OpenBSD: una alternativa a Linux basada en la Seguridad

Iñigo González Ponce <igonzalez@ati.es>

Octubre 1999

Resumen

El presente artículo presenta el sistema operativo OpenBSD como alternativa a Linux en entornos de explotación y desarrollo en los que la seguridad del sistema sea importante.

1 Si no puedes utilizar Linux, ofrece alternativas

Todos hemos oído hablar de Linux en la prensa, hemos visto algún sistema Linux en funcionamiento; algunos, incluso nos hemos *peleado* con Linux configurando una serie de dispositivos y subsistemas de nombre desconocido para los no iniciados. Hasta hay quien, ahora mismo, utiliza Linux en su casa o en el trabajo.

Quienes conocemos Linux hemos podido comprobar que es un gran sistema informático: es estable, flexible, funciona en la mayoría del hardware disponible, y además es barato. Sin embargo, esto no es suficiente para que una organización elija Linux como plataforma para sus servidores o estaciones de trabajo. ¿Porqué? los factores que influyen en esta decisión son muy variados: desde rechazo total por parte del *jefazo* de turno, desconfianza a un producto gratuito, desconocimiento, miedo a no encontrar soporte, o poca confianza en la seguridad que ofrece Linux.

Si te sientes a gusto utilizando Software Libre y te has encontrado en esta situación anteriormente, propón otra alternativa basada en software libre además de Linux. En cualquier caso, eso siempre es mejor que acabar utilizando sistemas propietarios como Solaris, o NT; a largo plazo, tus jefes y la empresa te lo agradecerán.

2 Cómo presentar OpenBSD al jefe.

La próxima vez que tu jefe te diga que no vais a integrar Linux ofrecele OpenBSD como alternativa. Basta con preguntarle algo así como: "¿Es que esta vez has decidido utilizar OpenBSD?" al menos, le picará la curiosidad y te preguntará qué es OpenBSD.

OpenBSD es un Sistema Operativo orientado a la Seguridad. Es el sistema más seguro que actualmente puede obtenerse libremente sin pasar por registros de exportación que limiten sus características.

Las características de seguridad se han cuidado hasta el más mínimo detalle. El sistema soporta por defecto IPSec, varios algoritmos de cifrado (DES, 3DES, Blowfish, Cast, y Skipjack) y funciones hash criptográficas como MD5, y RIPE MD-180.

Después de una instalación típica, el sistema se encuentra cerrado ante un posible ataque. El administrador del sistema debe activar explícitamente aquellos servicios que desea utilizar en la máquina. Esto hoy no es muy novedoso, pero cuando se introdujo, en 1995, sí lo era.

En lo referente a software hay un problema con OpenBSD: tiene una colección de *ports* (es decir, de software preparado para este sistema) limitada. A pesar de ello, esta colección de *ports* es muy cómoda; y si dispones de una conexión a Internet basta con montar el CD correspondiente para que automáticamente busque el software, lo baje, aplique los parches necesarios, y finalmente lo compile y se instale en el lugar adecuado.

Si no tienes suerte y el programa que quieres utilizar no está disponible para OpenBSD, puedes obtener un binario para Linux, SCO, o para otro BSD (FreeBSD, NetBSD, o BSDI), y seguramente sea posible utilizarlo.

Para utilizar este programa, el kernel se ha tenido que compilar habilitando la opción de compatibilidad binaria con estos sistemas, y tienes que tener instaladas sobre `/emul/sistema_a_emular` las bibliotecas de enlace dinámico del sistema operativo correspondiente al ejecutable, así como ciertos archivos (como `/etc/shadow`) de los que este dependa.

A pesar de que la compatibilidad binaria funciona bien, no hace milagros: no puedes cargar LKM de Linux, y los programas como `top` que accedan a características específicas de otros sistemas operativos (como `/proc` o `/dev/hda1`) no funcionarán correctamente.

OpenBSD funciona perfectamente en una Intranet o en redes con conexión directa a Internet. La razón es muy simple: Este Sistema Operativo deriva de 4.3 y 4.4BSD, donde se publicó por primera vez la implementación de referencia del protocolo TCP/IP. Desde entonces el código fuente ha pasado por auditorías de seguridad periódicas y se ha actualizado para incluir las modificaciones que se han ido produciendo al protocolo IP (path mtu discovery, prevención contra SYN-Flood, slow start, y slow recovery, etc...).

Puede que estés utilizando productos que contiene código derivado de BSD, o de OpenBSD sin saberlo. Si utilizas routers Cisco, servidores Apple con MacOS X, OS/2 Server, Solaris y/o SunOS, SRI IRIX, etc... habrás podido comprobar cómo funciona el código de red de BSD. Si hay quien depende de estos productos para gestionar la informática de su organización ¿porqué no utilizar la base común de la que derivan?

Un último argumento para impresionar a los jefes: A partir de la versión 2.5 de OpenBSD disponemos de un Sistema Operativo seguro con el que podemos tener preparado un servidor HTTPS en menos de una hora.

