servicios de red descansa en gran medida en conocer una contraseña o clave. Así la seguridad del servicio descansa en que solo nosotros conocemos la clave y ésta es difícil de adivinar por otra persona/máquina que no este autorizado a usarlo.

Lamentablemente, muchos usuarios tiende a poner claves sencillas, o relacionadas con elementos de su entorno, de forma que sean fáciles de recordar. Esto tiene como efecto, que no es muy difícil para un ciberdelincuente de adivinar lo que le permite acceder a nuestra información y recursos.

Este sistema de autenticación[1] es bueno en tanto en cuanto definamos lo que se denomina una *clave fuerte*, es decir, es difícil de adivinar. Para generar una clave con esta característica se establecen una serie de reglas que debemos considerar[2], como son:

- Tiene ocho caracteres como mínimo.
- No contiene el nombre de usuario, el nombre real, el nombre de la empresa o cualquier información que puedan relacionar con nosotros (nombre de un hijo, una mascota, etc.)
- No contiene una palabra completa.
- Es significativamente diferente de otras contraseñas anteriores.
- Está compuesta por caracteres de cada una de las siguientes cuatro categorías:
- Categoría de caracteres
- Letras mayúsculas
- Letras minúsculas
- Números
- Otros símbolos: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

Una contraseña puede reunir todos los criterios anteriores y aun así ser insegura. Por ejemplo, Hello2U! cumple con todos los criterios mencionados para una contraseña segura, pero es insegura porque contiene una palabra completa. H3ll02U! es una alternativa más segura porque reemplaza algunas de las letras en la palabra completa con números e incluye espacios.

Puede aplicar las siguientes recomendaciones para recordar una contraseña segura:

- Cree una sigla con una información que sea fácil de recordar. Por ejemplo, elija una frase que tenga significado para usted, como Mi hijo nació el 12 de diciembre de 2004. Con esa frase

1 Autenticación es el proceso de confirmar que algo o alguien es quién dice ser (https://es.wikipedia.org/wiki/Autenticaci%C3%B3n).

2 Extraídas de Extraida de http://windows.microsoft.com/es-es/windows-vista/tips-for-creating-a-strong-password.

como guía, puede usar Mhne12/Dic,4 como contraseña.

- Use números, símbolos y errores de ortografía para reemplazar letras o palabras en una frase fácil de recordar. Por ejemplo, Mi hijo nació el 12 de diciembre de 2004 puede transformarse en M'igon@$io 12124 (se pueden usar espacios en la contraseña).
- Relacione la contraseña con un pasatiempo o deporte favorito. Por ejemplo, “Me encanta el bádminton” puede transformarse en Mn'kant6ehlB@dm1nt()n.

En cualquier caso, si consideramos que debemos anotar la contraseña para poder recordarla, deberíamos plantearnos elegir otra ya si dejamos por escrito una contraseña es posible que caiga en manos de terceras personas.

El esquema anterior es válido en tanto en cuanto gestionemos pocas contraseñas. Pero la realidad es que cada día más usamos Internet para desarrollar muchas actividades de nuestra vida y eso nos obliga a mantener un elevado número de contraseñas: tiendas online, redes sociales, banca electrónica, etc. Para evitar tener que recordar tantas contraseñas han surgido programas, *gestores de contraseñas*, que nos permiten tanto gestionar como generar las contraseñas que necesitemos. Para ello, solo debemos limitarnos a recordar la contraseña maestra del gestor y este se encarga de almacenar el servicio y la contraseña.

El gestor de contraseñas mantiene cifradas las contraseñas de todos los servicios para que nadie pueda leerlas. De esta forma podemos usar contraseñas muy fuertes que no necesariamente sean fáciles de recordar.

El gestor que nosotros vamos a utilizar se llama **KeePass**[3], que es de código abierto (si bien hay otros para Windows como LastPass, 1Password, Jpasswords, etc.). Podéis encontrar una guía rápida de uso en la dirección http://www.destroyerweb.com/manuales/keePass/keePass.htm.

Ejercicio 1.- Utilizar *KeePass* para generar y almacenar la contraseña de un servicio de Internet.

Nota: Dado que el servicio es personal, borrar de las capturas de pantalla realizadas la información personal que aparezca.

