OBJETIVO: Protege tu equipo…. de intrusiones

INVESTIGA:

- ¿qué son las cuentas de usuario? ¿Y los roles?
- ¿Qué es un software antivirus? ¿qué es la base de datos de firmas?
- ¿En qué se diferencia un antivirus de un antiespía?

USA:

- Avast, Avira
- Spybot S&D

EXPLICA:

Haz un juego en Scractch que explique, durante el juego, qué es el malware y la importancia de los antivirus.

Como hemos dicho en los apartados anteriores, la confidencialidad es una de las propiedades fundamentales que debe ofrecer un sistema de computación considerado seguro. ***Confidencialidad*** es asegurar que a tu sistema, y en particular a tus datos, sólo acceden aquellos usuarios que tienen los privilegios para hacerlo.

Utilizando herramientas de cifrado, como se ha detallado en el proyecto anterior, protegemos nuestros datos de aquellos que no disponen de la clave para poder acceder a los mismos. Sin embargo, podemos platearnos dos preguntas.

La primera es, ¿no sería mejor, quizás, que se cortase el camino antes? Es decir, ¿por qué alguien sin permiso para acceder a los datos, puede llegar a ellos, aunque estén cifrados?

Y la segunda, ¿estamos seguros de que nadie ha podido entrar a nuestro sistema y, por lo tanto, llegar a nuestros datos, de una manera fraudulenta, sin que nosotros lo sepamos?

En este último caso, además, podríamos estar ante otro peligro que atentaría contra otro de los principios de un sistema seguro: la ***integridad***. Alguien que de manera fraudulenta entrase en nuestro sistema, no sólo podría acceder a nuestros datos sin nosotros saberlo, sino que podría, incluso, poner en peligro el buen funcionamiento del sistema.

Por tanto, debemos asegurarnos que la respuesta a ambas preguntas es positiva.

En el caso de la primera, la herramienta a utilizar son las cuentas de usuario y los roles de usuario. Una ***cuenta de usuario*** es un mecanismo de control de acceso a un sistema de computación. Dicho mecanismo consiste en el control y autentificación de los distintos usuarios de un sistema por medio de una lista donde se encuentran definidos nombres de usuario y contraseñas asociadas a los mismos. Además, cada cuenta de usuario lleva asociada los permisos que tendrá el usuario

propietario de la misma respecto al uso de los recursos del sistema (almacenamiento, acceso a datos y aplicaciones…)

El punto débil de este sistema de control puede encontrarse en las contraseñas elegidas por los usuarios. Las recomendaciones para que una contraseña sea segura son:

- ***longitud mínima***: las contraseñas deben tener un mínimo de 8 caracteres, aunque lo recomendado es que supere los 14.
- ***combinación de caracteres***: las contraseñas deben estar compuestas por una combinación de caracteres de distinta naturaleza. Es decir, deben mezclarse mayúsculas y minúsculas, letras y números y deben contener caracteres no alfabéticos.
- ***Sin significado ni repeticiones***: se debe evitar que la contraseña contenga caracteres con significado (palabras de algún idioma, números que indiquen fechas o referencias conocidas...)y deben evitarse las contraseñas con repeticiones de caracteres del tipo '1111111' o '123456'.

Los sistemas de computación disponen, además, de mecanismos que pueden obligar al usuario a cambiar la contraseña de forma periódica y que prohiben la repetición de contraseñas en periodos de uso relativamente cercanos.

No seguir estas recomendaciones permitiría a cualquiera que quisiera acceder a un sistema el realizar ***ataques de fuerza bruta***[13] o ***ataques de diccionario***[14] para tratar de averiguar la contraseña de una cuenta determinada.