3 El entorno de trabajo de OpenBSD sin sorpresas (desagradables)

Hasta este momento todo han sido buenas noticias, pero nos hemos guardado una mala: OpenBSD no es Linux.

Esto quiere decir que tendremos que aprender a utilizar un nuevo Unix con todos los inconvenientes que conlleva: localizar los scripts de arranque, bibliotecas de enlace dinámico, dónde se encuentran los ejecutables más comunes (como, por ejemplo sendmail, que tiende a cambiar de ubicación de un sistema a otro), distintas sintaxis para ordenes comunes, etc...

Si esta es la primera vez que utilizas otro sistema Unix, estos cambios te van a parecer al principio un mundo, sobre todo en OpenBSD donde cada usuario (especialmente root) tiene el path más restringido posible para evitar futuros problemas de seguridad.

Después del choque cultural empezamos a ver las ventajas de conocer cómo funciona OpenBSD. La primera de ellas es que es sencillo, y tiene que serlo por dos razones:

a) Si quieres un sistema que sea seguro tienes que construirlo sobre una base sencilla

b) Sólo hay un OpenBSD, lo que evita el problema de tener que aprender las peculiaridades de una nueva distribución (¿qué usuario de Slackware no ha pasado horas buscando en Red Hat el archivo con la dirección de red de su tarjeta?).

En este aspecto OpenBSD es similar a la distribución Slackware de Linux con la salvedad de que los scripts de arranque se encuentran en `/etc` y tienen nombres tales como `/etc/rc` *(arranque inicial)*, `/etc/rc.local`, `/etc/rc.conf`, `/etc/netstart`, etc... Por cierto, hay varios archivos fundamentales para que arranque correctamente el subsistema de red TCP/IP: `/etc/defaultrouter`, `/etc/hosts`, y `/etc/hostname.interfaz_de_red`. Curiosamente, SunOS y Solaris necesitan estos mismos archivos para arrancar el subsistema de red; de hecho, quien ha administrado previamente RedHat Linux y OpenBSD, puede hacerse cargo de un sistema basado en Solaris con apenas una semana de adaptación.

Después de instalar Linux, una gran cantidad de usuarios se preguntan ¿qué voy a hacer ahora? En OpenBSD la respuesta es muy simple: cuando entramos por primera vez al sistema como superusuarios, vemos un mensaje que nos anima a ver la página del manual afterboot(8). Allí podemos consultar una página del manual de OpenBSD en la que se ayuda al usuario a configurar el sistema, y de paso nos muestra algunas de las características más notables de OpenBSD.

Esto es lo que hace fácil usar OpenBSD: aunque no dispongamos de una serie de documentos como los HOWTO de Linux, es posible obtener esta información de forma sencilla en las páginas del manual en línea de Unix.

Ademas de la página afterboot(8), otras páginas que podemos consultar para obtener ayuda son las que describen el protocolo TCP/IP tcp(4), ip(4), ipsec(4); disponemos de páginas describiendo cada uno de los dispositivos del sistema como, por ejemplo el dispositivo de CD-Rom Atapi acd(4), o la interfaz de red loopback lo(4); además de páginas dedicadas a temas determinados como la configuración de redes virtuales privadas vpn(4).

4 Perfiles de Uso para OpenBSD

Un sistema puede ser muy amigable y estar muy bien diseñado, pero lo que realmente importa es que funcione como se espera de él, lo que lleva a preguntarnos lo siguiente ¿ cómo se comporta OpenBSD en un entorno de trabajo real ?

4.1 Características útiles para cualquier entorno de trabajo

- Protección contra toma de conexiones:
  - TCP ISN Aleatorio basado en estado de la máquina (ratón, teclado, paquetes recibidos, etc...)
  - Verificación *fuerte* del estado de la conexión TCP.

- Protección contra ataques de fragmentación.

- Entrada al sistema reforzada
  - S/KEY integrado de serie en el Login, tanto en `/bin/login` (consola local, y telnet), como en transferencias de archivos vía FTP.
  - Opcionalmente se incluye Kerberos IV (KTH-Kerberos) para autenticación con tickets.
  - A partir de OpenBSD 2.6 no será necesario instalar SSH.
  - Los servidores desarrollados para OpenBSD han sido comprobados previamente contra posibles problemas de seguridad.

- Nivel de Usuario
  - Generación de números de i-nodo aleatoria (aunque se penaliza ligeramente en la caché de disco).
  - Se alerta en consola de intentos fallidos o exitosos de realizar un `login` o un `su` a la cuenta de *root*.
  - Se incluye un generador de números aleatorios no predecibles en `/dev/urandom`.
  - Distintos niveles de seguridad en las contraseñas. Se puede especificar un algoritmo de cifrado específico para cada usuario y, según el algoritmo, el número de bits que se utilizarán para cifrar la clave.
  - Solo se pueden obtener datos válidos de getpwnam(2) con euid=0 *(root)* si se utiliza `/etc/passwd.db` para almacenar las claves de acceso.

