

PRÁCTICA 4. CREAR UN BANCO DE PRUEBAS. (Por HxC Mods-Adm)

Hemos hablado de *eSafe*, a estas alturas ya lo deberías tener instalado en tu PC, ahora vamos a configurar el módulo *sandbox*, la traducción literal sería *caja de arena*, esto es, un banco de pruebas para que las aplicaciones que se instalen en tu PC las puedas seguir paso a paso durante su ejecución y así conocer las zonas de disco que acceden, si efectúan o no conexiones a Internet, abren puertos, etc. Todo ello dentro de un “cajón” del que no puedan salir de forma que podemos anticiparnos a los posibles daños antes de que estos se produzcan.

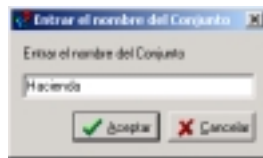
El módulo *sandbox* puede proteger los diferentes componentes software y hardware de tu PC, los más importantes deberían ser los discos duros y sistemas de archivos, nuestro *cajón de arena* puede ser configurado de tal forma que permita al nuevo programa el acceso a directorios muy concretos, como mínimo debe estar permitido la lectura y ejecución del propio directorio de la aplicación, para la primera prueba se debería desactivar los permisos de escritura y eliminación, son especialmente críticas las aplicaciones con vínculos *on-line* y acceso a módems, adaptadores RDSI, tarjetas de red, etc., de ellos pueden abusar los troyanos para transmitir datos confidenciales e incluso modificar los números de marcado telefónico y efectuar llamadas a números de pago 906, o al extranjero. También debemos prestar especial atención a los accesos a los archivos del registro.

Para usar *eSafe* como *sandbox* podemos utilizar las reglas predefinidas o crear un conjunto de reglas especiales para la nueva aplicación, las reglas predefinidas son:

- **Blank:** Conjunto de reglas vacío que sólo protege al propio eSafe.
- **Freeze Desktop:** Bloquea el escritorio y el menú de inicio.
- **Internet Applications:** Protege de los peligros procedentes de Internet y *scripts* peligrosos
- **Internet Explorer:** Permite acceder a las áreas donde IE tenga algo que buscar e impide la creación de archivos *script* en todos los dispositivos.
- **NetScape:** Idem de IE pero para NetScape Navigator
- **Untrusted Applications:** Es el conjunto de reglas para aplicaciones sospechosas, restringe el acceso a esas aplicaciones a unos pocos directorios de prueba y descarga, así como a la carpeta temporal, también bloquea la creación de *scripts*.



Si lo que se desea es crear un conjunto de reglas personalizado, hay que seleccionar **Blank** y luego pulsar el botón **Salvar Como** para darle un nombre al nuevo conjunto de reglas, en el ejemplo vamos a crear un sencillo conjunto de reglas para el inofensivo programa que distribuye *Hacienda* para el cálculo del *IRPF*, para ello creamos un nuevo conjunto de reglas llamado **Hacienda**.



Ahora hay que escoger los discos, carpetas, etc., a proteger. Lo normal sería bloquear el acceso a todas las unidades de disco y directorios excepto el de la propia aplicación (en nuestro caso *C:\AEAT*, debería de quedar como sigue:



Aunque no se observe en la pantalla anterior, antes de permitir todas las actividades a la carpeta *AEAT* se negaron Todas las Actividades Permitidas sobre la unidad A: y Sólo se permite Leer y ejecutar en C:

En ocasiones resulta lógico autorizar más directorios, por ejemplo muchas aplicaciones necesitan escribir en el directorio Temporal de Windows, si hace falta podemos autorizar con permisos de escritura a ese directorio, por el momento no lo haremos, y así *eSafe* nos informará de aquellos accesos que precisa la aplicación.

Después de crear el conjunto de reglas, selecciona la Ficha **Activación** y activa el conjunto de reglas



Ahora, en la zona **de Áreas protegidas cuando**: define la aplicación a utilizar, para ello pulsa en el botón de **Añadir** (es el icono que parece un documento situado a la izquierda de la x en rojo, que por supuesto sirve para eliminar la aplicación del **sandbox**), busca el nombre de la aplicación en su carpeta y añádela, aparecerá algo así:



Vamos a la ficha **de Cómo reaccionar**, deberías **negar el acceso y parar** en todas sus opciones, esto sólo afectará a las infracciones cometidas, recuerda que el propio directorio de la aplicación tiene permitida todas las actividades. Se puede bloquear la aplicación silenciosamente, pero eso no nos daría la posibilidad de conocer los lugares no permitidos a los que accede nuestra aplicación.



Finalmente pulsa sobre **Salvar**, para almacenar el conjunto de reglas.

Cuando la aplicación se ejecute, en el caso de que viole alguna de las reglas establecidas, **eSafe** parará y preguntará qué debe hacer, dejándote elegir entre:

Permita hasta siguiente: Permite un acceso provisional hasta el próximo reinicio del ordenador, las reglas no se cambian, de manera que la próxima vez que se ejecute el programa volverá a preguntar.

Permita en el futuro: Autoriza el acceso ahora y para siempre, **eSafe** modifica las reglas de protección para que no le vuelva a preguntar nunca.

No permita: Impide totalmente el acceso, elige esta opción si tienes dudas, puede ocurrir que el programa no funcione pero tu máquina estará a salvo,

Foro de HackXcrack

Antes de realizar la prueba, esto es, ejecutar la aplicación, deberíamos decidir el modo de ejecución, entre **Automático o interactivo**, por regla general se debe ejecutar el modo automático, que es el que hay si no se modifica nada, para cambiar al modo interactivo, es preciso acceder al **panel de Administración** y **ficha administración de usuarios**, escoger el **usuario anónimo** y en la **categoría de Privilegios-eSafe Desktop-Opciones de Permisos**, verificar esta opción (hacer doble clic sobre ella) de forma que verás algo parecido a esto:



A partir de ahora cada vez que se produzca una violación de las reglas, se advertirá para que se tome una decisión. El hecho de haberlo realizado sobre el usuario anónimo es por que afectará a **TODOS** los usuarios registrados en **eSafe**.

Si se detectan accesos prohibidos o simplemente la aplicación no se ejecuta correctamente por que **eSafe** no lo permite, puedes y debes, ver los **Informes**, para ello desde el **panel de Administración**, pulsa sobre la **ficha Configurar Informe** y haz clic en el **Botón Ver Informe**, en nuestro ejemplo se verá lo siguiente:

Date	Time	User	Type	Report
2002-11-01	20:38	ADMINISTRADOR	Acceso	RET2002 EXE trató de Leer C:\WINNT\SYSTEM32\MSVBM60.DLL
2002-11-01	20:41	ADMINISTRADOR	Acceso	RET2002 EXE trató de Ejecutar C:\WINNT\SYSTEM32\FRESIZER21

Fíjate que puedes guardar, imprimir, borrar, ... el informe. Fíjate también que el usuario que provocó la violación de las reglas es el **Administrador**, que en mi caso estoy utilizando Windows 2000 Server, con plenos derechos y privilegios sobre todo el sistema, y sin embargo **eSafe** bloquea el acceso a esos archivos aunque los permisos **NTFS** de ellos son de control total.