protegemos su mundo digital

ESET File Security

Manual de instalación y documentación para el usuario

Contenidos

ESET File Security, Primera Edición
Fecha de publicación 13 de marzo de 2007

Capítulo 1:

Introducción

Estimado usuario, Ud. acaba de adquirir ESET File Security - probablemente el mejor sistema de seguridad ejecutable en los sistemas operativos Linux y BSD. Como descubrirá muy pronto, el sistema, que utiliza el motor de análisis de última tecnología ESET, posee una velocidad de búsqueda y tasa de detección de virus hasta el momento insuperables, y el uso de recursos es tan bajo que lo convierte en la elección ideal para cualquier servidor con SO Linux o BSD.

En el resto del capítulo analizaremos las características principales del sistema.

- Los algoritmos del motor de análisis del antivirus ESET proveen la mayor tasa de detección de virus y las búsquedas más veloces.
- ESET File Security está preparado para trabajar en unidades con un procesador o con procesadores múltiples.
- Incluye una heurística única y avanzada para la detección de gusanos y componentes de puerta trasera (*back-doors*) en Win32.
- Los archivos autoextraíbles no requieren el uso de programas externos.
- Para incrementar la velocidad y la eficiencia del sistema, su arquitectura se basa en un programa residente activo (*daemon*), donde se envían todos los pedidos de análisis.
- El sistema soporta la configuración selectiva para la identificación diferenciada del usuario o cliente/servidor.
- Se pueden configurar hasta seis niveles de registración de eventos (l*ogging*) para obtener información sobre la actividad del sistema y las infiltraciones.
- La instalación de ESET File Security no requiere bibliotecas ni programas externos excepto la biblioteca estándar de C (*LIBC*).
- El sistema puede configurarse para notificar a una persona determinada en caso de que se detecte una infiltración.

Para un funcionamiento eficiente, ESET File Security requiere tan solo 16MB de espacio en disco rígido y 32MB de memoria. Opera sin problemas con las versiones 2.2.x, 2.4.x y 2.6.x del núcleo (*kernel*) del SO Linux y también con las versiones 5.x y 6.x del núcleo (*kernel*) de FreeBSD.

Desde pequeños servidores de oficina hasta servidores para proveedores de servicios de Internet con miles de usuarios, el sistema proporciona el rendimiento y la escalabilidad que se esperan de una solución basada en UNIX y la inigualable seguridad de los productos marca ESET.

Capítulo 2:

Terminología y abreviaciones

A continuación exponemos brevemente los términos y abreviaciones utilizados en este documento. Recuerde que en este documento en formato PDF se reserva el uso de la letra negrita para los nombres de componentes del producto y, en este capítulo, para abreviaciones y términos nuevos. También tenga en cuenta que los términos y abreviaciones explicados en este capítulo aparecerán en cursiva en el resto del documento.

ESETS

ESET Security (Seguridad) es el acrónimo que abarca todos los productos de seguridad desarrollados por ESET, spol. s r.o. para los sistemas operativos Linux y BSD. También es el nombre (o parte del nombre) del paquete de programas que contiene los diversos productos.

RSR

Es la abreviación de "RedHat/Novell(SuSE) Ready". También soportamos la variante del producto llamada "RedHat Ready y Novell(SuSE) Ready". La diferencia con la versión "estándar" de Linux es que el paquete RSR reúne criterios definidos por el documento *FHS* (Estándar de Jerarquía de Sistema de Ficheros definido como parte de la Base Estándar para Linux) requerido por la certificación RedHat Ready y Novell(SuSE) Ready. Esto significa que el paquete RSR, por ejemplo, se instala como una aplicación suplementaria, es decir, el directorio principal de instalación es '/opt/eset/esets'.

Daemon de ESETS (programa residente)

Es el sistema principal de control y análisis residente de *ESETS*: **esets_daemon.**

Directorio base de ESETS

Es el directorio donde se guardan los módulos ejecutables de *ESETS* que contienen, por ejemplo, bases de datos con firmas de virus. En este documento utilizaremos la abreviación **@BASEDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /var/lib/esets
Linux RSR: /var/opt/eset/esets/lib
BSD: /var/lib/esets
```

Directorio de configuración de ESETS

Es un directorio donde se guardan todos los archivos relacionados con la configuración de ESET File Security. En este documento utilizaremos la abreviación **@ETCDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /etc/esets
Linux RSR: /etc/opt/eset/esets
BSD: /usr/local/etc/esets
```

Archivo de configuración de ESETS

Es el archivo de configuración principal de ESET File Security. La ruta absoluta del archivo es la siguiente:

```
@ETCDIR@/esets.cfg
```

Directorio de archivos binarios de ESETS

Es el directorio donde se guardan los archivos binarios relevantes de ESET File Security. En este documento utilizaremos la abreviación **@BINDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/bin
Linux RSR: /opt/eset/esets/bin
BSD: /usr/local/bin
```

Directorio de archivos binarios del sistema de ESETS

Es el directorio donde se guardan los archivos binarios del sistema relevantes de ESET File Security. En este documento utilizaremos la abreviación **@SBINDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/sbin
Linux RSR: /opt/eset/esets/sbin
BSD: /usr/local/sbin
```