Si bien no vamos a cubrirlo en nuestras prácticas, comentar que hay gestores de contraseñas para diferentes plataformas:
- Windows: https://www.adslzone.net/2016/04/07/los-mejores-gestores-contrasenas-windows-10/.
- Android: http://www.elandroidelibre.com/2015/02/los-mejores-gestores-de-contrasenas-para-android.html.
- iPhone: http://www.ipadizate.es/2015/05/16/los-mejores-gestores-de-contrasenas-para-iphone-y-ipad/
- Gestores que almacena las contraseñas en la nube: http://www.genbeta.com/web/especial-contrasenas-seguras-cinco-herramientas-para-gestionar-contrasenas-online, que permiten acceder a ellos desde cualquier lugar.

Actualmente, muchos servicios de red permiten configuralos para utilizar dos claves: una que recordamos nosotros y con la que nos identificamos en primera instancia; otra, que el servicio nos hace llegar por otro medio (SMS, correo electrónico, etc.) y que usamos en un segundo paso. Es los que se denomina *autenticación en dos fases* (2FA). En las prácticas de la asignatura no vamos a cubrir este tipo de autenticación dado que cada servicio de la red se configura normalmente. Este tipo de autenticación es el que actualmente utiliza la banca electrónica para hacer una transacción, pero que también esta presente por ejemplo en muchas redes sociales, si bien no esta configurado por defecto.

3 https://keepass.info/

- **Gestor de contraseñas del navegador**

Un caso particular de gestor de contraseñas nos lo suministran los navegadores que son capaces de almacenar de forma segura las contraseñas de los sitios web (no de servicios locales) en los que nos debemos de autenticar.

Al navegar por Internet, cuando alcanzamos un sitio que nos pide autenticación, el navegador automáticamente nos pregunta si deseamos almacenar el usuario y contraseña del sitio. Esto es cómodo pues nos evita tener que recordar los diferentes identificadores de usuarios que tenemos en banca, redes sociales, etc.

El problema que por defecto esta información no tiene protección, cualquiera que acceda físicamente a nuestro navegador persona puede conocer esa información. El proceso para verlas es diferente según el navegador que usemos:

- Chrome: https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=es.
- Firefox: https://support.mozilla.org/es/kb/administrador-de-contrasenas-recordar-borrar-cambiar-importar-contrase%C3%B1as-firefox.

Podemos mejorar la seguridad evitando que cualquiera acceda a las contraseñas del navegador utilizando una contraseña maestra. El procedimiento será diferente según el navegador:

- Firefox: https://support.mozilla.org/es/kb/Proteger%20las%20contrase%C3%B1as%20almacenadas%20mediante%20una%20contrase%C3%B1a%20maestra.

- Chrome: lo permite solo si estas se almacena en la nube (passwords.google.com).

Importante: En Firefox, si olvidamos la contraseña maestra podemos restablecerla pero el proceso borrará todas las contraseñas guardadas localmente.

> **Ejercicio 2**: Utiliza el navegador Firefox que esta instalado en el equipo de prácticas y accede a algún servicio de la ugr o externo a la universidad que te solicite autenticación de forma que el navegador te solicite almacenar el identificador y contraseña. Una vez realizado, indica que deseas almacenar la contraseña. Tras lo cual:
> a) Muestra cómo podemos acceder a los datos almacenados en el navegador relativos a la contraseña almacenada.
> b) Activa la contraseña maestra del navegador. Cierra el navegador y vuelve arrancarlo y accede a la dirección utilizada antes. Cuales son ahora los pasos para autenticarte.
> c) Si bien esta contraseña guardada se borrará al reiniciar el computador, puedes borrar la contraseña guardada, restableciendo la contraseña maestra.
>
> Nota: no olvides borrar de las capturas de pantalla los campos de datos que contengan información privada.

Nota: en equipos públicos debemos de tener especial cuidado en NO almacenar contraseñas en el navegador bajo ningún concepto.

2.- Registros de eventos del sistema

Windows, como el resto de sistemas operativos, mantiene un registro de los eventos significativos

que ocurren en el sistemas y las aplicaciones al objeto de que podamos realizar una auditoría del sistema para ver si el equipo esta funcionando correctamente o ver si se ha producido algún incidente.

Para acceder estos registros se utilizar el "Visor de eventos" al que podemos acceder desde "Inicio→Panel de control→ Rendimiento y Mantenimiento→ Herramientas administrativas→ Visor de eventos". También lo podemos lanzar directamente desde "Inicio→Ejecutar" invocando la orden "`eventvwr.msc`". En Windows XP se mostrará de forma similar a la Figura 1.

