Taller HackMe

1. Primero reseteamos la maquina vitual para llegar al menú de grub y apretamos el botón e para editar los parámetros de inicioInterfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
2. En esta pantalla vamos a la línea que empieza con “linux16” y al final escribimos rb.breakInterfaz de usuario gráfica, Texto

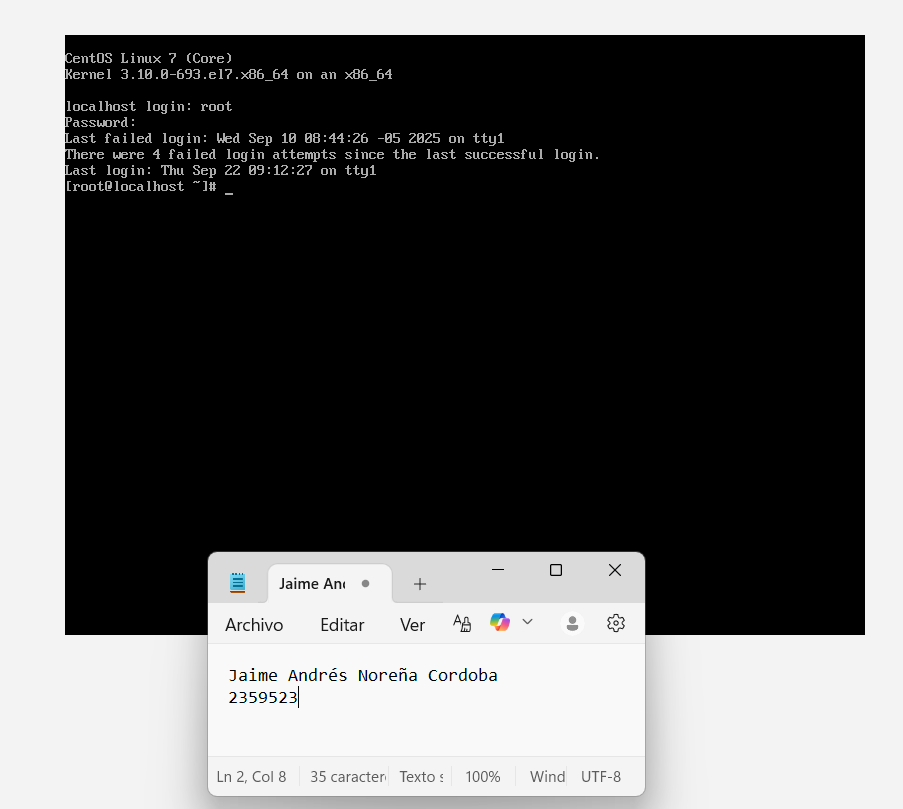
   El contenido generado por IA puede ser incorrecto.
3. Presionamos ctrl+x para ejecutar y esto nos debería llevar a una consola de recuperacionInterfaz de usuario gráfica, Texto, Aplicación

   El contenido generado por IA puede ser incorrecto.
4. Montamos la partición en modo read write con mountInterfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
5. Ahora entramos al directorio sysroot con el comando chroot /sysrootInterfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
6. Cambiamos la contraseña con passwd Interfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
7. Ahora escribimos touch /.autorelabel para que sistema acepte las modificación que se hicieron cuando reiniciemos. Interfaz de usuario gráfica, Texto

   El contenido generado por IA puede ser incorrecto.
8. Salimos de la consola con exit y luego reiniciamos con reboot. Y nos logeamos con las nuevas credenciales