Directorio de archivos con códigos objeto de ESETS

Es el directorio donde se guardan los archivos con códigos objeto y bibliotecas relevantes de ESET File Security. En este documento utilizaremos la abreviación **@LIBDIR@** para referirnos a dicho directorio. La ubicación del directorio es la siguiente:

```
Linux: /usr/lib/esets
Linux RSR: /opt/eset/esets/lib
BSD: /usr/local/lib/esets
```

Capítulo 3:

Instalación

Este producto se distribuye como un archivo binario:

```
esets.i386.ext.bin
```

donde 'ext' es un sufijo dependiente de la distribución del SO Linux/BSD, es decir, 'deb' para Debian, 'rpm' para RedHat y SuSE, 'tgz' para otras distribuciones del SO Linux, 'fbs5.tgz' para distribuciones de FreeBSD 5.xx y 'fbs6.tgz' de FreeBSD 6.xx respectivamente.

Tenga en cuenta que el formato de archivo binario para Linux *RSR* es:

```
esets-rsr.i386.rpm.bin
```

Para instalar o actualizar el producto, utilice el comando:

```
sh ./esets.i386.ext.bin
```

En la variante del producto para Linux *RSR*, utilice el comando:

```
sh ./esets-rsr.i386.rpm.bin
```

Como respuesta, aparecerá el Contrato de Licencia del producto para la aceptación por parte del usuario. Una vez confirmado el Contrato de Licencia, el paquete de instalación se ubica en el directorio activo actual y se imprime información relevante sobre el paquete de instalación, desinstalación o actualización en la terminal.

Una vez que el paquete está instalado y el servicio principal de *ESETS* está en funcionamiento, en el SO Linux se puede observar su desempeño usando el comando:

```
ps -C esets_daemon
```

En caso de que el SO sea BSD, se usa un comando similar:

```
ps -ax esets_daemon | grep esets_daemon
```

Como respuesta, verá el siguiente mensaje (o uno similar):

```
PID TTY          TIME CMD
2226 ?        00:00:00 esets_daemon
2229 ?        00:00:00 esets_daemon
```

donde al menos dos procesos *daemon* de *ESETS* deben estar activos en segundo plano. Uno de dichos procesos es el gestor de procesos y de hilos de ejecución del sistema. El otro constituye el proceso de análisis de *ESETS*.

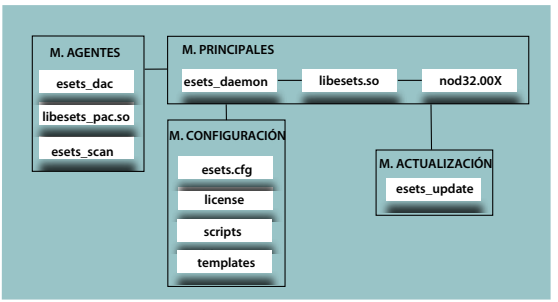
Capítulo 4:

Estructura del producto

Una vez que el paquete del producto se ha instalado exitosamente, llega el momento de familiarizarse con su contenido.

La estructura de ESET File Security se muestra en la imagen 4-1. El sistema está formado por los siguientes componentes.

Imagen 4-1. Estructura de ESET File Security



MÓDULOS PRINCIPALES

La parte principal de ESET File Security consiste en el *daemon* de *ESETS* **esets_daemon.** El *daemon* utiliza la biblioteca de interfaz de programas de aplicación (*API*) **libesets.so** y los módulos ejecutables nod32.00X de *ESETS* para realizar las tareas básicas del sistema: análisis, mantenimiento de los procesos agentes *daemon*, mantenimiento del sistema de envío de muestras, registros, notificación, etc. Por favor, consulte la página del manual esets_daemon(8) para más detalles.

MÓDULOS AGENTES

El propósito de los módulos agentes de *ESETS* es integrar a *ESETS* con el entorno del servidor Linux/BSD. En este manual encontrará un capítulo especial dedicado al tema.

MÓDULOS DE ACTUALIZACIÓN

La utilidad de actualización es una parte importante del sistema. Fue desarrollada para actualizar los módulos ejecutables de *ESETS* que contienen, por ejemplo, bases de datos con firmas de virus, soporte de ficheros, soporte de heurística avanzada, etc. En este documento encontrará un capítulo especial dedicado al tema.

MÓDULOS DE CONFIGURACIÓN

La correcta configuración es la condición principal para el buen funcionamiento del sistema. Es por eso que en el resto de este capítulo describiremos todos los componentes relacionados a la configuración. También recomendamos la página del manual esets.cfg(5), una fuente de información esencial sobre la configuración de *ESETS*. Una vez que el producto se encuentra correctamente instalado, todos sus componentes para la configuración se guardan en el *directorio de configuración* de *ESETS*. El directorio está formado por los siguientes archivos:

***@ETCDIR@*/esets.cfg**

Éste es el archivo de configuración más importante ya que preserva la mayor parte del funcionamiento del producto. Luego de explorar el archivo, notará que está creado por varios parámetros distribuidos dentro de secciones. Los nombres de las secciones aparecen entre corchetes.