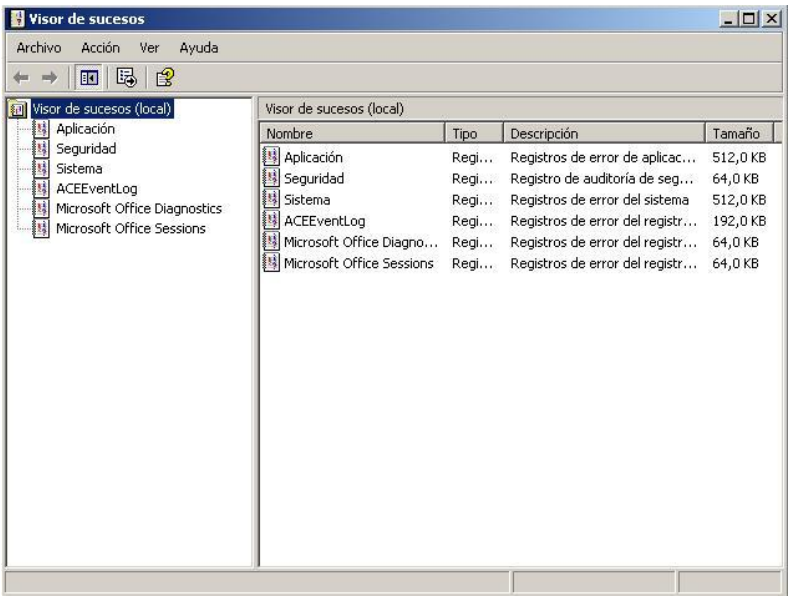

Figura 1.- Ventana principal del Visor de sucesos.

Como muestra el panel izquierdo de la ventana, los registros se agrupan lógicamente en cuanto afectan entre otros a:

- *Aplicaciones* – incluyen eventos relacionados con los programas que se estan ejecutando (acciones importante, avisos, errores, caídas).
- *Seguridad* – Incluyen eventos relacionados con entradas/salidas de usuarios del sistema, cambios en las políticas de seguridad, bloqueo de cuentas, etc.
- *Sistema* – eventos sobre Windows y sus servicios (parada o arranque), eventos hardware, etc.

Al elegir una opción de las anteriores, en el panel derecho se nos muestran todos los registros que afectar a la selección registrados por el sistema.

Dado que el número de registros suele ser muy elevado, la opción "View" del menú principal permite definir un filtro para que se muestre en un momento dado los eventos relevantes de un tipo.

Desde el punto de vista de la "Seguridad" algunos eventos importantes en Windows XP son:

Event ID 528 – Un usuario se ha autenticado correctamente.
Event ID 529 – Un usuario ha fallado al autenticarse debido a una clave errónea.
Event ID 535 – Fallo de autenticación debido a que la clave a expirado.
Event ID 538 – El usuario ha salido del sistema.
Event ID 539 – Fallo de autenticación de usuario debido a que la cuenta está bloqueada (demasiadas claves erróneas).

Event ID 682 – Autenticación nuevas tras cambiar de sesión.
Event ID 683 – El usuario sale del sistema tras cambiar de sesión.

Nota: Debemos tener presente que los identificadores de los eventos varían según la versión del sistema Windows que usemos.

Ejercicio 3. Accede al visor de eventos de Windows y localiza dos eventos de cada categoría. Indica que reflejan cada uno de estos eventos buscando información de los mismos en Internet.

En la dirección que se indica a continuación, puedes encontrar un pequeño manual para usar el gestor de eventos en Windows XP:
http://www10.ujaen.es/sites/default/files/users/sinformatica/guiaspracticas/Windows%20XP%20-%20El%20visor%20de%20sucesos.pdf

3.- ¿Quién esta conectado a mi equipo?

Si deseamos conocer quién esta conectado a mi equipo, Windows suministra la herramienta **`netstat`**. Para usarla, bien abrimos una consola de texto a través de "Inicio→Todos lo programas→Accesorios→Command Prompt", o bien la invocamos directamente desde "Inicio→Ejecutar" escribiendo "`cmd`".

Una vez que tenemos abierta la consola de órdenes utilizaremos la orden `netstat -noa` que nos muestra estado de las conexiones de red. Sera algo similar a la Figura 2.

```
D:\DOCUME~1\ADMINI~1>netstat -noa

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1132
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING       400
  TCP    127.0.0.1:1035         0.0.0.0:0              LISTENING       3792
  TCP    127.0.0.1:1067         127.0.0.1:1068         ESTABLISHED     2688
  TCP    127.0.0.1:1068         127.0.0.1:1067         ESTABLISHED     2688
  TCP    127.0.0.1:1070         127.0.0.1:1071         ESTABLISHED     2688
  TCP    127.0.0.1:1071         127.0.0.1:1070         ESTABLISHED     2688
  TCP    169.254.[illegible].170:139    0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       1132
  TCP    [::1]:1025             [::]:0                 LISTENING       400
```

Figura 2.- Salida de la orden `netstat`.