Laboratio Proteccion grub

1. Vamos a la carpeta boor/grub para vericar que existe el archivo usr.cfgInterfaz de usuario gráfica, Texto, Aplicación

   El contenido generado por IA puede ser incorrecto.
2. Usamos grub2-setpassword

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

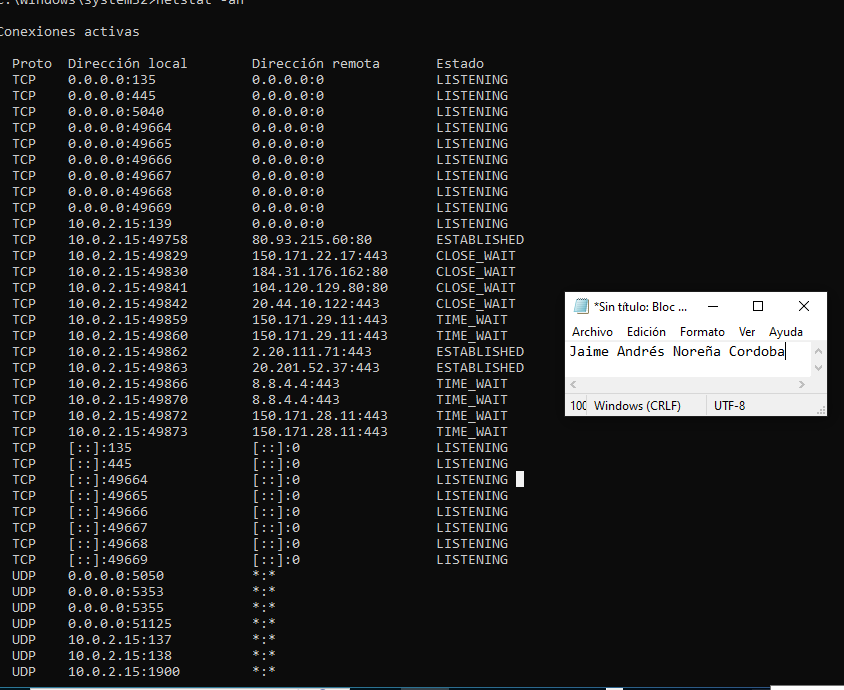
1. Cambiamos la contraseña del rootTexto

