**Desafío 16**

Nombre: Matias O. Riedel

1. **Modificación User Account Control:**

Para el primer paso procederemos a configurar el User Account Control, para eso nos vamos a dirigir a nuestro servidor de Windows Server y abriremos nuestro Panel de Control:

Podemos buscarlo como “Control” en el inicio de nuestro sistema:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

O como otra opción podemos abrir un ejecutar con la combinación de teclas “Windows + R” lo que nos abrirá un ejecutar donde colocaremos lo siguiente:

Interfaz de usuario gráfica

Descripción generada automáticamente

Luego de estar en nuestro apartado de nuestro panel de control

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Procedemos a buscar Sistema y Seguridad

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Nos vamos al apartado de Seguridad y Mantenimiento:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y aca procedemos a elegir la siguiente opción:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Donde inicialmente tendremos nuestro control de actividad habilitado de la siguiente manera, y que pocredemos a cambiar en este momento:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y procedemos a dejarlo de la siguiente manera:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Guardamos los cambios en OK y listo tendremos deshabilitado nuestro control de cuentas de usuario en nuestro Sistema Operativo Windows Server.

1. **Habilitar Acceso Escritorio Remoto (Remote Desktop)**

Para este paso procederemos a ir a nuestro explorador de archivos de nuestro Windows Server

Seleccionamos “Este Equipo / This PC”

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Donde le daremos click derecho con el mouse y nos iremos a propiedades:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Una vez que nuestro sistema nos abra el apartado de propiedades de nuestro sistema operativo nos apareceré lo siguiente:  
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde procederemos a irnos al apartado de Remote Desktop:  
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde tendremos para habilitar la opción de remote desktop de nuestro servidor:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

(El mismo en figura activo ya que se usó como prueba un servidor en Windows server 2022 de terminal server que uso actualmente como remoto para trabajar).

Luego de habilitar nuestro permiso ya podremos ingresar a nuestro servidor por medio de la ip privada de nuestro servidor y el puerto default 3389 de escritorio remoto de Windows.

1. **Crear cuenta de usuario “bonustrack”**

Ahora bien habilitado nuestro servicio de escritorio remoto procedemos a crear nuestra cuenta de usuario con la que accederemos al mismo, para eso nos vamos a ir al inicio de nuestro sistema, y buscaremos “herramientas administrativas de Windows / Windows administrative tools ”

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

Abriremos nuestro administrador de equipo:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nos aparecerá la siguiente ventana:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Donde nos iremos al siguiente apartado para crear nuestro usuario solicitado

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Procedemos a dar click derecho en nuestra lista de usuarios donde nos aparecerá la opción para crear usuario nuevo:

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Donde nos aparecerá la siguiente ventana donde colocaremos los datos de nuestro usuarios a crear:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Colocaremos nuestro nombre de usuario y una clave “con norma de seguridad de almenos 10 caracteres Alfanumérica ” para el mismo que al usuario en cuestión se le solicitara cambiar al momento de iniciarlo.   
Una vez creado nuestro usuario nos aparecerá en nuestra lista de usuarios:

Tabla

Descripción generada automáticamente

Donde procederemos a ingresar a las propiedades del usuario y darle permisos de acceso remoto al mismo

Para eso le damos click derecho a nuestro usuario creado y nos dirigiremos al apartado de propiedades del usuario

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Donde iremos a la pestaña:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde tendremos la posibilidad de agregar el grupo de permisos que necesitamos para este usuario en particular

Donde al mismo tendrá que tener asignado los grupos de permisos de “Usuarios / Users” y de “Usuarios de Escritorio Remoto / Remote Desktop Users”

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

1. **Directivas de Seguridad:**

Para este paso procederemos a ir a nuestro ejecutar con “Windows + R” donde colocaremos lo siguiente “gpedit.msc” donde editaremos las políticas de seguridad de nuestro sistema

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Nos abrirá la siguiente ventana donde procederemos a ir a la siguiente ruta:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ruta: Computer Configuration/Windows Settings/Security Settings/Account Policy/Password Policy. Donde nos aparecerá lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y procederemos a editar la política que dice:

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Abriremos las propiedades de nuestra política de claves y nos aparecerá lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Donde el valor en “0” lo cambiaremos por “10” lo que llevara a que nuestros usuarios tengan un requisito mínimo de 10 caracteres para las claves de acceso  
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Guardamos los cambios y los mismos quedaran aplicados.

Ahora cambiaremos la duración máxima de nuestras claves a “0” para que las mismas no tengan vencimiento:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde procederemos a modificar las propiedades de la misma y colocar en “0”

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ahora una vez guardados los cambios procedemos a modificar el mínimo de historia de claves que se puedan utilizar para eso procedemos a modificar el siguiente valor:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde setearemos nuestro parámetro en “10” para que las ultimas 10 claves del usuario no puedan ser reutilizadas.