En el *archivo de configuración* de *ESETS* siempre hay una sección global y varias secciones agentes. Los parámetros en la sección global se usan para definir las opciones de configuración del *daemon* de *ESETS* así como los valores predeterminados de las opciones de configuración del motor de análisis de *ESETS*. Los parámetros de las secciones agentes se utilizan para definir las opciones de configuración de los agentes, es decir, módulos usados para interceptar diversos tipos de flujo de datos en la computadora y/o su entorno y preparar dichos datos para su análisis. Recuerde que, además del número de parámetros usados para la configuración del sistema, también existe una serie de reglas que determinan la organización del archivo. Para familiarizarse con esta información, consulte las páginas del manual esets.cfg(5), esets_daemon(8) así como otras páginas sobre agentes relevantes.

***@ETCDIR*@/certs**

Este directorio se utiliza para guardar los certificados usados por la Interfaz WWW de *ESETS* para la autenticación (ver la página esets_wwwi(8) para más detalles).

***@ETCDIR*@/license**

Este directorio se utiliza para guardar la/s clave/s de licencia que Ud. ha adquirido de su vendedor. El residente *daemon* de ESETS siempre se dirigirá sólo a este directorio para confirmar la validez de la clave de licencia, a menos que sea redefinido desde el parámetro 'lic_dir' en el *archivo de configuración* de *ESETS*.

***@ETCDIR*@/scripts/license_warning_script**

Este *script*, si se habilita desde el parámetro 'license_warn_enabled' en el *archivo de configuración* de *ESETS,* se ejecuta durante los 30 días anteriores al vencimiento de la licencia del producto. Se utiliza para enviar notificaciones por correo electrónico sobre la fecha de vencimiento al administrador del sistema.

***@ETCDIR*@/scripts/daemon_notification_script**

Este *script*, si se habilita desde el parámetro 'exec_script' en el *archivo de configuración* de *ESETS*, se ejecuta en caso de que el sistema anti-virus haya detectado una infiltración. Se utiliza para enviar notificaciones por correo electrónico sobre la detección al administrador del sistema.

Capítulo 5:

Integración con los servicios del Sistema de Archivos

Este capítulo describe los procesos de configuración del sistema ESET File Security para lograr una protección eficiente contra infecciones de virus y gusanos en los sistemas de archivos utilizando técnicas de análisis a petición de usuario/sistema y análisis en el acceso. ESET File Security está compuesto por el análisis a petición de usuario/sistema: esets_scan, y análisis en el acceso: **esets_dac**. La versión del producto para Linux también implementa una técnica adicional de análisis en el acceso que utiliza un módulo de biblioteca de carga previa en memoria: **libesets_pac.so**. En las siguientes secciones se describen todos los componentes relevantes.

5.1. Análisis a petición de usuario o sistema

El análisis a petición de usuario o sistema puede ser activado ya sea por un usuario con privilegios (en general, el administrador del sistema) a través de una interfaz de línea de comandos o por el SO que responde a comandos periódicos según las tareas programadas. Esto también explica el término "a petición" cuando decimos que los objetos del sistema de archivos son analizados a petición de usuario o sistema.

El análisis a petición de usuario o sistema no presenta requerimientos especiales para su funcionamiento. Luego de la instalación apropiada del paquete *ESETS* y de que se ha suministrado una clave de licencia válida que se guarda en el directorio de licencias, el usuario puede ejecutar el análisis a petición por medio de una interfaz de línea de comandos o utilizando la herramienta para la configuración de tareas programadas.

Para efectuar el análisis a petición por línea de comandos, habrá que ingresar lo siguiente:

```
@SBINDIR@/esets_scan [option(s)] INCL_DIR -- -EXCL_MASK
```

donde INCL_DIR (o EXCL_MASK) es la lista de directorios y/o archivos que deberán ser analizados (o excluidos del análisis, respectivamente).

Dentro del análisis a petición de *ESETS* se implementan múltiples opciones de línea de comandos. Para obtener la lista completa, leer la página del manual esets_scan(8).

No existe una interfaz de configuración de archivos soportada para este módulo.

5.2. Análisis en el acceso utilizando la interfaz Dazuko

El análisis en el acceso es un análisis ejecutado cuando el/los usuario/s y/o el SO acceden a un objeto del sistema de archivos. Esto también explica el término "en el acceso" cuando decimos que el análisis comienza al intentar acceder a un objeto seleccionado de un sistema de archivos.

La técnica utilizada por el análisis en el acceso de *ESETS* se basa en la intercepción de llamadas de acceso a archivos y el envío de información al núcleo, procesos generados por el módulo para núcleos Linux llamado Dazuko (pronunciado da-tsu-co). El proyecto Dazuko es un programa gratuito, por lo que se distribuye como código de fuente libre para permitir que los usuarios compilen el módulo del núcleo para sus propios núcleos específicos. Recuerde que el módulo para núcleos de Dazuko no forma parte del producto *ESETS*, por lo tanto debe ser compilado e instalado en el módulo en forma previa a iniciar el controlador de acceso **esets_dac** de *ESETS*. Por otra parte, la técnica de Dazuko hace que el análisis en el acceso sea independiente del tipo de sistema de archivos utilizado. También es apropiada para controlar objetos del sistema de archivos a través del sistema de archivos distribuidos NFS, de Nettalk y de Samba.