   El contenido generado por IA puede ser incorrecto.
2. Reiniciamos

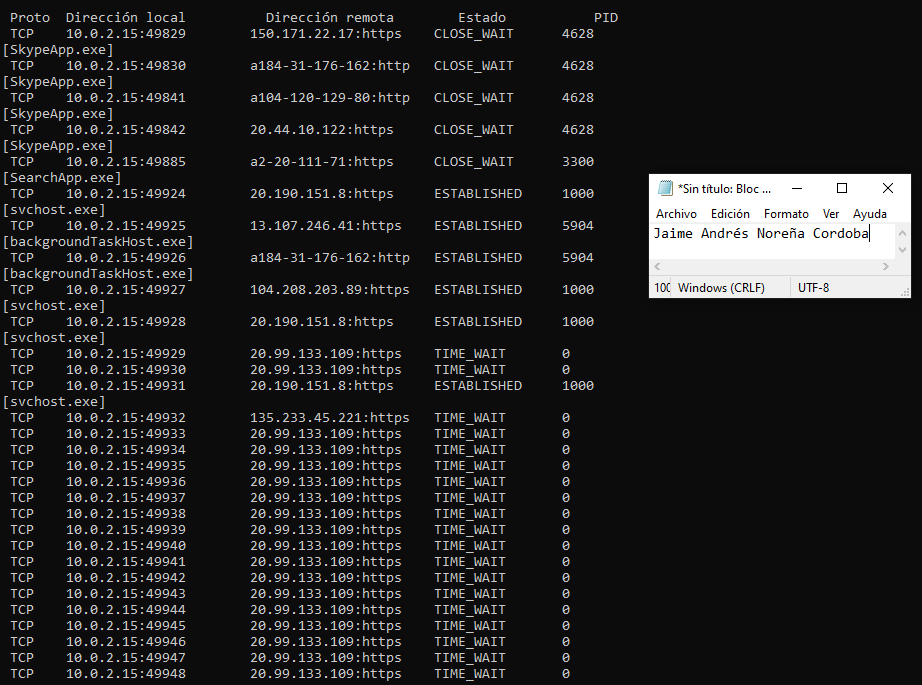
Laboratorio 3

Netstat

Vemos puertos abiertos con: netstat -an



Vemos aplicaciones con conexiones: nestat -bo

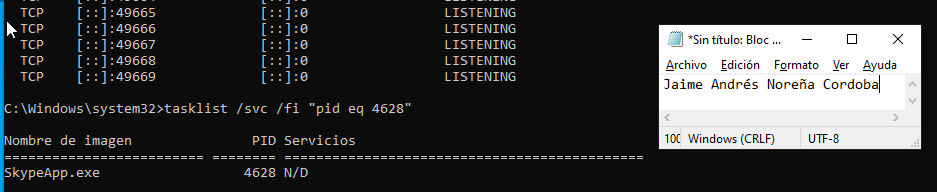


Ver los puertos abiertos: netstat -an |FINDSTR /C:LISTENING

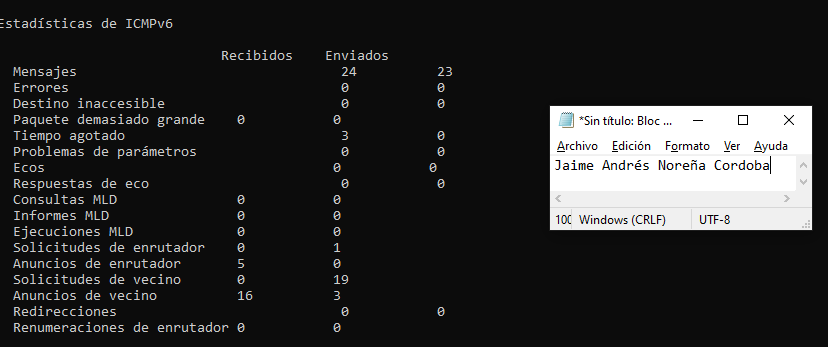
Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Aplicación que inicia un proceso: tasklist /svc /fi “pid eq 3912”



IPv6?

netstat -s -p icmpv6 

Puertos abiertos, conecciones activas e ID de procesos

netstat -ano

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Matar procesos

Taskkill /f /im nombre\_proceso.exe



Informe de conecciones establecidas

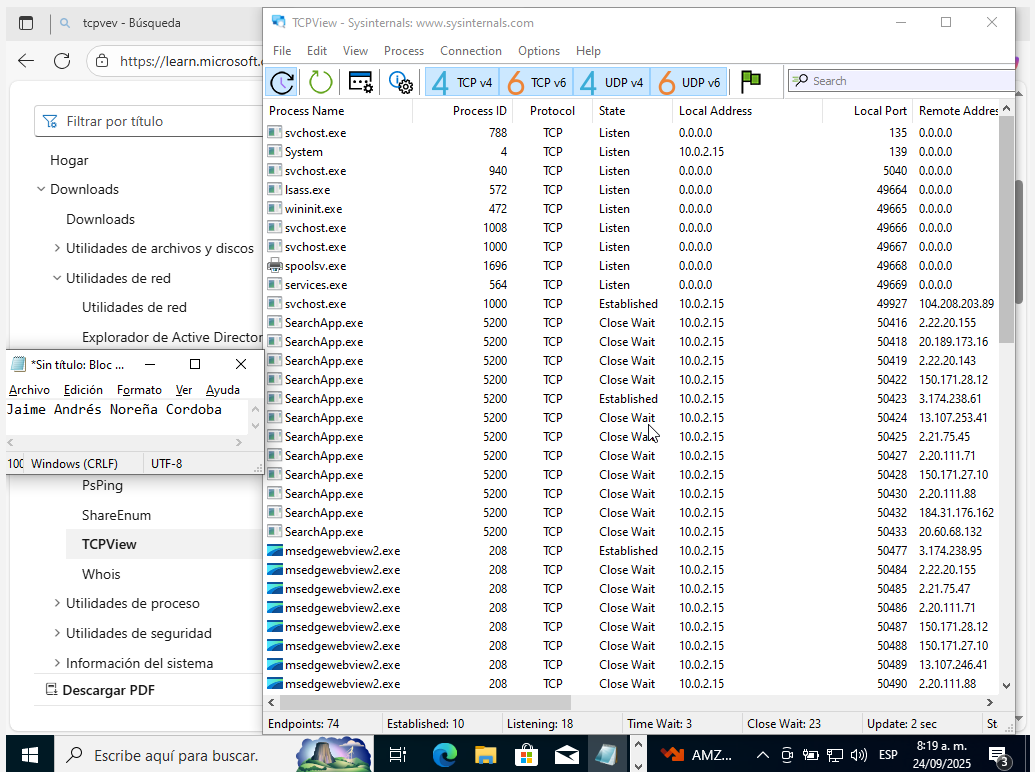
Netstat -ano -p tcp |findstr /c:ESTABLISHED>C:\conecciones.txt

Una captura de pantalla de una computadora

El contenido generado por IA puede ser incorrecto.

