IS23 Mantenimiento de Instalaciones Informáticas
Práctica 5. Mantenimiento preventivo (II)

Ingeniería Técnica Informática de Sistemas

1 – Objetivos

En la presente sesión se pretende familiarizar al alumno con la instalación y el uso de aplicaciones destinadas a proteger el sistema de virus y de las intrusiones a través de la conexión a una red.

2 – Material

Para el desarrollo de la práctica se va a utilizar un ordenador PC con sistema operativo Windows 2000 y las aplicaciones:

- AVG Antivirus
- AD-Aware
- Zone Alarm

además de varios disquetes 3½" HD 1.44 Mb.

3 – Introducción teórica

Una segunda perspectiva del mantenimiento preventivo consiste en impedir que programas u otros usuarios malintencionados perturben el correcto funcionamiento del sistema.

Por una parte existen los denominados ***virus*** que son programas que, como actividad principal, se transmiten de unos computadores a otros (consiguiendo cuando menos consumir espacio de almacenamiento y capacidad de cálculo del computador) y adicionalmente pueden producir todo tipo de daños en el computador en que se encuentran.

Otra categoría son los programas que se instalan en nuestro sistema aprovechando alguna de las vulnerabilidades de *Windows* y que, sin ser virus propiamente dichos, se dedican a realizar acciones nada recomendables como la de enviar información privada a terceros, abrir periódicamente una nueva ventana del navegador con propaganda, sustituir el número de acceso a *Internet* por un número con tarificación especial (los antiguos 906), etc.

Finalmente, otros usuarios pueden utilizar la conexión a *Internet* para acceder a nuestro sistema de forma no autorizada y producir todo tipo de desastres.

En la presente sesión de prácticas se procederá a emplear aplicaciones desarrolladas específicamente para impedir todos los modos de actividad malintencionada citados.

4 – Desarrollo de la práctica

Durante la sesión de prácticas se procederá a la instalación y uso de las aplicaciones propuestas como ejemplo representativo de cada una de las categorías anteriormente enunciadas.

4.1 – AVG antivirus

Uno de los problemas más acuciantes en los sistemas operativos *Windows* es la existencia y proliferación de virus que pueden poner en peligro la integridad del sistema a la vez que se sirven de él para su propagación (también denominada ***infección*** o ***ataque***) a otros computadores. Con la aparición de *Internet* como medio de comunicación, la propagación y virulencia de los virus ha alcanzado niveles dramáticos.

Existen muchos productos antivirus en el mercado. Algunos de los fabricantes de antivirus más reconocidos son:

Computer Associates
F-secure
McAfee
Panda Software
Symantec
Trend Micro

Dentro de los distintos productos antivirus de estos fabricantes se encuentra una gran variedad de soluciones que ofertan más o menos servicios además, claro está, de la clásica búsqueda de los posibles virus que pueda haber en el computador en que se instale la aplicación. También es posible encontrar algunas soluciones antivirus gratuitas, como por ejemplo:

AVG antivirus (free edition). http://www.grisoft.com/us/us dwnl free.php
OpenAntivirus. http://www.openantivirus.org

De éstos, el antivirus AVG es más sencillo de instalar. Desgraciadamente, es necesario registrarse para poder obtener una versión gratuita. Para evitar tener que realizar este registro sólo para realizar la práctica (puedes hacerlo si quieres tener una copia propia del antivirus) y puesto que la versión completa permite un periodo de prueba de 30 días, se ha dejado una copia de esta versión en:

ftp://lorca.act.uji.es/933/apps/avg_antivirus/avg70t_230.exe

Procede a instalar esta versión del antivirus AVG. Una vez comenzado el proceso de instalación se te pedirá que reinicies el computador. Una vez hayas reiniciado el computador y se te presente el menú de arranque, vuelve a seleccionar la opción *Windows*.

1 - ¿Ha ocurrido algo distinto a lo que era el proceso de arranque hasta ahora? ¿Qué?

2 - Cuando vuelvas a iniciar la sesión, el proceso de instalación continuará. ¿Por qué crees que el instalador ha reiniciado el computador en mitad del proceso de instalación en lugar de continuar con completarla de una sola vez?

En esta nueva fase del proceso de instalación se te ofrecerá la posibilidad de realizar una actualización (***update***). Pulsa el botón Run Update para que dicha actualización se produzca.

3 - ¿Qué es exactamente lo que se está actualizando?

En la tercera fase de la instalación, se te ofrecerá la posibilidad de crear un juego de disquetes de arranque. Acéptala pulsando el botón correspondiente.

4 - Si vamos a tener instalado el antivirus en el computador, ¿por qué crear una copia en disquetes? ¿qué sentido tiene?

El asistente para la creación del juego de disquetes de arranque proporciona la opción de elegir aquellos componentes que deben guardarse.