IMPORTANTE: Antes de proporcionarle al usuario la información detallada sobre la configuración y el uso del análisis en el acceso, nos gustaría destacar que no se espera que los análisis en el acceso de *ESETS* protejan el sistema completo de archivos donde fue instalado. El análisis en el acceso fue diseñado y probado para proteger principalmente los sistemas de archivos ejecutados externamente. Si este no es su caso, necesitará excluir directorios múltiples del control del acceso

a archivos para evitar que el sistema no responda. En este caso, un directorio típico que deberá ser excluido es el directorio '/dev' y los directorios utilizados por *ESETS*.

5.2.1. Pautas generales de uso

El análisis en el acceso **esets_dac** (archivo controlador de acceso que utiliza la interfaz Dazuko) es un programa residente que vigila y controla en forma continua el sistema de archivos. El análisis de cada objeto del sistema de archivos se lleva a cabo como respuesta a eventos configurables de acceso a archivos. Los siguientes tipos de acceso a archivos son soportados por la versión actual:

Eventos ON_OPEN (al abrir)

Este tipo de acceso al archivo es controlado cuando el primer bit del parámetro integrador 'event_mask' en el *archivo de configuración* de *ESETS* (sección [dac]) es 1. En ese caso, se activa el bit ON_OPEN del filtro de acceso de Dazuko.

Eventos ON_CLOSE (al cerrar)

Este tipo de acceso al archivo es controlado cuando el segundo bit del parámetro integrador 'event_mask' en el *archivo de configuración* de *ESETS* (sección [dac]) es 1. En ese caso, se activa el bit ON_CLOSE y el bit ON_CLOSE_MODIFIED del filtro de acceso de Dazuko.

Recuerde que algunas versiones del núcleo no soportan la intercepción de los eventos ON_CLOSE. En este caso se pueden detectar problemas durante el funcionamiento del módulo **esets_dac**.

Eventos ON_EXEC (al ejecutar)

Este tipo de acceso al archivo es controlado cuando el tercer bit del parámetro integrador 'event_mask' en el *archivo de configuración* de *ESETS* (sección [dac]) es 1. En ese caso, se activa el bit ON_EXEC del filtro de acceso de Dazuko.

Al utilizar este mecanismo, todos los archivos normales son analizados contra virus por **esets_** *daemon* al abrirse, cerrarse y ejecutarse. Según el resultado de este análisis, el acceso a los archivos es permitido o denegado.

5.2.2. Instalación y configuración

Ya se ha explicado que, antes del inicio de **esets_dac**, el módulo para núcleos Dazuko debe estar compilado e instalado dentro del núcleo activo. Para compilar e instalar Dazuko, consulte la página web *http://www.dazuko.org/howto-install.shtml*.

Una vez que Dazuko esté instalado, lea y edite las secciones [global] y [dac] del archivo de configuración de *ESETS*. Recuerde que para un correcto funcionamiento del análisis en el acceso es necesario habilitar la opción 'agent_enabled' dentro de una sección [dac] del *archivo de configuración* de *ESETS*. También es necesario definir los objetos del sistema de archivos (es decir, directorios y archivos) que se desea que sean controlados por el análisis en el acceso. Esto se realiza definiendo las opciones de configuración de los parámetros 'ctl_incl' y 'ctl_excl' dentro de las secciones [dac] del archivo de configuración de *ESETS*. Para que se active la configuración que acaba de crear, cargue nuevemante el *daemon* de *ESETS*.

5.2.3. Consejos

Para activar el módulo de Dazuko antes del inicio de cada *daemon* **esets_dac**, siga los siguienetes pasos:

Copie el módulo Dazuko en algunos de los directorios ubicados dentro del directorio reservado para los módulos del núcleo

```
/lib/modules
```

o

```
/modules
```

Utilice las utilidades del núcelo 'depmod' y 'modprobe' (para el SO BSD, use 'kldconfig' y 'kldload') para administrar las dependencias y para la ejecución apropiada del módulo Dazuko recién agregado. Inserte la siguiente línea de comandos en el *script* '/etc/init.d/esets_daemon' del **esets_daemon** antes del mensaje del inicio de ejecución del *daemon*.

```
/sbin/modprobe dazuko
```

En el SO BSD, la línea de comandos

```
/sbin/kldconfig dazuko
```

debe ser insertada en el *script* '/usr/local/etc/rc.d/esets_daemon.sh'.

IMPORTANTE: Es de suma importancia ejecutar los pasos individuales mencionados en el orden exacto en que fueron escritos. El motivo es que en caso de que el módulo del núcleo no se halle dentro del directorio, 'modprobe' (o para el SO BSD, 'kldload') no podrán soportar la ejecución del módulo y pueden provocar que el sistema no responda.

5.3. Análisis en el acceso utilizando la biblioteca de carga previa LIBC

En las secciones precedentes hemos descripto la integración del análisis en el acceso usando la interfaz Dazuko con los servicios del sistema de archivos de Linux/BSD. Llegado este punto nos gustaría aclarar que la técnica que requiere el uso de Dazuko puede no ser bien aceptada por los administradores de sistemas que llevan adelante los sistemas críticos donde el código fuente y/o el archivo de configuración apropiados para el actual núcleo activo no están disponibles o el núcleo es monolítico en vez de modular. En este caso resulta muy útil la segunda técnica presentada de análisis en el acceso basado en la biblioteca estándar de C (*LIBC*) de carga previa.