Laboratorio 4

TCPview



Laboratorio 5

WSUS offline

Descargamos e instalamos wsus offline

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Seleccionamos las opcionesque necesitemos

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

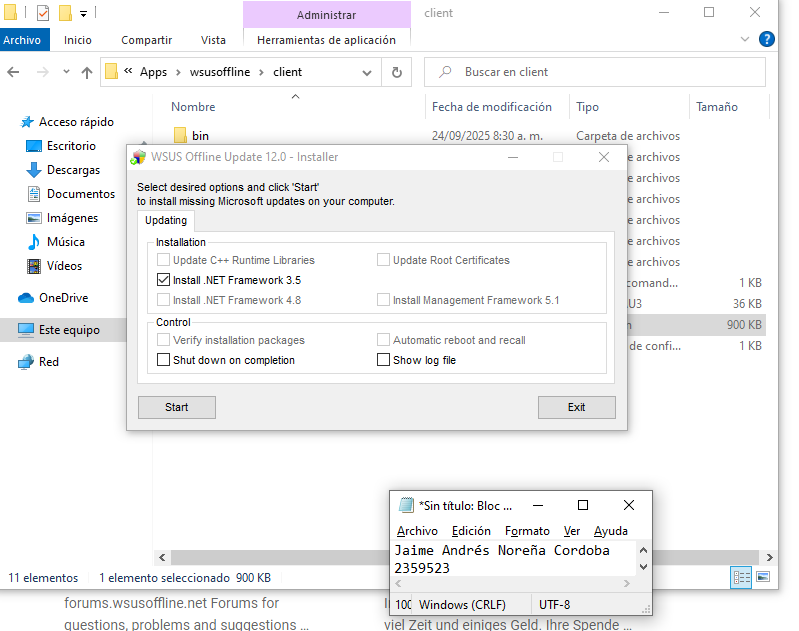
El contenido generado por IA puede ser incorrecto.

Esperamos a que descargue

Texto

El contenido generado por IA puede ser incorrecto.

Luego vamos a la carpeta client y ejecutamos updateIntaller



Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Laboratorio 6

Vamos a mirar las opciones del Windows update

Interfaz de usuario gráfica, Texto, Aplicación, Word

El contenido generado por IA puede ser incorrecto.

Podemos ver que faltan actualizaciones importantes y tenemos varios apartados para explorar

Interfaz de usuario gráfica, Texto, Aplicación, Word

El contenido generado por IA puede ser incorrecto.

Vemos que tenemos unas cuantas opciones. Podemos ver el historial de actualizaciones, entrar a las opciones avanzadas y cambiar las horas activas.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Aquí podemos cambiar las horas en las cuales no se va reiniciar la maquina al hacer actualizaciones.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Aquí vemos el historial de actualizaciones

Interfaz de usuario gráfica, Texto, Aplicación

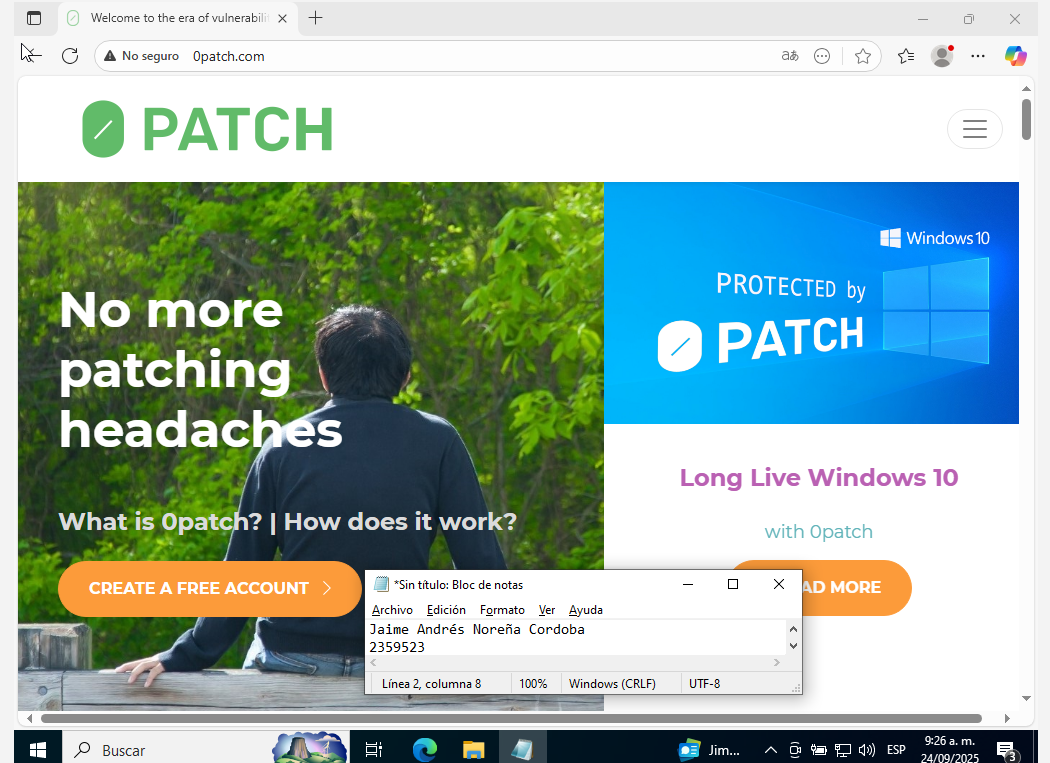
El contenido generado por IA puede ser incorrecto.