Como podemos observar en la columna "Foreing Addres" aparecen las IP de máquinas conectadas a la nuestra. Aclarar que en el caso de la Figura 2, la dirección 127.0.0.1 es lo que se denomina *localhost* (huesped local) corresponde a nuestra máquina, es decir, podemos interpretarla como "esta máquina". Es lo que se denomina *dirección IP loopback* y es el mecanismo por el cual nuestro computador accede a los servicios de red locales, o sea, que nuestro computador esta conectado a la red con él mismo.

Esta orden además nos permite conocer los puertos abiertos, su estado, etc.

Ejercicio 4. Busca en Internet información sobre esta orden de cara a poder indicar cuales son los datos que nos muestra la orden, es decir, cual es el significado de cada campo (columna).

Nota: En clase de teoría veremos con detalle el significado de cada uno de ellos.

4.- ¿Quién usa nuestra WiFi doméstica?

Este apartado tiene como objetivo que podáis comprobar en casa que otros equipos están conectados a nuestro *router* a través de la WiFI. Esto no es posible en nuestro laboratorio ya que los equipos no disponen de tarjetas WiFi.

- **Ver red doméstica con las herramientas de Windows**

Para ver la topología (estructura) de red doméstica, pinchamos en el icono de la red wifi y elegimos "Abrir el Centro de Redes y recursos compartidos", como se indica en la Figura 3.

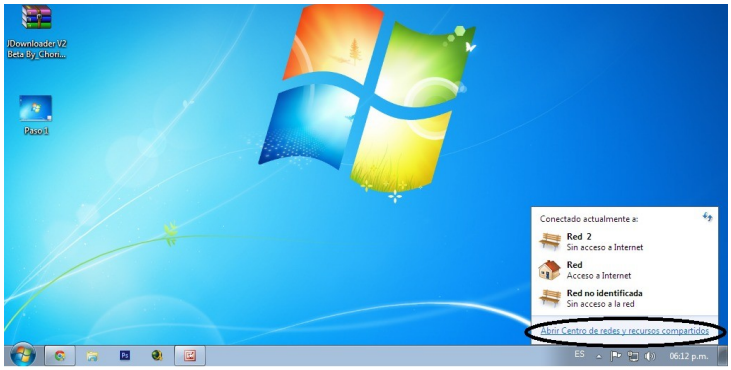

Figura 3.- Acceso a la configuración de la red desde la barra de tareas.

En la ventana que se abre, pinchamos en el enlace "Ver mapa completo" como en la Figura 4.

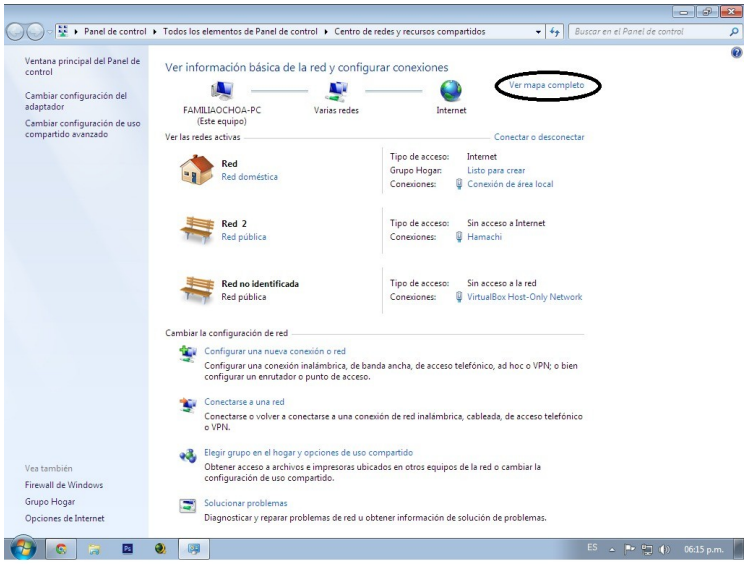

Figura 4.- Ventana "Centro de redes y recursos compartidos".

En la ventana se nos muestra el mapa de la red doméstica con los diferentes equipos conectados, como por ejemplo puede verse en la Figura 5.