- Mantenimiento
  - El proyecto OpenBSD continúa en activo y, a pesar de sus acostumbrados problemas de financiación, lanza una nueva versión del sistema cada seis meses aproximadamente.
  - Entre dos versiones consecutivas del sistema se suele disponer de 6 a 8 parches de seguridad como resultado del proceso de auditoría continua del sistema. Estos parches se dan a conocer junto con el problema que corrigen a través de foros de discusión públicos como Bugtraq y `comp.security.unix`.
  - El sistema se puede actualizar en línea mediante ftp, web, ctm, o utilizando cualquiera de los repositorios CVS distribuidos en todo el mundo.

4.2 Plataforma de desarrollo

A partir de la instalación base de OpenBSD y del paquete de compiladores, podemos empezar a desarrollar nuestros proyectos en los lenguajes C, C++, Fortran 77, y Fortran 90. Se utiliza el compilador gcc de la Free Software Fundation, aunque en la distribución oficial se incluye también el compilador egcs como un paquete aparte.

Para desarrollar y probar aplicaciones Xwindow es conveniente instalar un administrador de ventanas con el que nos encontremos a gusto: el administrador de ventanas fwmn, que viene de serie con OpenBSD, no es precisamente el colmo de la amabilidad.

4.3 Servidor en Explotación

Los demonios que implementan los servicios de Internet más comunes se incluyen por defecto en la distribución base de OpenBSD. A partir de la versión 2.5 se incluye además el servidor web Apache preparado para utilizar SSL.

Todos los servidores desarrollados por el proyecto OpenBSD han sido comprobados en busca de fallos de seguridad; si el servidor no se ha desarrollado específicamente para OpenBSD, o no tiene control sobre su código fuente, se ejecuta en un entorno restringido para prevenir posibles problemas. Este es el caso de bind, o el servidor ftp.

Para obtener un rendimiento adecuado es necesario *afinar* la configuración del sistema (como en cualquier sistema operativo).

El único inconveniente que podemos tener es que OpenBSD no soporta todavía varios procesadores, algo que Freebsd y Linux manejan sin problemas desde hace tiempo.

4.4 Firewall

OpenBSD puede ofrecer un nivel de protección en una red comparable al ofrecido por cortafuegos comerciales. Incluye un mecanismo similar al *stateful-inspection* de Firewall-1.

La aplicación más común de OpenBSD consiste en utilizar dos o más máquinas configuradas como routers para crear redes virtuales privadas sobre IPSEC.

4.5 Administración de red

OpenBSD incluye de serie el programa netcat (*nc*). En caso de problemas con cualquier servidor siempre puedes utilizar el netcat para redirigir una conexión desde tu estación a otro host, etc...

Si necesitas una consola de administración segura para tu red de computadores, puedes instalar SSH en cada una de las máquinas y acceder a ellas desde tu consola de administración.

5 Conclusiones

Hemos visto cómo OpenBSD puede realizar las mismas funciones que cualquier sistema Linux, haciendo hincapié en los aspectos de seguridad en los que Linux es menos riguroso.

En la actualidad no hay tanto software disponible para OpenBSD como para otros sistemas como Linux, o FreeBSD; sin embargo, poco a poco, esta situación está cambiando. Hay compañías, como NFR, Network Associates, o Price Waterhouse, que se están tomando en serio este nuevo Sistema Operativo como plataforma de desarrollo de software, para administración de red, o bien como Firewall.

Tarde o temprano un administrador de Linux que desee dedicarse a profesionalemente a la administración de sistemas va a tener que hacerse cargo de más de un tipo de Unix. En este caso OpenBSD resulta ser una buena introducción al heterogéneo mundo de los sistemas Unix, además de una herramienta de trabajo útil y agradable; aunque nunca hay nada más agradable que el Unix con el que aprendiste.

6 Referencias

6.1 WWW

- `Daemon News`http://www.daemonnews.org/ Revista de información general acerca de sistemas BSD.
- `FreeBSD`http://www.freebsd.org/ Información sobre el Sistema Operativo utilizado por Yahoo!, BSD para el 386. Hay un mirror en españa en `http://www.es.freebsd.org`
- `NetBSD`http://www.netbsd.org/ BSD multiplataforma: alpha, atari, amiga, mips, etc...)
- `OpenBSD`http://www.openbsd.org/ BSD Orientado a la seguridad.
- `OpenBSD Explained`http://www.dayrom.com.au/ satyricon/
- `Network Flight Recorder`http://www.nfr.net/

6.2 News

- `comp.unix.bsd`news:comp.unix.bsd
- `comp.unix.bsd.misc`news:comp.unix.bsd.misc
- `comp.unix.openbsd.misc`news:comp.unix.openbsd.misc
- `comp.unix.openbsd.announce`news://comp.unix.openbsd.announce