DESAFÍO 16 - INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

OBJETIVO

Conocer las herramientas y buenas prácticas en seguridad informática.

Aplicar estrategias para proteger información personal y profesional.

Configurar contraseñas seguras y utilizar directivas de grupo o local, para un control más exhaustivo.

Familiarizarse con antivirus, y sistemas de detección de intrusos.

WINDOWS

USER ACCOUNT CONTROL

1. Configurar User Account Control para que solicite confirmación siempre.

REMOTE DESKTOP

2. Habilitar el acceso por Remote Desktop.
3. Crear una cuenta de usuario llamada *bonustrack.*
4. Asignar permisos básicos (users) al usuario creado anteriormente.
5. Conceder privilegios al usuario *bonustrack* para tener la posibilidad de iniciar sesión a través de Remote Desktop.

DIRECTIVAS DE SEGURIDAD

6. Habilitar la complejidad de contraseñas.
7. Configurar:
    a. No expiren las contraseñas.
    b. Contraseñas con 10 caracteres de longitud.
    c. Evitar la reutilización de las últimas 10 contraseñas.
    d. Bloqueo de cuentas luego de 7 intentos fallidos.
    e. Desbloqueo automático después de 10 minutos.

WINDOWS DEFENDER

8. Habilitar *Windows Defender* (en el caso de que no se encuentre presente).
9. Descargar *raffle.exe* desde:

https://mega.nz/file/y24W2TSD#e6GxenMG4RGTzCsS9J9R2KlSFp9uvb13-qbzjNxvv64.

10. Verificar que Windows Defender lo haya detectado.

11. Subir el archivo descargado al sitio *VirusTotal*. https://www.virustotal.com/gui/home/upload
12. Analizar y mostrar el resultado.

HASHES

13. Crear un archivo de texto plano con el nombre *prueba1.txt* en donde el contenido del archivo sea únicamente *EducaciónIT*.
14. Calcular los valores hash del archivo con diferentes algoritmos, utilizando la herramienta *HashMyFiles*. https://www.nirsoft.net/utils/hash_my_files.html
15. Crear un segundo archivo, agregar el siguiente contenido *EducacionIT1,* agregando un 1 (uno) al final, y guardar con el nombre *prueba2.txt.*
16. Volver a calcular los hashes y verificar si los mismos han cambiado con respecto a los anteriores.

VOLÚMENES DE DISCOS CIFRADOS

17. Usar *VeraCrypt* para crear un volumen de disco cifrado de 10 *MB* que utilice el algoritmo de *Hash SHA 512* y el algoritmo de cifrado *AES*. https://www.veracrypt.fr/en/Downloads.html
18. Montar el volumen cifrado.
19. Almacenar el archivo *prueba1.txt* del ejercicio 13 dentro del volumen.
20. Desmontar el volumen, volver a montarlo y verificar si los archivos se encuentren intactos.

ALMACENAMIENTO DE CONTRASEÑAS

21. Usar *KeePassXC* para crear una base de datos de contraseñas. https://keepassxc.org/download/#windows
22. Almacenar credenciales con los siguientes datos:
    a. Usuario: *Prueba1*.
    b. Contraseña: "*AlgoSuperSeguro.7823*"
23. Cerrar *KeePassXC y v*olver a abrir.
24. Verificar si la contraseña que se ha almacenado esté presente en la base.

GITHUB

1. Publicar la documentación en un *readme* de su repositorio personal.

Es importante que se trabaje el *readme* del repositorio (incluso pueden agregar un *readme* por carpeta con más información para probar cada parte de este).

El objetivo es que una persona pueda visualizar su repositorio y testear (es decir, probar todo en conjunto y también cada una de las partes por separado).

MODALIDAD DE TRABAJO

En el archivo, documentar lo siguiente:

- Comandos.
- Capturas de pantalla que respaldan la documentación.
- Problemas que se presentaron, pasos a seguir para encontrar la solución, etc.

Además, el documento debe tener una portada, datos personales y titulo del desafío.

ENTREGABLE

Los documentos son almacenados en la carpeta compartida que tienen en *Google Drive* con el formato:

<carpeta con su nombre>/<Fase>/<desafío>/archivo.

Por ejemplo, el instructivo se debe almacenar en la carpeta compartida con el nombre del alumno, en una carpeta llamada Fase 4, dentro debe tener otra carpeta llamada Desafío 16 y, por último, almacenar dentro de ella todos los archivos relevantes a este desafío.

Se esperan los siguientes archivos:

- Instructivo.
- Enlace del repositorio de código donde publican los archivos creados (dentro del instructivo).
- Archivos adicionales.

Recuerden seguir las instrucciones para los entregables.

CONSEJOS

- Crear una VM para poder realizar las pruebas y así, aislar las configuraciones de seguridad necesarias.