

PRACTICA 2. Vigilancia de PC's no custodiados con Salus (Por HxC Mods-Adm)

Salus, es un programa que se ejecuta en segundo plano, como servicio o *background*, que registra todo lo que ocurre en un PC sin que el usuario se percate de ello, es como vigilar el ordenador con una cámara de seguridad y luego ver la cinta de lo que ha ocurrido, *Salus* permite registrar información de:

- Hora de arranque y terminación de la sesión, junto con el usuario que la inicia
- Aplicaciones y documentos usados
- Conexión y Desconexión a Internet
- Direcciones Web visitadas
- Caracteres, palabras y textos tecleados
- Datos copiados, pegados o cortados de aplicaciones al portapapeles

Todo ello se muestra en una secuencia temporal y continua, con lo cual podemos hacernos una idea bastante fiable de lo que un usuario a realizado.

Lo primero que debemos realizar una vez instalado el programa es verificar la casilla *Start at Windows Start up (iniciar salus al arrancar Windows)* y elegir el idioma, existe un módulo en Español.

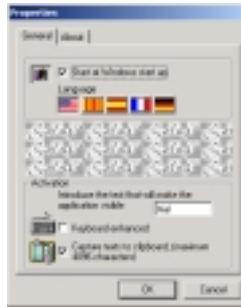
También es muy importante elegir la *palabra de activación*, si no se indica lo contrario, *Salus* establece la palabra *trial*, como clave de activación, eso quiere decir que cuando el usuario escriba esa palabra, *Salus* mostrará los informes obtenidos, como es obvio, hay que cambiar dicha palabra, la sabe todo el mundo y además si en un documento quisiéramos escribir esa palabra iniciaríamos el informe de *Salus*, por tanto elegiremos otra, que no exista en el diccionario y que no pueda ser escrita casualmente, por ejemplo:

kelisto

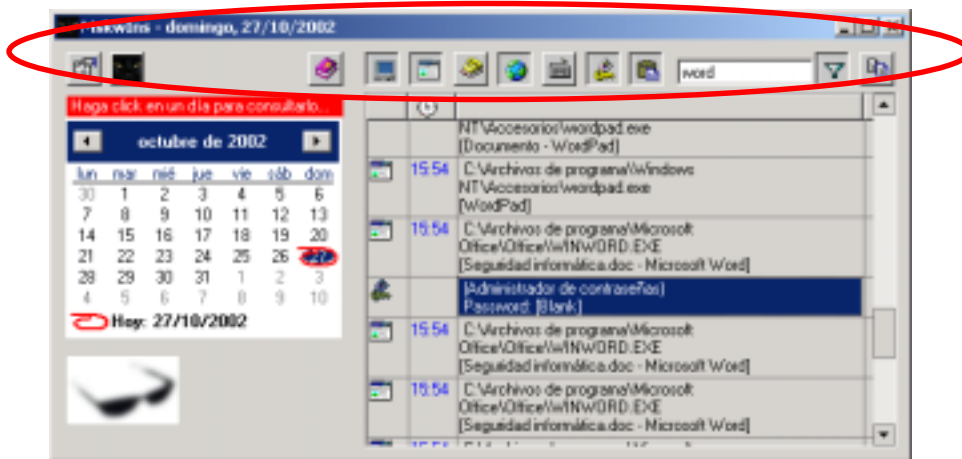
Foro de HackXcrack

La casilla de verificación **Keyboard enhanced**, además permite utilizar otros símbolos junto con los caracteres alfanuméricos.

Por último, indicaremos a **Salus** cual es la longitud máxima de los textos que se cortan o pegan al portapapeles, por defecto 4Kb.



Una vez confirmada la contraseña, tras escribir la clave secreta (*kelisto*), veremos una pantalla como la que sigue con el registro de actividades detectadas por **Salus**.



Podemos observar los informes de cada actividad pulsando sobre los **iconos de la parte superior** y en la tabla de abajo se mostrarán, horas, usuarios y actividad descrita.

Si se combinan las representaciones proporcionadas en **Claves de Acceso** (la llave amarilla) y las de Texto escrito, puedes averiguar la contraseña del usuario o vigilar que nadie conoce la tuya.

Por último, el icono que parece un altavoz hacia arriba, permite buscar las palabras escritas en la casilla de texto que hay a su izquierda, en el ejemplo la palabra Word, para saber cuando se inició Wordpad o MsWord.

Para desactivar **Salus** hay que seguir un procedimiento determinado:

- 1º) Llame al programa Salus introduciendo la clave secreta (en nuestro caso: *kelisto*)
- 2º) Clic en el botón de propiedades (arriba a la izquierda, la mano y el papel)
- 3º) Desactivar la casilla de arrancar al iniciar Windows y Aceptar
- 4º) Cierra la ventana o alt+F4
- 5º) Responder afirmativamente a las dos preguntas que se realizan, dice algo así como que el programa dejará de capturar información y pide confirmación