Seguridad en Sistemas Informáticos (SSI)

Laboratorio: tcpd y xinetd

Contenido

Introducción

Las herramientas tcpwrappers y xinetd han sido introducidas en el tema de teoría. La información adicional necesaria para la realización de la práctica se puede obtener de las siguientes páginas de manual:

* tcpwrappers: tcpd, hosts_access, hosts_options, tcpdchk, tcpdmatch
* xinetd: xinetd, xinetd.conf

Objetivos

* Introducir el control de acceso a los servicios como una herramienta útil para aumentar la seguridad de los sistemas.
* Introducir tcpwrappers como caso de estudio básico.
* Introducir xinetd como herramienta adicional complementaria.

tcpwrappers

Configurar tcpd en exta siguiendo las reglas de control de acceso siguientes:

* denegar por defecto todos los servicios
* daytime [1]
    - o permitirlo desde el nodo local (se debe ofrecer el servicio sin modificar)
    - o permitirlo desde base; pero, en vez de ejectuar el demonio habitual, enviar al cliente la salida de la orden w
* ftp [2]
    - o permitirlo desde el nodo local
    - o permitirlo desde base, añadiendo un mensaje al fichero /root/tcpd.log indicando desde dónde se ha intentado.
* daytime y ftp
    - o denegarlo mostrando un mensaje cuando la conexión se intenta desde extb
    - o el mensaje debe ser personalizado, indicando que el servicio tal no puede ser utilizado desde tal ordenador

Comprobar que, efectivamente, el control de acceso funciona tal y como se ha especificado. Sugerencia: usar extf como ordenador al que no le está permitido ningún tipo de acceso.

Nota

La versión de inetd instalada por defecto en las UML es openbsd-inetd, por lo que el guión para gestionar el servicio es /etc/init.d/openbsd-inetd.
[1] El servicio daytime consiste en devolver la hora del sistema e inetd puede ofrecerlo sin recurrir a un servidor externo. Sin embargo, eso supone que no puede ser controlado por tcpd. Por ese motivo, cuando se especifica que se ofrezca este servicio sin modificar, lo que significa es que se utilice un programa externo para ofrecerlo que devuelva la hora del sistema (sugerencia: usar /bin/date).

[2] El servicio ftp lo ofrece el programa VSFTPD, cuyo ejecutable es /usr/sbin/vsftpd y cuyo fichero de configuración es "/etc/vsftpd.conf". Para VSFTPD sea lanzado por inetd, es necesario modificar la configuración por defecto de VSFTPD. Ello supone modificar en el fichero de configuración "/etc/vsftpd.conf" la línea:

listen=YES
por
listen=NO

Material a entregar

Se pide:
* Ficheros de configuración de tcpwrappers
* Descripción de las comprobaciones realizadas y discusión los resultados obtenidos
* Incluir comentarios adicionales sobre las dificultades surgidas al realizar este apartado de la práctica

xinetd

Configurar xinetd en exta siguiendo las reglas de control de acceso siguientes:

* denegar por defecto todos los servicios
* daytime [3]
    o permitirlo desde base restringiendo las conexiones a una franja de 5 minutos (se establece una franja tan estrecha para facilitar la comprobación) y redirigiendo las conexiones a extc (será necesario activar este servicio en extc permitiendo conexiones al menos desde exta)
* discard
    o permitir dos conexiones simultáneas por nodo desde el nodo local, base y extb
    o limitar el número total de conexiones simultáneas a 3

Comprobar que, efectivamente, el control de acceso funciona tal y como se ha especificado. Sugerencia: usar extf como ordenador al que no le está permitido ningún tipo de acceso.
[3] A diferencia de inetd, xinetd puede controlar el acceso a servicios internos, por lo que en este caso no será necesario utilizar un servidor externo como date.

Nota

El guión para gestionar el servicio xinetd es /etc/init.d/xinetd.

Se recomienda modificar la configuración por defecto de xinetd (fichero /etc/xinetd.conf) para que utilice syslog como destino de sus mensajes. Así mismo, se recomienda activar la opción HOST del registro en caso de fallo.
Material a entregar

Se pide:

* Ficheros de configuración de xinetd
* Descripción de las comprobaciones realizadas y discusión los resultados obtenidos
* Incluir comentarios adicionales sobre las dificultades surgidas al realizar este apartado de la práctica

Entrega de material

Subir a Aula Virtual el material solicitado en cada uno de los apartados de la práctica.