Apéndice D. Wrappers

"Los pequeños actos que se ejecutan son mejores que todos aquellos grandes que se planean."

George Marshall

Todos los servicios ofrecidos desde una máquina son potenciales puertas para un atacante, y por ellos es necesario cerrar todo aquello que no se necesite. [VIL00]

Instalación:

Un aspecto importante de seguridad es proteger a los nodos con un programa que le niegue el permiso (acceso) a usuarios que provengan de nodos externos a la UDLA, asi como permitirlo a los que sean nodos internos. El programa que logra ese proposito se llama Wrapper y en la UDLA se implanta el tcpd que se generó a partir de la version de dominio publico tcpd de Wietse Venema.

En Solaris 1.x y Solaris 2.0, 2.1 − 2.7 existe principalmente TCP/IP version 4. Para Solaris 8 existen ambas versiones de TCP/IP, pero el wrapper de la version 4 no sirve en solaris 8.

El wrapper de la version 6 solo sirve para solaris 8 y wrappea las conexiones tanto de version 4 como de version 6.

Pasos:

1. Copiar el programa wrapper **tcpd6.tar** al directorio /usr/sbin.
   En el caso de tener kerberos, ponerlo tambien en /usr/local/sbin.
2. Editar el archivo /etc/inetd.conf y para los servicios de udp y tcp como telnet, ftp, shell, login, rexec, etc. cambiar las lineas originales que son de este tipo:
   ftp stream tcp6 nowait root /usr/sbin/in.ftpd in.ftpd
   telnet stream tcp6 nowait root /usr/sbin/in.telnetd in.telnetd
   Al siguiente tipo:
   ftp stream tcp6 nowait root /usr/sbin/tcpd6 in.ftpd
   telnet stream tcp6 nowait root /usr/sbin/tcpd6 in.telnetd

   Lo que se hace es cambiar la penultima columna, sustituyendo el ´invocador´ de servicio original por el programa ´tcpd6´
3. Re−inicializar el superdaemon ´inetd´ con un kill −HUP <PID>,
   ejemplo:
   # ps −ef| grep inetd
   root 147 1 0 11:12:27 ? 0:02 /usr/sbin/inetd −s
   # kill −HUP 147
4. Editar los archivos /etc/hosts.allow y /etc/hosts.deny, especificando que nodos pueden usar servicios de nuestra maquina asegurada. La politica general del centro de computo es "cualquier nodo dentro de la UDLA puede entrar a cualquier nodo dentro

de la UDLA", lo cual se hace poniendo el /etc/hosts.allow con este contenido:
ALL:140.148.:
Y la otra politica del centro de computo es: "Todo nodo fuera de la UDLA no puede accesar ningun nodo dentro de la UDLA", esto se logra poniendo el contenido de /etc/hosts.deny asi:
ALL:ALL

5. Para comprobar que funciona bien, hacer un telnet desde un nodo dentro de la udla hacia la maquina asegurada y el telnet debera permitir el acceso (pidiendo username y password, por supuesto). Hacer un telnet desde fuera de la UDLA y el telnet ni siquiera pide el username, sino que rechaza la conexión.

índice figuras introducción 1 2 3 4 5 A B C D referencias