Taller de Seguridad

Javier Fernández-Sanguino Peña
Debian GNU/Linux

En este documento se presentarán las actividades a realizar durante el Taller de Seguridad que se celebrará durante el Congreso de Hispalinux 2002.

¿Por qué un taller de seguridad? La realidad actual es que existe un riesgo muy elevado para cualquier sistema de información que está conectado (aunque sea momentáneamente) a cualquier otro sistema de información. Igualmente, los usuarios no son generalmente conscientes de los riesgos existentes ni de la forma de paliarlos. El objetivo del taller es aumentar el conocimiento de los asistentes en seguridad y, particularmente, en las médidas para mejorar la seguridad de sistemas basados en software libre.

No se tratarán, directamente, los conceptos clásicos de seguridad (teórica) como puedan ser los de confidencialidad, integridad, disponibilidad, y no repudio. Así, se dará por supuesto que el análisis de riesgos (paso previo imprescindible para cualquier acercamiento) ha sido realizado y que la política de seguridad está definida. Estos son pasos previos necesarios a la implementación de seguridad en sí y no son, realmente, abordados con software. El talle será, fundamentalmente, práctico y, por tanto, se centrará en las herramientas de software libre que ayudan a implementar la seguridad que previamente se haya definido.

Cuando se habla de utilizar software libre para implementar seguridad en sistemas no se habla, exclusivamente, de la utilización de software para implementar mecanismos de cifrado (ya sea asimétrico o simétrico) sino de herramientas para implementar la cadena completa de un ciclo de vida (en lo que a seguridad) se refiere de un sistema informático: protección (o prevención), detección, reacción (o respuesta) y recuperación. Evidentemente, es necesario herramientas para cubrir todos y cada uno de estos aspectos, no siendo útiles ninguno de ellos de forma aislada y debiendo combinarse para adaptarse a la política de seguridad.

El interés de utilizar, exclusivamente, herramientas de software libre dentro del taller no sólo nace del hecho puntual de que el congreso se celebre entorno a éste tipo de software sino por las ventajas ofrecidas en el ámbito de la seguridad informática de la utilización de software libre:

- El coste del software es reducido (podría decirse que nulo). Algo raro cuando se habla de software relacionado con la seguridad informática.

- Es posible auditar la implementación del software, minimizando la posibilidad de "puertas traseras" y fallos de seguridad derivados de una mala implementación.

- Las posibilidades derivadas de las licencias asociadas al software libre permiten que el software pueda ser adaptado según las necesidades del usuario (eliminando funciones no deseadas o incorporando nuevos mecanismos de protección, detección y reacción), arreglado cuando se descubran problemas (que lo son más graves en el mundo de la seguridad) y mejorado de forma que éste evolucione.

Evidentemente, la seguridad no es un producto, es un proceso (ésta es una máxima comúnmente olvidada por los fabricantes de productos). Los productos no tienen un fín en sí mismo sino que tienen que estar integrados dentro de una política coherente de seguridad. Política que una empresa podría desarrollar basándose en estándares como el ISO 17799 (anteriormente conocido como el British Standard 7799) o el RFC 2196. Sin embargo, también es cierto que, sin un adecuado conocimiento de las capacidades de protección pueden llegarse a diseñar políticas de seguridad cuya implementación práctica no sea posible con la tecnología actual.

El taller se desarrollará de forma práctica, realizando distintas tareas de todas las fases relacionadas con la seguridad que puedan afectar a un sistema informático. Así se mostrarán las fases de:

- Instalación y configuración. En este paso se mostrarán algunos de los conceptos básicos a tener en cuenta como son: determinación de la función del sistema, selección del software más adecuado a la tarea a realizar y mecanismos básicos de protección a implementar previos a la puesta en marcha.

- Bastionado (fortificación) del sistema, incluyendo la instalación de cortafuegos locales, adaptación del núcleo del sistema, compartimentalización del acceso de los servicios, revisión de la instalación, etc.