5 - ¿Cuáles son?

6 - ¿Este juego es específico para el computador en el que realizas las prácticas o serviría para otro computador?

Sigue todos los pasos (puede que necesites 3 disquetes) para la creación del juego de disquetes. Una vez finalizada la creación de los disquetes, continuamos con el asistente para la instalación del AVG antivirus. Salta el paso correspondiente al ***mail scanner*** (esta opción es sumamente interesante, pero no podemos probar su funcionalidad en el laboratorio). La última posibilidad que se nos ofrece consiste en la realización de un rastreo completo del sistema para encontrar posibles virus. Selecciona la opción correspondiente para que se lleve a cabo dicha exploración.

Mientras se realiza el rastreo vamos a suponer que hemos encontrado un virus y queremos saber cuán peligroso es, en qué consiste su actividad y cómo se puede detectar. Para ello, y utilizando el navegador, podemos entrar en la siguiente página de Panda antivirus:

http://www.pandasoftware.es/virus info/enciclopedia/

En dicha página aparecen los virus más activos del momento permitiendo encontrar información sobre algún virus en particular. Busca información sobre el virus ***mydoom*** y selecciona alguna de sus variantes.

7 - Resume la ficha de la variante que hayas escogido.

Una vez haya terminado su rastreo el antivirus contesta a la siguiente pregunta:

8 - ¿Ha encontrado algún virus?

Examina con detenimiento la aplicación y explora su funcionalidad. Si tienes alguna duda consulta al profesor.

De entre las opciones que ofrece este antivirus hay una llamada ***virus vault***.

9 - ¿Qué es y para qué sirve el ***virus vault***?

(Puedes buscar la traducción de ***vault*** en http://www.diccionarios.com/)

Durante el proceso de instalación del antivirus has creado un juego de disquetes de arranque. Pon el primer disquete de arranque en la disquetera y reinicia el computador. Una vez finalizado el proceso de arranque del antivirus desde el disquete aparece una aplicación con una serie de opciones.

10 - ¿Cuáles son?
11 - ¿Cuál de ellas es específica para el computador en el que se creó el juego de disquetes?
12 - ¿Podrías pasar el test en otro computador utilizando este juego de disquetes?

No es necesario que pruebes ninguna de ellas, selecciona la opción ***Exit*** y reinicia el computador sin ningún disquete en la disquetera.

4.2 – Ad-aware

Una de las aplicaciones que permite detectar si se ha instalado software malintencionado en un equipo con *Windows* es ***Ad-aware***.

Hay que tener en cuenta que el software malintencionado no se instala como lo haría una aplicación corriente ya que su objetivo es el de permanecer oculto: no debe delatarse cuando se instala y no debe ser fácilmente identificable una vez esté instalado. Esto es así precisamente para que pueda llevar a cabo su labor durante el mayor tiempo posible. Tanto es así, que muchos usuarios suelen desconocer que tienen instalados multitud de estos componentes. Dichos componentes suelen conseguir su objetivo aprovechando algún fallo de seguridad de alguna de las aplicaciones de *Windows* (suelen instalarse aprovechando que el usuario visita ciertos sitios *web* en los que están al acecho). Debido justamente a la dificultad de su identificación es necesario recurrir a utilidades como ésta para su detección y eliminación. Es interesante destacar, además, que algunas de las utilidades que se anuncian para eliminar gratuitamente a estos componentes constituían a su vez software de este tipo.

Según su propia definición, ***Ad-aware*** es una utilidad destinada a mantener la privacidad de los usuarios de un equipo, capaz de rastrear la memoria, el registro del sistema, los discos duros, extraíbles y ópticos buscando componentes conocidos que se dedican a obtener información, realizar publicidad agresiva y registrar los movimientos del usuario. Una vez finalizado el rastreo, muestra una lista los componentes encontrados y ofrece la oportunidad de ponerlos en cuarentena eliminándolos del sistema. Puedes descargar el instalador de ***Ad-aware*** desde:

ftp://lorca.act.uji.es/933/apps/ad-aware/aawsepersonal.exe

Una vez instalada la aplicación, actívala haciendo doble-clic sobre el icono del escritorio. Antes de comenzar el rastreo es conveniente actualizar la base de datos de componentes conocidos. Para ello pulsa en el botón Check for updates now. Una vez

realizada la actualización pulsa Next, selecciona la opción ***Perform smart system-scan*** (activa por defecto) y continúa. Espera a que acabe la detección.

13 - ¿Ha encontrado algún componente extraño?
14 - ¿Cuáles?

Observa cómo al seleccionar el botón de continuar, los objetos son borrados del sistema y almacenados en un fichero en cuarentena.

15 - ¿Por qué crees que no se borran sin más? ¿Qué objetivo tiene ponerlos en cuarentena?