Aquí podemos ver el menú de opciones avanzadas donde podemos elegir si recibir actualizaciones de otros productos al actualizar Windows, que se puedan descargar actualizaciones desde datos y si se reiniciara el dispositivo inmediatamente después de la actualización y si se debe mostrar una notificación al mostrar una actualización

Laboratorio 7

0patch

0patch es una empresa que se dedica desarrollar pequeños parches para vulnerabilidades del tipo zeroday



Descarguemos el agente gratuito para ver como funciona

Interfaz de usuario gráfica, Texto, Aplicación

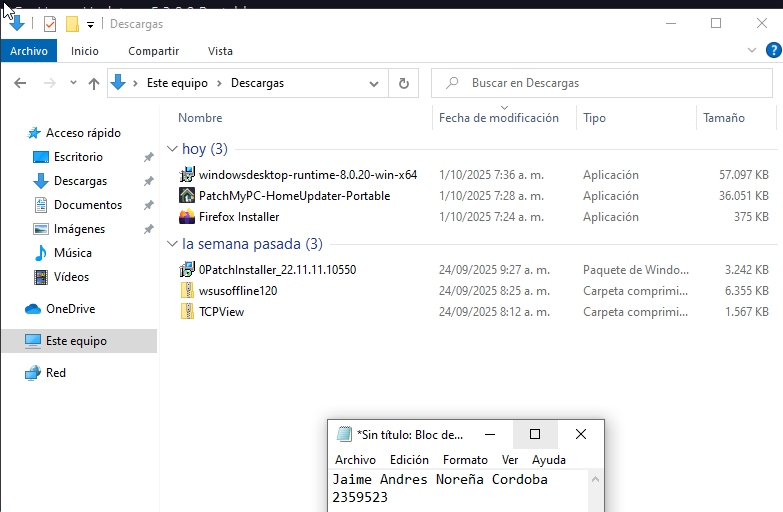
El contenido generado por IA puede ser incorrecto.

0path requiere una cuanta entonces nos logueamos y una vez logueados vemos el dashboard

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

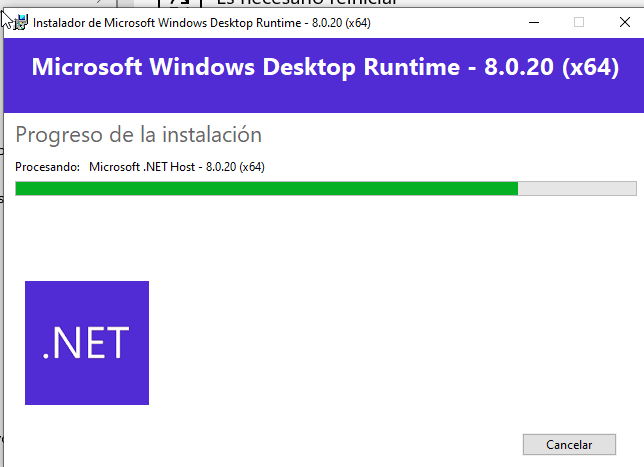
Aquí nos muestra los parches que hay disponibles para nuestro dispositivo en las aplicaciones especificas