Asociado al concepto de cuenta de usuario se encuentra el de rol. El ***rol o perfil de un usuario*** son los permisos que se establecen sobre determinada cuenta de usuario y que especifican lo que ese usuario podrá hacer con el sistema. El concepto de perfil de usuario está relacionado, también, con la seguridad de un sistema, ya que en caso de violación de una cuenta de usuario (por que, por ejemplo, se ha descubierto la contraseña de la misma) el intruso sólo podrá hacer aquello que el perfil del usuario le permita. Es por ello que operaciones que permitan cambios importantes de configuración de un sistema se asocien únicamente a perfiles de tipo administrador, mientras que roles de tipo usuario limitado se asocien a los usuarios comunes del sistema, otorgándoles permisos de acceso únicamente a sus propios datos y a la ejecución y uso de aplicaciones determinadas.

Por tanto, una buena política de cuentas de usuario y perfiles locales en un ordenador pueden evitarnos accesos no deseados al sistema. Sin embargo, a día de hoy, no existe sólo esa "puerta de

13 *Ataque de fuerza bruta*: proceso para tratar de averiguar una contraseña y que consiste en probar todas las posibles combinaciones de caracteres hasta encontrar la coincidencte con la contraseña.

14 *Ataque de diccionario*: proceso que intenta averiguar la contraseña de acceso a un sistema probando con una lista o diccionario de contraseñas comunes o palabras comunmente utilizadas como contraseña.

entrada" a nuestros sistemas, pues existe otra puerta por la que, si no tenemos cuidado, pueden introducirse intrusos en nuestro sistema: la conexión de red.

La conexión constante a la red y el uso que hacemos de ella puede producir que, sin saberlo, intrusos accedan a nuestro sistema, se escondan en él y hagan uso del mismo para fines no lícitos sin que nosotros lo sepamos.

Por ello es fundamental que todo sistema de computación disponga de software especializado que esté constantemente vigilando todo aquello que llega y sale de y por la red, y todo aquello que se está haciendo en el sistema de computación. Este software especializado son los antivirus y los programas antiespía.

Un ***antivirus*** es un software que se encuentra residente en el sistema (siempre está en ejecución) y que está especialmente diseñado para analizar todo proceso que se realiza en un sistema de computación para detectar, bloquear y eliminar posibles ejecuciones de software malicioso o *malware*.

En entornos no profesionales es habitual usar versiones gratuitas de los programas de antivirus más conocidos, como Avast, McAffe o Avira (ver una comparativa en la entrada "Los mejores antivirus para protegerte este 2017", de SoftZone[15]). Estos antivirus, a pesar de su gratuidad, mantienen las ***bases de datos de firmas de antivirus***[16] actualizadas y son una solución eficaz ante un uso moderado y prudente de un sistema conectado en red.

Sin embargo, muchas veces es necesario complementarlos con otros programas especializados en la búsqueda de un tipo especial de malware: el software espía.

Los programas antiespía buscan malware del tipo spyware, programas que se instalan en el sistema con la intención de recopilar información del mismo y enviarla a través de la red. Habitualmente son programas que recopilan información con intención de usarla para campañas de marketing posteriores e, incluso, generación y envío de spam.

Programas como Spybot S&D (Search&Destroy) o Malwarebytes nos permiten protegernos de estos programas espías. En la página web de la *Oficina de Seguridad del Internauta*[17] (bajo el auspicio del *Instituto Nacional de Ciberseguridad, INCIBE*[18]) encontramos un conjunto de herramientas aconsejadas del tipo antivirus y antiespía[19] que podemos usar en nuestros ordenadores.

15 Los mejores antivirus para protegerte en Windows este 2017. SoftZone. URL: https://www.softzone.es/2017/04/29/los-mejores-antivirus-gratis-para-windows-para-protegerte-este-2017/

16 Todo antivirus, que no deja de ser un programa de ordenador, tiene unas características que lo identifican. Estas características son lo que se denomina la ***firma del virus***. Los antivirus mantienen una base de datos con estas firmas que les ayudan a identificar la presencia de un posible virus en un sistema de computación.

17 Oficina de Seguridad del Internauta, OSI. URL: https://www.osi.es/es

18 Instituo Nacional de Seguridad. INCIBE. URL: https://www.incibe.es/

19 OSI. Herramientas antivirus/antiespía. URL: https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=115