- Actualización de parches de seguridad. Este aspecto describirá la evolución natural de los sistemas operativos (afectados por el descubrimiento de problemas de seguridad) y los pasos a dar para solucionar los problemas de seguridad conocidos de antemano.

- Instalación de herramientas de monitorización del sistema y de detección de instrusos, describiendo las distintas herramientas disponibles para implementar mecanismos de detección y sus funciones.

- Utilización de herramientas de auditoría para la comprobación de la seguridad local y remota. Estas herramientas facilitan la revisión contínua del estado de seguridad y cumplimiento de la política de seguridad.

- Herramientas a utilizar en el caso de que el sistema sea comprometido y en aquellos casos en las que los análisis forenses formen parte del mecanismo de reacción.

Para ello, el ponente realizará el taller basándose en el sistema operativo Debian GNU/Linux y herramientas de seguridad de software libre incluídas en éste (y algunas que aún no lo están) como puedan ser:

- Bastionado: Bastille Linux, Makejail, jailer, (del núcleo) SElinux, grsecurity, openwall.
- Auditoría: Nessus, Tiger, Nikto, Whisker, John, Crack, Nmap, raccess, xprobe.
- Detección de intrusos: Snort, Tiger, ippl, chkrootkit, psad, portsentry.
- Monitorización de integridad: aide, integrit, tripwire, fcheck.
- Monitorización: logcheck, syslog-ng, ucd-snmp, fwlogwatch, fwctl
- Protección tcpwrappers (herramientas para generación de reglas para cortafuegos) fwbuilder, shorewall, firestarter, knetfilter, shorewall (cortafuegos proxy) zorp,
- Análisis forense: tct, strace, ltrace, fenris.

Evidentemente, la demostración práctica del funcionamiento de las herramientas dependerá del tiempo disponible durante el taller. Asímismo, hay ciertas herramientas que no serán tratadas en el taller. Como son las implementaciones de antivirus, sistemas de ficheros con journaling, implementaciones de túneles cifrados, herramientas de firma digital... que, por supuesto, también forman parte de una solución de seguridad.

Nota: Se recomienda a los asistentes que lleven sus propios equipos (preferiblemente portátiles) con tarjetas de red (la organización informará de las condiciones y métodos de acceso) para poder realizar estas mismas pruebas descargándose el software necesario del servidor instalado al efecto. No será necesario (pero sí aconsejable) que las distribuciones instaladas sean Debian GNU/Linux pudiéndose utilizar cualquier otra distribución de Linux o derivado de BSD.

El desarrollo del taller seguirá el acercamiento a la seguridad de sistemas mostrado en el http://www.debian.org/doc/manuals/securing-debian-howto/index.en.html#contents[Manual de Seguridad de Debian]

Referencias:

1. http://www.tldp.org/HOWTO/Security-HOWTO/index.html [Linux Security HOWTO]
2. http://www.tldp.org/HOWTO/Security-Quickstart-HOWTO/ [Security Quick-Start HOWTO for Linux]
3. http://www.debian.org/doc/manuals/securing-debian-howto/index.en.html[Debian Security Manual]
4. http://www.linuxsecurity.com/docs/colsfaq.html[comp.os.linux.security FAQ]
5. http://www.tldp.org/HOWTO/Security-Quickstart-HOWTO/ [Security Quick-Start HOWTO for Linux]
6. http://people.freebsd.org/~jkb/howto.html[FreeBSD security HOWTO]

7. http://www.susesecurity.com/faq/[SUSE security FAQ]

8. http://www.mandrakesecure.net/en/[Mandrake Security]

9. http://www.openbsd.org/security.html[OpenBSD Security]

10. http://www.dwheeler.com/oss_fs_why.html[Why Open Source Software / Free Software (OSS/FS)? Look at the Numbers!

11. Seguridad en UNIX y Redes, Antonio Villalón Huerta.

12. http://congreso.hispalinux.es/congreso2001/actividades/ponencias/ferrer/[El sistema operativo GNU/Linux y sus herramientas libres en el mundo de la seguridad: estudio del estado del arte.]