x|

Laboratorio 8 patchmypc

Descargamos patchmypc

Instalamos una librería .NET requerida



Este es el menú principal del patchmypc

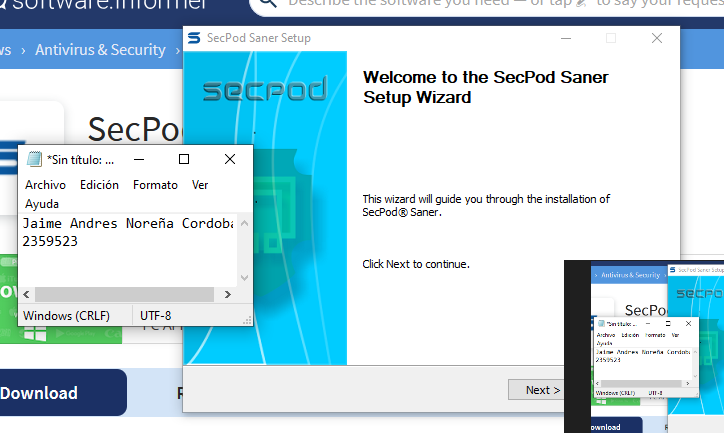
Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Donde podemos ver las aplicaciones intaladas y ver si están actualizadas

Laboratorio 9 Secpod

Instalamos secpod

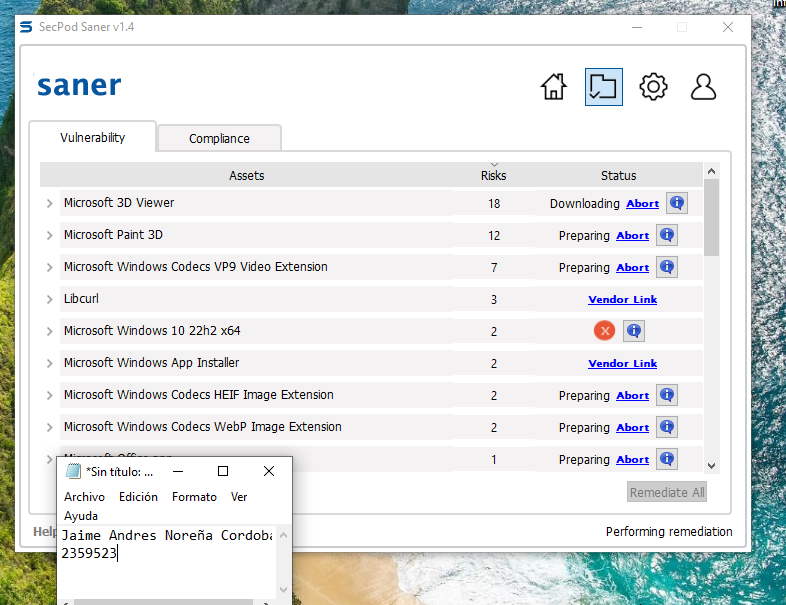


Iniciamos el escaneo

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

El contenido generado por IA puede ser incorrecto.

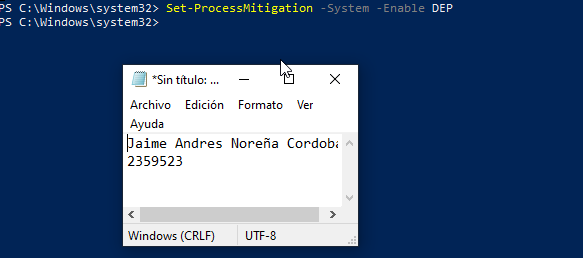
Despues del escaneo vemos que hay fixes que se pueden aplicar.