Esta sección sólo es relevante para usuarios del SO Linux. Contiene información sobre el uso, la instalación y la configuración del análisis en el acceso utilizando la biblioteca de carga previa **libesets_pac.so**.

5.3.1. Pautas generales de uso

El análisis en el acceso **libesets_pac.so** (el archivo controlador de acceso de *ESETS* basado en una biblioteca de carga previa) es una biblioteca de objetos compartidos utilizada como biblioteca de carga previa de LIBC y puede activarse durante el inicio del sistema. Por lo tanto, es aplicable a los servidores del sistema de archivos que trabajan con llamadas a la biblioteca LIBC, por ejemplo, los servidores FTP, servidores Samba, etc. El análisis de cada objeto del sistema de archivos se lleva a cabo como respuesta a eventos configurables de acceso a archivos. Los siguientes tipos de acceso a archivos son soportados por la versión actual:

Eventos ON_OPEN (al abrir)
Este tipo de acceso al archivo es controlado cuando el primer bit del parámetro integrador 'event_mask' en el archivo de configuración de ESETS (sección [pac]) es 1. En este caso se interceptan todas las llamadas 'open' u 'open64' de la biblioteca LIBC.

Eventos ON_CLOSE (al cerrar)
Este tipo de acceso al archivo es controlado cuando el segundo bit del parámetro integrador

'event_mask' en el archivo de configuración de ESETS (sección [pac]) es 1. En este caso se interceptan todas las llamadas 'close', 'dup' y 'dup2' de la biblioteca LIBC.

Al utilizar este mecanismo, todos los descriptores sujetos a archivos comunes son analizados contra virus por el *daemon* de ESETS al abrirse y cerrarse. Según el resultado de este análisis, el acceso a los archivos es permitido o denegado.

5.3.2. Instalación y configuración

La instalación de **libesets_pac.so** se lleva a cabo por medio del mecanismo de instalación estándar de las bibliotecas de carga previa. Uno sólo debe definir la variable 'LD_PRELOAD' del entorno con valor absoluto de la biblioteca **libesets_pac.so**. Para mayor información, por favor consulte la página del manual ld.so(8).

IMPORTANTE: Es importante señalar que la variable de entorno 'LD_PRELOAD' debe ser definida expresamente para el proceso *daemon* del servidor de red (FTP, Samba, etc.) que deseamos tener controlado por medio del análisis en el acceso. En general no se recomienda la carga previa de llamadas en bibliotecas LIBC en todos los procesos operativos del sistema, ya que puede retrasar dramáticamente el rendimiento del sistema e incluso provocar que no responda. En este sentido, todos los mecanismos que utilizan el archivo de configuración '/etc/ld.so.preload' no son tan correctos como los que utilizan el comando 'export LD_PRELOAD'. Ambos sobrescriben todas las llamadas relevantes de la biblioteca LIBC del sistema completo que pudieran generar la sobrecarga del sistema durante su inicio.

Entonces, para interceptar nada más que las llamadas relevantes de acceso a archivos relacionadas con objetos que se encuentran sólo dentro del sector del sistema de archivos seleccionado, hay que sobrescribir un comando ejecutable del servidor apropiado del sistema de archivos de red con la siguiente línea de comandos:

```
LD_PRELOAD=libesets_pac.so COMMAND COMMAND-ARGUMENTS
```

donde 'COMMAND COMMAND-ARGUMENTS' es el comando ejecutable original.

Lea y edite las secciones [global] y [dac] del *archivo de configuración* de *ESETS*. Recuerde que para un correcto funcionamiento del análisis en el acceso es necesario definir los objetos del sistema de archivos (es decir, directorios y archivos) que se desea que sean controlados por la biblioteca de carga previa. Esto se puede lograr definiendo las opciones de configuración de los parámetros 'ctl_incl' y 'ctl_excl' dentro de la sección [dac] del *archivo de configuración*. Para que se active la configuración que acaba de crear, cargue nuevamente el *daemon* de *ESETS*.

5.3.3. Consejos

Para activar el funcionamiento del análisis en el acceso junto al inicio del servidor del sistema de archivos de red, se recomienda definir la variable de entorno 'LD_PRELOAD' directamente con un *script* apropiado de inicio del servidor de archivos de red.