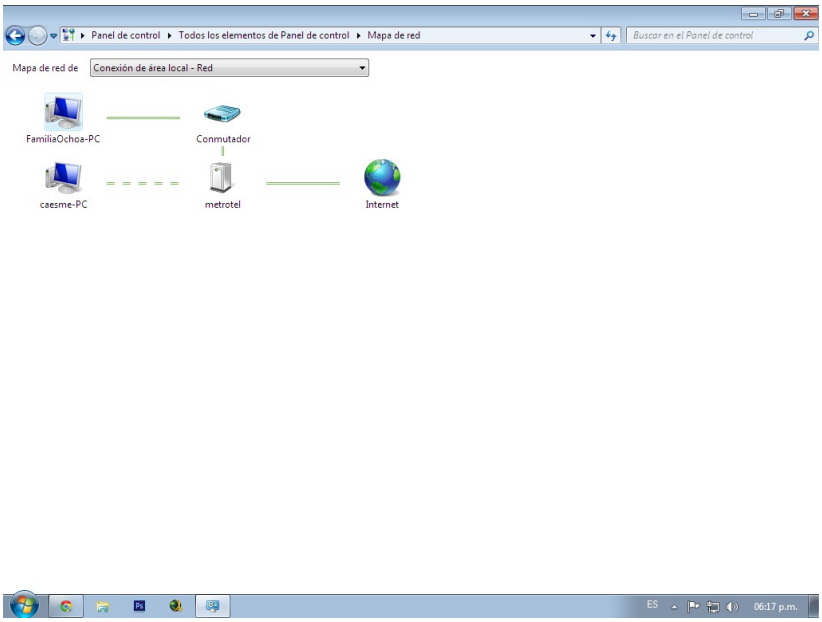

Figura 5.- Ventana del “mapa de red”.

- **Mapa de red con herramientas adicionales**

Existen multitud de herramientas para analizar los equipos conectados a la red, como por ejemplo, *Wireless Network Watcher*, *Air Dnare*, etc. Nosotros veremos una herramienta más simple pero efectiva, denominada **WiFI Guard**.

Tras instalar e iniciar la herramienta, la pantalla que nos muestra es similar a la Figura 6 salvo que inicialmente esta con la ventana principal en blanco:

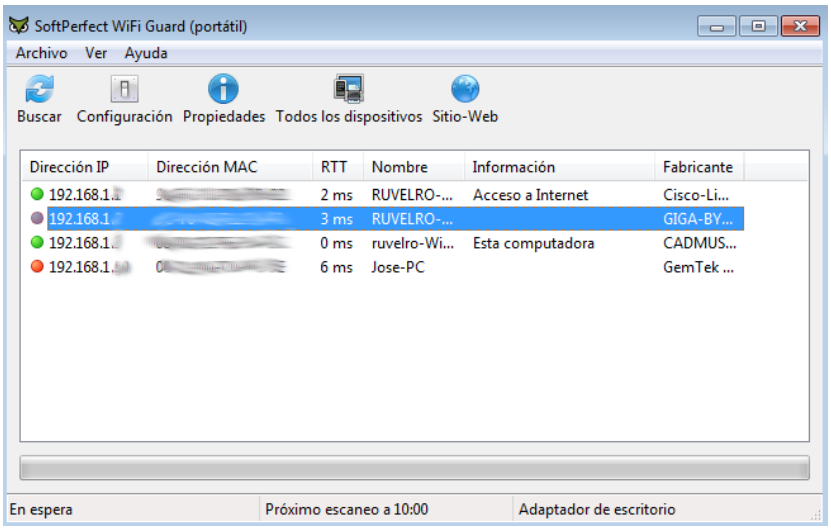

Figura 6.- Ventana de *WiFiGuard*.

Para analizar la red, seleccionamos el icono “Buscar” y tras finalizar podemos ver y analizar los equipos de la red.

Para finalizar, indicar que en dispositivos móviles también disponemos de varias aplicaciones para ver que equipos están conectados a nuestro router. Por ejemplo, el escáner de red `Fing` (https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=es). Esta aplicación y una vez identificados todos los equipos autorizados a conectarse a nuestro router, nos permitirá identificar si hay algún intruso en la misma.

También existen apps para ver las WiFis que están a nuestro alcance y sus características, como por ejemplo `Wifi Analyzer` para Android.

Ejercicio 5. Utiliza *WiFI Guard* o una aplicación del móvil para identificar los equipos conectados en tu WiFi doméstica.
Nota: como siempre no olvides borrar de las capturas de pantalla la información personal.