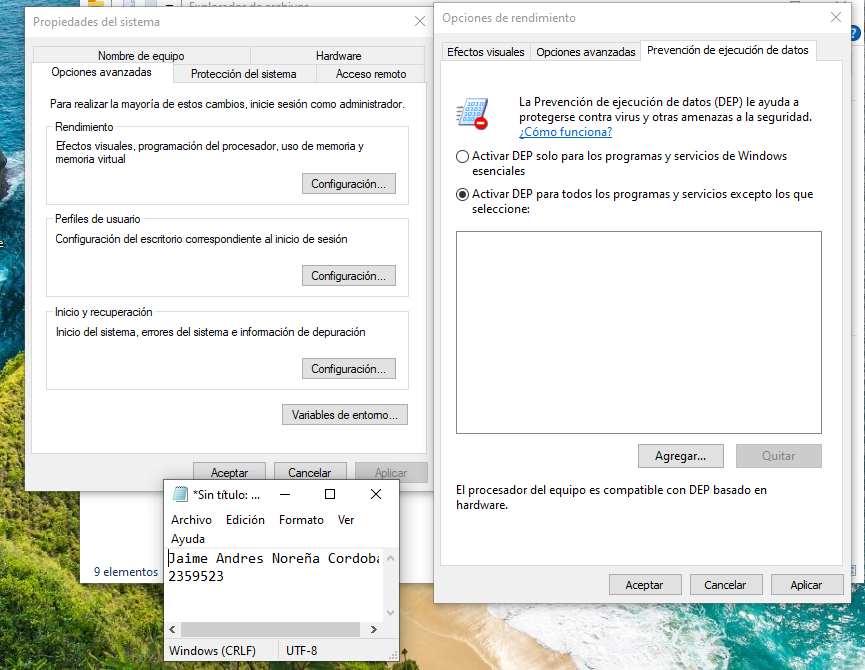
Laboratorio 10 DEP

Utilizamos para mitigar la ejecución de código malicioso



Laboratorio 11 DEP grafico

Tambien existe una manera grafica de activar DEP y de hacer excepciones ya que esta herramienta puede interferir con la ejecución de algunas aplicaciones que no son maliciosas



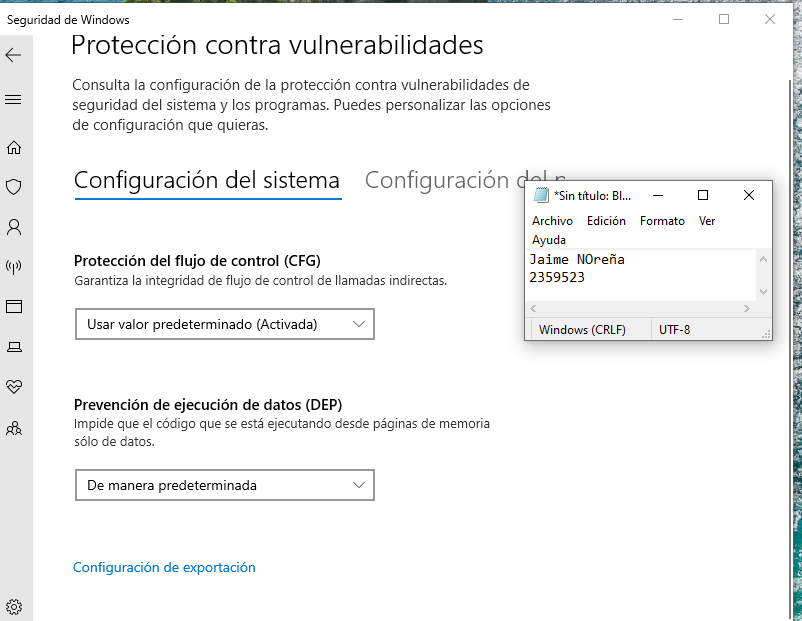
En esta pestaña podemos elegir que aplicación excluir