4.3 – Zone Alarm

El medio por el que llegan la mayor parte de los ataques a computadores en la actualidad es justamente *Internet*. Uno de los principales mecanismos para la difusión de virus y gusanos informáticos es, de hecho, el correo electrónico: el usuario no debería abrir sin más todos los archivos adjuntos que le lleguen ya que éstos pueden estar infectados (los más sofisticados ni siquiera necesitan que el usuario abra el archivo adjunto para actuar).

De todas formas, navegar o leer el correo no es la única forma de ser atacado. Es decir, sin que hagamos nada, un computador conectado a la red puede ser atacado desde otro computador. Estos ataques son principalmente de dos tipos: ***dirigidos*** o ***indiscriminados***.

El primero de ellos, el ***ataque dirigido***, supone que somos objeto del ataque: alguien quiere acceder a nuestro computador o a la red en la que está conectado nuestro computador (empresa, universidad...). Probablemente recibiremos pocos ataques de este tipo. Sin embargo, el segundo de los casos, es decir, el ***ataque indiscriminado***, se da constantemente: cuando un gusano informático conquista un ordenador, intenta atacar a cuantos ordenadores se encuentren conectados en ese momento. Puesto que se trata de un programa no se cansará de hacerlo hasta que encuentre otros computadores que presenten la misma vulnerabilidad que él utilizó para entrar en su actual anfitrión.

Un ejemplo de este último caso, es el del gusano denominado ***Blaster*** que afecta a las plataformas *Windows* y se aprovecha de una vulnerabilidad existente en las versiones NT, 2000 y XP. Durante el periodo de mayor actividad de este virus se daba el caso de que, pese a que *Microsoft* poseía la actualización necesaria para evitarlo, en cuanto un ordenador se conectaba a *Internet* con la intención de descargarse la actualización correspondiente, era infectado antes de conseguirlo. Lo increíble del caso es que el usuario se conectaba a la página de *Microsoft* para proteger su computador y, durante ese escaso intervalo de tiempo, su computador era atacado de forma totalmente aleatoria por alguna de las múltiples copias del gusano.

Para evitar en la medida de lo posible este tipo de ataques es posible instalar un tipo de aplicación que recibe el nombre de ***cortafuegos*** (***firewall***). Un cortafuegos tiene como función controlar quién intenta acceder o salir de nuestro computador y autoriza o deniega dicho acceso o salida dependiendo de una serie de reglas. Algunas de las aplicaciones cortafuegos existentes en el mercado son:

ZoneAlarm Pro (Zone Labs)
Tiny Personal Firewall (Tiny Software)
Outpost Firewall (Agnitum)
Kerio Personal Firewall (Kerio Technologies)
BlackICE PC Protection (Internet Security Systems)

Como ejemplo de la utilización de alguna de ellas vamos a instalar y utilizar *ZoneAlarm*. Puedes instalar dicha aplicación desde la siguiente dirección:

ftp://lorca.act.uji.es/933/apps/zonealarm/zlsSetup_45_594_000.exe

Este programa de instalación permite la instalación de la versión profesional (*ZoneAlarm Pro*, de pago) o la versión gratuita. De hecho, podemos seleccionar la versión *Pro* y si en 30 días no introducimos el número de serie correspondiente se quedaría instalada la versión gratuita (perdiendo las funcionalidades añadidas que posee la versión superior).

Para la realización de la práctica seleccionaremos la versión *Pro*. Durante el proceso de instalación, se pedirán una serie de datos personales. Es conveniente, por regla general, no revelar información privada a terceros por lo que se recomienda utilizar direcciones de correo falsas del tipo *noestoy@aqui.com* o similares. Asimismo, conviene desactivar aquellas casillas que ofrezcan la posibilidad de recibir correo sobre actualizaciones o similares.

Sigue el proceso de instalación teniendo en cuenta las siguientes consideraciones:

- Cuando se te pregunte sobre el tipo de *Access permission*, selecciona la opción: ***"No, quiero que me pregunte cada vez que un nuevo programa intenta acceder a Internet"***.
- Cuando se te ofrezca la posibilidad de seguir el tutorial, selecciona dicha opción y descubre las principales características de la aplicación.

Con la aplicación *ZoneAlarm* en funcionamiento, abre una ventana del navegador e intenta acceder a una página web.

16 - ¿Qué ha ocurrido?
17 - ¿Cómo has conseguido navegar?

Si continúas navegando con el explorador que habías abierto, no debería haber ningún problema. Sin embargo, si vuelves a abrir otro navegador,

18 - ¿Puedes navegar?
19 - Si has llegado a navegar, ¿qué has hecho para conseguirlo?
20 - Si no has podido navegar, ¿qué debes hacer para que en el futuro puedas navegar con el explorador sin que seas preguntado cada vez?