EJEMPLO: En el caso de que quisiéramos realizar un análisis en el acceso que abarque todos los accesos al sistema de archivos inmediatamente luego de iniciar el servidor Samba, dentro del comando de inicio relacionado con el *daemon* del samba (/etc/init.d/smb) deberemos reemplazar el comando

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

responsable del inicio del *daemon* smbd, por la siguiente línea de comandos:

```
LD_PRELOAD=libesets_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

De esta manera, los objetos del sistema de archivos controlados por Samba serán analizados inmediatamente después del inicio del servidor Samba, es decir, durante el inicio del sistema.

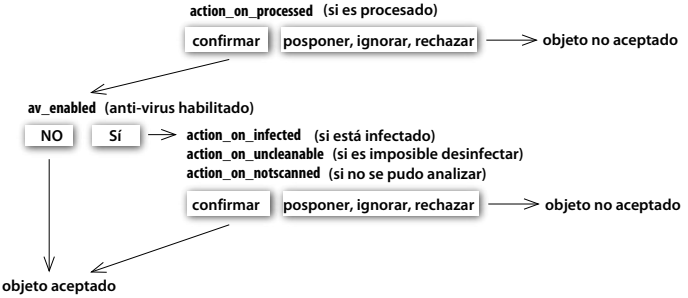
Capítulo 6:

Mecanismos importantes de ESET File Security

6.1. Política para el Manejo de Objetos

La Política para el Manejo de Objetos (ver imagen 6-1) es un mecanismo que permite tomar decisiones sobre los objetos analizados según el estado de su análisis. El mecanismo se basa en las opciones de configuración de las acciones que se deberán realizar ('action_on_processed': si es procesado, 'action_on_infected': si está infectado, 'action_on_uncleanable': si es imposible desinfectar, 'action_on_notscanned': si no se pudo analizar), además de la opción de configuración que habilita el Anti-Virus ('av_enabled').
Para mayor información sobre las opciones, consulte la página del manual esets.cfg(5).

Imagen 6-1. Esquema del mecanismo de la Política para el Manejo de Objetos.



Cada objeto primero se maneja según la opción de configuración 'action_on_processed' (si es procesado). Si se elige 'accept' (confirmar), el destino del objeto dependerá del estado de la opción de configuración 'av_enabled' (anti-virus habilitado). Cuando se habilita 'av_enabled', se procede al análisis del objeto para detectar infiltraciones y se toman en cuenta las opciones de configuración 'action_on_infected' (si está infectado), 'action_on_uncleanable' (si es imposible desinfectar) y 'action_on_notscanned' (si no se pudo analizar) para realizar las acciones pertinentes. Si se elige la acción 'accept' (confirmar) como respuesta a cualquiera de las tres opciones anteriores o la opción 'av_enabled' está deshabilitada, se permite el acceso al objeto; de lo contrario, el objeto se bloquea.

6.2. Configuración específica de Usuario

El producto implementa el mecanismo de Configuración Específica de Usuario para otorgarle practicidad al administrador por medio de una mayor libertad de configuración. El mecanismo permite definir los parámetros de los análisis efectuados por el anti-virus *ESETS* en forma selectiva para que el usuario acceda a los objetos del sistema de archivos.

Recuerde que podrá encontrar una descripción más detallada de esta función en la página del manual esets.cfg(5) y en las demás páginas a las que allí se hace referencia. Por lo tanto, en esta sección sólo daremos un ejemplo conciso sobre la definición de la configuración específica de usuario.

En el caso de que usemos **esets_dac** para controlar los accesos ON_OPEN (al abrir) y ON_EXEC (al ejecutar) de un disco externo cargado bajo el directorio '/data', el módulo está sujeto a la sección de configuración [dac] en el *archivo de configuración ESETS*. La sección es la siguiente:

```
[dac]
agent_enabled = yes
```

```
event_mask = 5
ctl_incl = "/home"
action_on_processed = accept
```

Para establecer la configuración de los parámetros individuales hay que definir el parámetro 'user_config' ingresando la ruta al archivo de configuración especial donde se guardará la configuración individual. En el siguiente ejemplo hacemos referencia al archivo de configuración especial 'esets_dac_spec.cfg' ubicado dentro del *directorio de configuración* de *ESETS*.

```
[dac]
agent_enabled = yes
event_mask = 5
ctl_incl = "/home"
action_on_processed = accept
user_config = "esets_dac_spec.cfg"
```

Una vez que se realizó la configuración especial a la que se hace referencia dentro de la sección [dac], debemos crear el archivo en el *directorio de configuración* de *ESETS* y proporcionarle una configuración individual apropiada. El siguiente ejemplo muestra la configuración individual del parámetro 'action_on_processed' para el usuario 'username'.