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

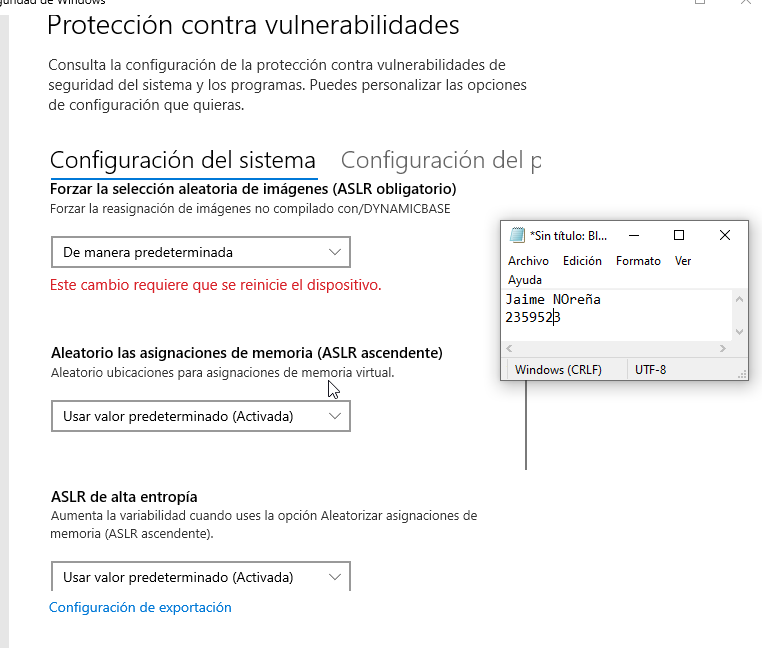
El contenido generado por IA puede ser incorrecto.

Laboratorio 12 ASLR

Esta herramienta sirve para mitigar ataques de desbordamiento y ejecución de programas en direcciones de confianza

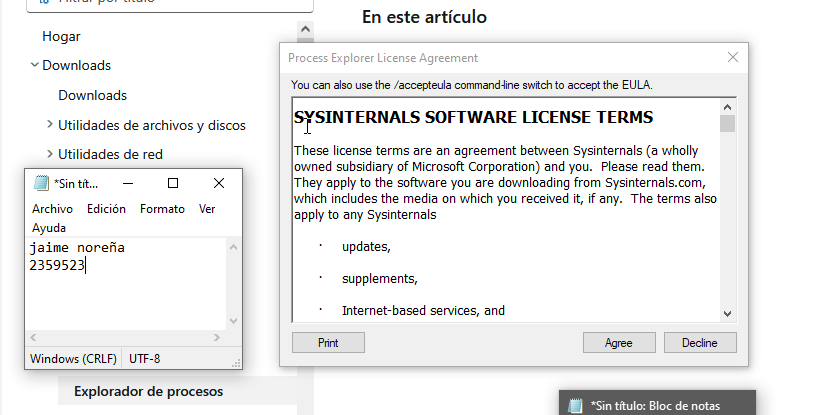


Activamos las opciones y listo



Laboratorio 13

Process explorer es una herramienta parecida administrador de tareas

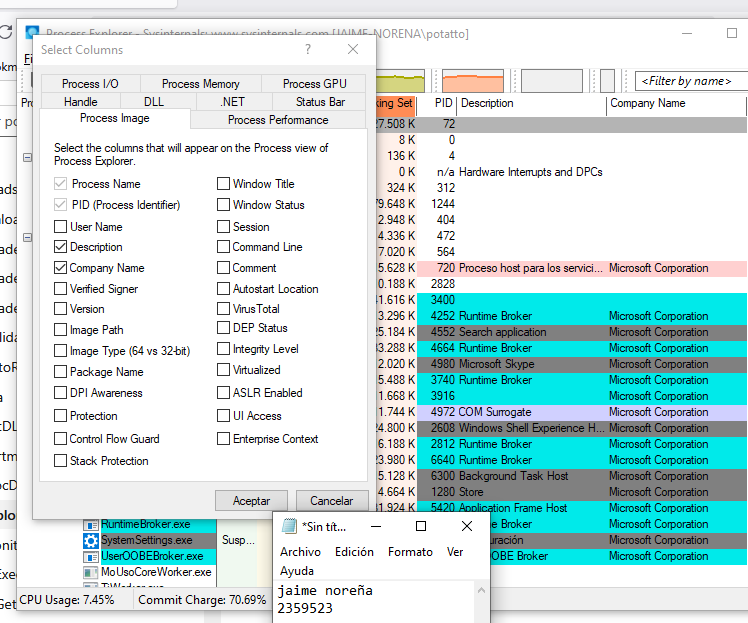


Asi se ve el programa

Interfaz de usuario gráfica, Aplicación, Tabla, Excel

El contenido generado por IA puede ser incorrecto.

Vamos a view seleccionar columna y seleccionamos virus total}



Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Ahora checkeamos la opción de virus total en opciones y ahora tenemos una nueva columna que analiza los procesos

