Actividad

Curso**: Elaboración de material de apoyo para Tecnología y FPB de los CEPA**

Necesidad de la Ciberseguridad

Ciberseguridad – Sesión 2

Índice

Introducción

"*Data Security Breach*" *by* *Blogtrepreneur* *in Flickr*

En esta actividad veremos conceptos básicos sobre ciberseguridad y por qué necesitamos protegernos. Tenemos dos actividades, una de ellas de perfil más avanzado por si queremos ir un paso más allá.

Un buen punto de partida para estudiar esto es el capítulo 1 del curso "Introducción a la ciberseguridad" de la CISCO Academy. Este capítulo explica qué es la ciberseguridad y por qué la demanda de estos profesionales está creciendo.

- Explica qué es su identidad y sus datos en línea, dónde se encuentra y por qué es de interés para los delincuentes cibernéticos.
- Analiza qué son los datos de una organización y por qué deben protegerse. Analiza quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, pero los profesionales de la ciberseguridad deben trabajar de acuerdo con la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

- Este capítulo también incluye contenido que explica brevemente la guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de la ciberseguridad para proteger a sus ciudadanos y su infraestructura.

Objetivos

1. Qué es la ciberseguridad
2. Qué son los datos personales y los datos empresariales
3. El perfil del atacante cibernético
4. Violación de seguridad

Desarrollo de la actividad

Actividad: ¿Qué ha pasado?

Las violaciones de seguridad ocurren cuando personas o aplicaciones intentan obtener acceso no autorizado a datos, aplicaciones, servicios o dispositivos. Durante estas violaciones de seguridad, los atacantes, sean infiltrados o no, intentan obtener información que podrían usar para conseguir beneficios financieros u otras ventajas.

En esta práctica verás algunas violaciones de seguridad para determinar qué fue tomado, qué ataques se usaron y qué puede hacer para protegerse.

Investigación de las violaciones de seguridad

1. Utilice los tres enlaces proporcionados de violaciones a la seguridad para completar la siguiente tabla.
2. Busque algunas violaciones de seguridad interesantes adicionales y registre los hallazgos en la siguiente tabla.

Fuente de referencia	¿Cuántas víctimas? ¿Qué robaron?	¿Qué ataques se utilizaron? ¿Cómo se protege usted mismo?
Robo en una smart home		
Facilité mis datos personales a lo loco y cometí un gran error		
Mi mejor selfie, mi peor publicación		

Reflexión

Después de completar la tabla anterior sobre las violaciones de seguridad, ¿qué podemos hacer para evitar estos tipos de infracciones?

Actividad avanzada: Comparar datos con un hash

Es importante saber si los datos fueron dañados o manipulados. Para comprobar si los datos fueron cambiados o si permanecen igual, puede usarse un programa de hash.

Un programa de hash realiza una función hash en datos o en un archivo, lo cual devuelve un valor (generalmente, mucho más corto). Hay varias funciones hash distintas, algunas muy simples y otras muy complejas. Cuando se ejecuta el mismo hash en los mismos datos, el valor devuelto es siempre el mismo. Si se implementa algún cambio en los datos, el valor hash devuelto será diferente.

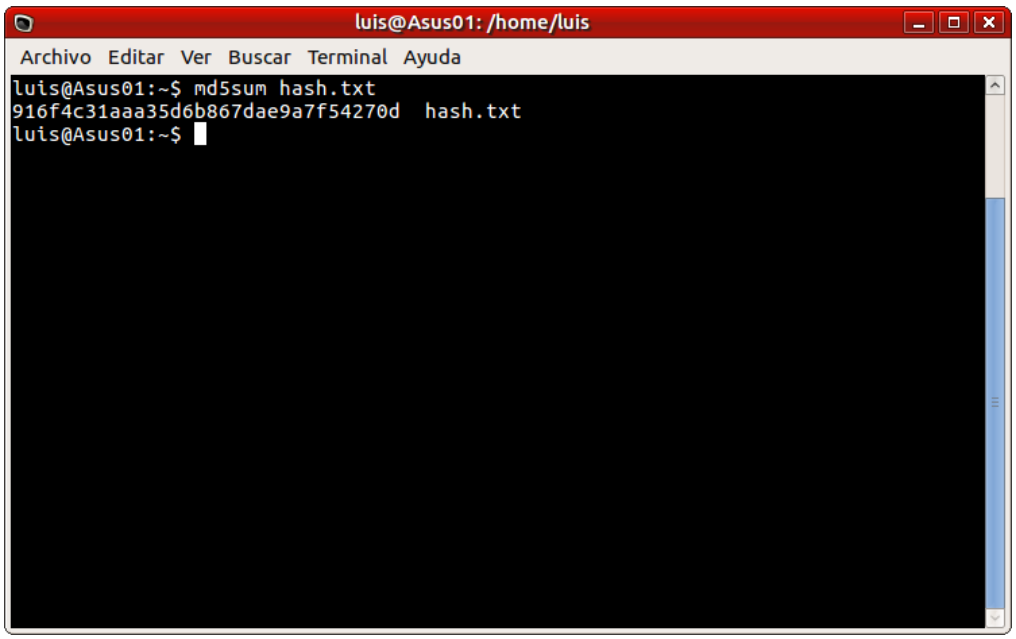
Procedimiento

Paso 1: Crear un archivo de texto.

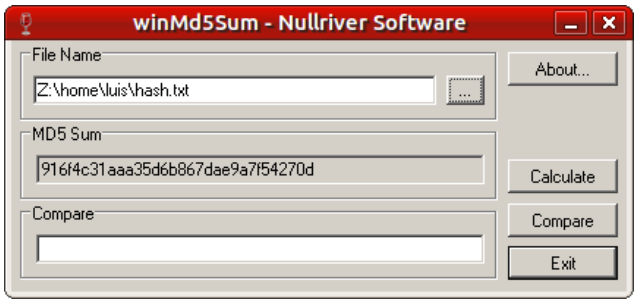
- Abre un editor de texto (bloc de notas) y escribe algún texto.
- Guarda el archivo con el nombre **hash.txt** en el Escritorio y cierra el editor de texto.

Paso 2: Cómo utilizar un programa para calcular hash

Para crear el hash en Linux, tenemos que abrir un terminal y escribir el comando `md5sum hash.txt` y pulsar intro.



Para crear el hash en Windows, podemos usar el programa portable winMd5Sum. Lo descargamos en nuestro equipo y hacemos doble clic para descomprimir en nuestro ordenador. Cuando terminemos, abrimos el programa y simplemente seleccionamos el archivo hash.txt y automáticamente nos dirá el hash md5 que ha generado.



Paso 3: Calcular un hash del archivo Hash.txt

- Calcula el hash del archivo. ¿Cuál es el valor junto a MD5? _____

Paso 4: Haga un cambio en el archivo Hash.txt

- Navegue hasta el Escritorio y abra el archivo Hash.txt.
- Realice un cambio menor en el texto, como eliminar una letra, o agregar un espacio o un punto y guarde de nuevo el archivo y cierre el bloc de notas.

Paso 5: Calcule un nuevo hash del archivo Hash.txt

- Calcule en Hash nuevamente.
- ¿Cuál es el valor junto a MD5? _____
- ¿El valor es diferente del valor registrado en el paso 3? _____