```
[username]
action_on_processed = reject
```

El nombre de la sección del encabezado contiene la identificación del usuario para el cual se ha creado una configuración individual. A continuación, el cuerpo de la sección contiene parámetros individuales específicos para ese usuario. De esta manera, con la configuración personalizada, todos los usuarios que intentan acceder al sistema de archivos serán procesados, es decir, todos los objetos del sistema de archivos a los que accedan los usuarios serán analizados para detectar infiltraciones con excepción de los usuarios 'username' cuyo acceso sea rechazado, es decir, esté bloqueado.

6.3. Sistema de Envío de Muestras

El sistema de envío de muestras es una tecnología inteligente ThreatSense.NET que permite detectar los objetos infectados descubiertos por el método de heurística avanzada y enviarlos al servidor del sistema de envío de muestras. Todas las muestras de virus que ingresan en el sistema de envío de muestras serán procesadas por el equipo del departamento de laboratorio de virus de ESET y, si es necesario, agregadas a la base de datos de virus de ESET.

NOTA: DE ACUERDO A NUESTRO CONTRATO DE LICENCIA, AL HABILITAR EL SISTEMA DE ENVÍO DE MUESTRAS UD. ACCEDE A QUE LA COMPUTADORA Y/O PLATAFORMA SOBRE LA QUE ESETS_DAEMON ESTÁ INSTALADO RECOPILE INFORMACIÓN (QUE PUEDE INCLUIR INFORMACIÓN PERSONAL SOBRE UD. Y/O EL USUSARIO DE LA COMPUTADORA) Y MUESTRAS DE VIRUS U OTRAS AMENAZAS DETECTADAS Y LAS ENVÍE A NUESTRO LABORATORIO DE VIRUS. ESTA OPCIÓN SE ENCUENTRA POR DEFECTO DESABILITADA. SÓLO USAREMOS LA INFORMACIÓN Y DATOS RECIBIDOS PARA ESTUDIAR LA AMENAZA Y DAREMOS PASOS RAZONABLES PARA PRESERVAR LA CONFIDENCIALIDAD DE DICHA INFORMACIÓN.

Para activar el sistema de envío de muestras, debe iniciarse el caché del sistema de envío de muestras. Esto se logra habilitando la opción de configuración 'samples_enabled' en la sección [global] del *archivo de configuración* de *ESETS*. Para activar el proceso de envío de muestras a los servidores del laboratorio de virus de ESET también es necesario habilitar el parámetro 'samples_send_enabled' en la misma sección.

El usuario decidirá si desea enviar información suplementaria opcional al equipo del laboratorio de virus de ESET, usando las opciones de configuración 'samples_provider_mail' y/o 'samples_provider_country'. Esta información nos resultará útil para formarnos una visión global sobre la propagación de infiltraciones a través de Internet.

Para obtener información detallada sobre el Sistema de Envío de Muestras, consulte la página del manual esets_daemon(8).

Capítulo 7:

Actualización del sistema de Seguridad de ESET

7.1. Utilidad de actualización de *ESETS*

Para que ESET File Security permanezca efectivo, es necesario mantener al día la base de datos de virus. La utilidad de actualización **esets_update** fue desarrollada con dicho propósito (consulte la página del manual esets_update(8) para más detalles). Si desea activar la actualización, debe definir las opciones de configuración 'username' (nombre de usuario) y 'password' (contraseña) en la sección [update] del *archivo de configuración* de *ESETS*. Recuerde que, en caso de que su acceso a Internet se realice por intermedio de un HTTP proxy, además deberá especificar las opciones de configuración adicionales de dirección: 'proxy_addr', puerto: 'proxy_port' y, en forma opcional, el nombre de usuario: 'proxy_username' y la contraseña: 'proxy_password' correspondientes. Para realizar una actualización, ingrese el comando:

```
@SBINDIR@/esets_update
```

Para otorgarle al usuario la mayor seguridad, el equipo de ESET recopila las definiciones de virus en forma continua de todas partes del mundo. Como los patrones nuevos pueden ser agregados a la base de datos en intervalos muy reducidos, se recomienda realizar las actualizaciones con regularidad. Recuerde que el *daemon* de *ESETS* es capaz de llevar a cabo la actualización periódica del sistema una vez que la opción de configuración 'av_update_period' especificada en la sección [update] del *archivo de configuración* de *ESETS y* el *daemon* se hayan habilitado y estén ejecutándose.

7.2. Descripción del proceso de actualización de *ESETS*

El proceso de actualización consiste en dos partes. Primero se replican todos los módulos relevantes de compilación previa desde el servidor ESET. Los módulos de compilación previa son descargados por defecto dentro del directorio

```
@BASEDIR@/mirror
```

Recuerde que la ruta del directorio de replicación puede modificarse usando la opción de la configuración 'mirror_dir' en la sección [update] del *archivo de configuración* de *ESETS*.

Los módulos de *ESETS* se dividen en dos categorías: la categoría motor y la categoría componente. Los módulos de la categoría componente en la actualidad sólo pueden utilizarse con el SO MS Windows. Hoy en día son soportados los siguientes tipos de módulos correspondientes a la categoría motor: módulos de análisis básicos (prefix engine) que contienen bases de datos con firmas de virus, módulos de soporte de ficheros (prefix archs) que soportan varios formatos de ficheros del sistema de archivos, módulos de heurística avanzada (prefix advheur) que contienen la implementación del método de heurística avanzada para detección de virus y gusanos, módulos de análisis de gusanos en archivos comprimidos (prefix pwscan) utilizados en el SO MS Windows, módulos para utilidades (prefix utilmod) utilizados en el SO MS Windows y módulos para soporte de tecnología ThreatSense.NET (prefix charon). Estos módulos son imprescindibles, en consecuencia todos ellos son descargados por defecto durante cada proceso de descarga. Por el contrario, los módulos de la categoría componente dependen de la plataforma y de la configuración del idioma, por lo tanto la descarga de los módulos de la categoría componente es opcional.

Luego de la descarga de los módulos de compilación previa, también se crea el archivo 'update.ver' en el directorio de réplica. Este archivo contiene la información sobre los módulos guardados actualmente en la réplica recién creada. La réplica recién creada sirve entonces como servidor completamente funcional de descarga de módulos y se puede utilizar para crear nuevas réplicas subordinadas; sin embargo, para ello será necesario cumplir con algunas condiciones adicionales. En primer lugar, debe haber un servidor HTTP instalado en la computadora desde donde los módulos puedan ser descargados. En segundo lugar, los módulos que sean descargados por otras computadoras deberán ser ubicados en la ruta de directorio:

```
/http-serv-base-path/nod_upd
```

donde 'http-serv-base-path' es una ruta al directorio del servidor HTTP básica, ya que constituye el primer lugar donde la utilidad de actualización busca los módulos.

La segunda parte del proceso de actualización consiste en la compilación de módulos que el programa de análisis de ESET File Security carga desde los módulos que se encuentran guardados en la réplica local. Los módulos de *ESETS* que suelen crearse son los siguientes: un módulo base (nod32.000), un módulo para soporte de archivos (nod32.002), un módulo de heurística avanzada (nod32.003), un módulo de análisis de gusanos en archivos comprimidos (nod32.004), un módulo para utilidades de Windows (nod32.005) y un módulo para soporte de la tecnología ThreatSense.NET (nod32.006). Todos los módulos mencionados son creados en el directorio:

```
@BASEDIR@
```

Recuerde que éste es exactamente el mismo directorio desde donde el *daemon* de *ESETS* carga los módulos, por lo tanto puede redefinirse usando la opción de configuración 'base_dir' en la sección [global] (o [update]) del *archivo de configuración* de *ESETS*.

Capítulo 8:

Contáctenos

Estimado usuario, el propósito de esta guía es brindarle la información necesaria sobre la instalación, configuración y mantenimiento de ESET File Security. No obstante, la tarea de redactar un manual es un proceso que nunca se finaliza. Siempre quedarán temas que podrían haber sido explicados con mayor detalle o que directamente se han excluido. Por lo tanto, si encuentra omisiones o inconsistencias en este documento, por favor, informe el problema a nuestro centro de atención:

http://www.eset.com/support

Deseamos poder ayudarlo a resolver cualquier tipo de problema sobre el producto.

Apéndice A. Licencia de PHP

La Licencia de PHP, versión 3.01 Copyright (c) 1999 - 2006 The PHP Group. Todos los derechos reservados. La redistribución y el uso en formas fuente y/o binaria, con o sin modificaciones, están permitidas siempre que se cumplan las siguientes condiciones:

1. Las redistribuciones de código fuente deben retener la advertencia de derechos de autor expresada arriba, esta lista de condiciones y el descargo expresado a continuación.

2. La redistribución en formato binario debe reproducir la advertencia de derechos de autor expresada arriba, esta lista de condiciones y el descargo expresado a continuación en la documentación y/u otros materiales que se proporcionen junto con la distribución.

3. El nombre "PHP" no debe utilizarse para respaldar o promocionar productos derivados de este programa sin el permiso previo por escrito. Para conseguir el permiso escrito, por favor, póngase en contacto con group@php.net.

4. Los productos derivados de este programa no podrán llamarse "PHP", ni contener las siglas "PHP" en su nombre, sin el permiso por escrito de group@php.net. Ud. podrá indicar que su programa funciona en conjunto con PHP llamándolo "X para PHP" en lugar de llamarlo "X de PHP" o "XPHP"

5. El grupo de PHP (PHP Group) puede publicar versiones nuevas o modificadas de la licencia con cierta frecuencia. Cada versión tendrá un número de versión diferente. Una vez que un código cubierto se haya publicado bajo una versión particular de la licencia, Ud. podrá continuar usándolo bajo los términos de dicha versión. También podrá optar por utilizar el código cubierto bajo los términos de cualquiera de las versiones posteriores de la licencia, publicadas por el grupo de PHP. Ninguna persona ajena al grupo PHP está autorizada a modificar los términos aplicables al código cubierto creados según esta Licencia.

6. Las redistribuciones en cualquier forma deben incluir la siguiente mención "Este producto utiliza el programa PHP, disponible en forma gratuita en la página web: <http://www.php.net/software/>".

ESTE PROGRAMA SE PROPORCIONA A TRAVÉS DEL EQUIPO DE DESARROLLO DE PHP "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA INCLUYENDO, PERO SIN LIMITACIÓN, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD Y ADECUACIÓN PARA UN PROPÓSITO EN PARTICULAR. EN NINGÚN CASO EL EQUIPO DE DESARROLLO DE PHP O SUS COLABORADORES SERÁN RESPONSABLES DE CUALQUIER DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO SIN LIMITACIÓN, LA PROCURACIÓN O SUSTITUCIÓN DE BIENES O SERVICIOS; PÉRDIDA DE USO, DATOS O BENEFICIOS; O INTERRUPCIÓN DE NEGOCIO) CAUSADO SIN EMBARGO Y EN CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA EN CONTRATO, RESPONSABILIDAD ESTRICTA O EXTRACONTRACTURAL (INCLUYENDO LA NEGLIGENCIA U OTRAS) EMERGENTES DEL USO DE ESTE PROGRAMA, INCLUSO SI SE ADVIERTE SOBRE LA POSIBILIDAD DE DICHOS DAÑOS.