Ahora procedemos a modificar los valores de intentos fallidos de intentos de sesión para los usuarios, para eso nos iremos a la siguiente ruta a modificar el valor de nuestra política en hasta 7 intentos fallidos:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y modificamos el parámetro de nuestra política:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Lo dejamos en “7 ” intentos fallidos  
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Guardamos cambios y queda nuestra política modificada

Editaremos tambien nuestra política de “Account lockout duration” para que la misma pueda ser desbloqueada luego de 10 minutos para eso modificaremos la siguiente política  
Tabla

Descripción generada automáticamente

Donde la editaremos y colocaremos el parámetro en “10 Minutos” guardaremos los cambios para que sean aplicados y listo. Tendremos terminada nuestra policita de seguridad para nuestros usuarios.

1. **Windows Defender:**

Para este paso procederemos a descargar el archivo solicitado, donde podremos observar en mi caso Analizado por Kaspersky Antivirus, automáticamente el archivo es eliminado del sistema una vez descargado

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Luego de verificar esto mismo procederemos a analizar el archivo con Virus Total:

Nos vamos a nuestro navegador de internet y nos vamos a la pagina de virustotal:

https://www.virustotal.com/gui/home/upload

Captura de pantalla de un celular

Descripción generada automáticamente

Donde procedemos a subir el archivo descargado anteriormente:  
Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Seleccionamos nuestro archivo descargado

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Y el mismo nos dará un reporte y un análisis del archivo:

Captura de pantalla de computadora

Descripción generada automáticamente

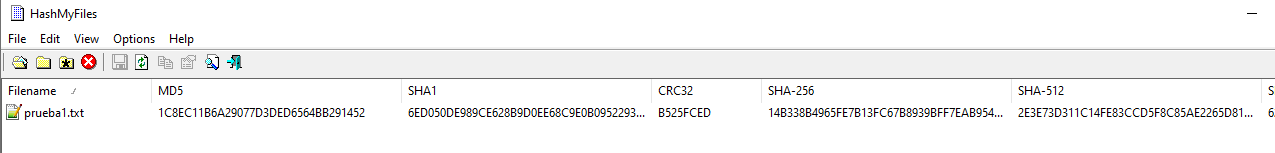
1. **Hashes**

Para esto procederemos a crear en una carpeta un archivo de texto que se llamara “prueba1.txt” y le agregaremos dentro del archivo solo el dato “EducacionIT”

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Descargaremos la herramienta con la que trabajaremos en esta ocasión que es HashMyFiles:



Y procedemos a crear un 2do archivo prueba2.txt donde colocaremos internamente EducacionIT1 y lo colocaremos en nuestro Hash para analizar los mismos

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde podremos observar que tenemos diferencia de hash entre los mismos.

1. **VeraCrypt**

Para este paso procederemos a crear un volumen de 10mb cifrado con Sha 512 y AES, nos iremos a nuestro veracrypt

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Donde iremos a crear un nuevo volumen de datos encryptado

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Donde crearemos un disco virtual encryptado

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Especificamos el tipo de disco que crearemos  
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Especificamos que sea multiboot para que pueda ser visualizado en diferentes sistemas operativos

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y Seleccionamos nuestros algoritmos de encryptacion para el mismo

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Crearemos una clave de acceso al mismo:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y le damos a siguiente donde el mismo se terminará de crear:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Una vez finalizado la creación procedemos a seleccionar el volumen de nuestro disco encryptado

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Donde como punto final tendremos un archivo como el siguiente:



Procedemos a montarlo en nuestro VeraCrypt, donde seleccionamos nuestro archivo generado:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y le damos a mount donde el mismo se va a montar para poder acceder al mismo:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

El mismo será accesible por medio de nuestro explorador de Archivos:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. **Almacenamiento de Credenciales**

Para esto procederemos a descargar una aplicación que se llama Keepass la que nos permitirá crear una Base de datos Cifrada para administrar nuestras credenciales:  
Luego de tener nuestro programa instalado procederemos a crear una base de datos nueva (El mismo no nos permitirá sacar screens a nuestro keepass, asi que se explicara paso a paso):  
  
Abriremos nuestro keepass:

* Crearemos una nueva base de datos donde le especificaremos (Nombre de Base de Datos)
* Especificaremos el Formato de la Base de datos en este caso será de (KDBX4) Y el tiempo de cifrado en nuestro estándar básico o en avanzado especificando nuestro algoritmo preferido de cifrado
* Crearemos nuestra clave de acceso a la base de datos que sea una única clave para acceder a la misma.

DBPass: “fvvHbHINBN+n80Qq9QdP3iKNFGJmB6fnBFhm+DmxtAVcIFujmhCMaXZLImlzSx+kHhkLzlnCWhlp7rB3Zei7Rg” - https://cifraronline.com/descifrar-aes

* Luego de crear nuestra base de datos podremos empezar a resguardar nuestros registros de claves.

Para este caso crearemos un registro de usuario y clave donde verificaremos que el mismo registro se mantenga una vez cerrada la sesión de nuestra base de datos.

El registro a ingresar es el siguiente:

Usuario: prueba1 – AlgoSuperSeguro.7823