Prácticas de la Sexta Entrega del Curso de Linux

6 de junio de 2005

En este fichero se enuncian 3 de las 4 prácticas correspondientes a esta entrega. Las tres prácticas se tienen que subir en ficheros independientes, para cada una de las tareas planteadas en Moodle.

Importante: Esta entrega tiene dos prácticas de Tipo I y dos de Tipo II:

Tipo I

E5-I-1 Realizar correctamente todas las preguntas del cuestionario que para esta entrega se ha habilitado en Moodle.

E6-I-2 Chequeo del sistema con Nessus

Utilizar la herramienta Nessus para hacer un chequeo de nuestro servidor. Para ello debemos instalar Nessus tal como se explica en los apuntes, instalando tanto el demonio `nessusd` como el cliente.

Para simplificar la instalación, no es necesario que realicemos una actualización de los plugins.

Una vez instalado arrancamos el demonio `nessusd` en segundo plano en una ventana de terminal:

```
nessusd -D &
```

A continuación arrancar el cliente:

```
nessus
```

Logarse con el usuario nessus que hemos creado en la instalación y realizar un chequeo de la misma máquina.

Como resultado de esta práctica será necesario enviar una copia de la pantalla con el resultado del chequeo. La captura gráfica, así como los prosibles comentarios se subirán en un fichero en formato OpenOffice, de nombre `e6-i-2.sxw`

Tipo II

E6-II-1 Jhon the ripper

Utilizar la herramienta Jhon the ripper para hacer un chequeo de las claves de nuestro servidor. Para ello debemos instalar la herramienta tal como aparece en los apuntes.

Se pide localizar la clave de, al menos, un usuario. Para ello (usando nuestros privilegios de administrador del sistema) haremos un chequeo de claves utilizando las palabras almacenadas en el fichero `password.lst`, previamente modificado.

Como resultado de la práctica será necesario enviar el proceso seguido para realizar el chequeo de claves, incluyendo los parámetros utilizados y los ficheros de configuración modificados. El fichero a subir tendrá por nombre `e6-ii-1.sxw`

E6-II-2 ClamAV

Instalar el antivirus ClamAV, integrándolo con un agente de transporte (postfix, por ejemplo). Para comprobar que funciona, debéis mandar un correo a un usuario local de vuestro sistema (no hace falta que estéis en Internet), incorporando como archivo adjunto el fichero `hsqejoq.exe`.

Como resultado, debéis subir en un fichero de nombre `e6-ii-2.sxw` el correo que se envía al postmaster de vuestro sistema, indicando que se ha detectado un virus, así como cualquier otro comentario que estiméis oportuno.