I Jornadas sobre Seguridad en GNU/Linux

Extensiones de seguridad en el kernel

Chema Peribáñez <chema@augcyl.org>

Seguridad tradicional de Unix

permisos
- grupos
- Trustees (ACL, lado cliente)

propietario/superusuario
- suid
- soltar los privilegios
- chroot

La flexibilidad: PAM
- módulos de autentificación
- módulos de cuentas
- módulos de cambio de clave
- módulos de sesión

¿dónde está el problema?

Un ataque tradicional:

- saltarse el cortafuegos
- obtener una cuenta local
- obtener la cuenta de root

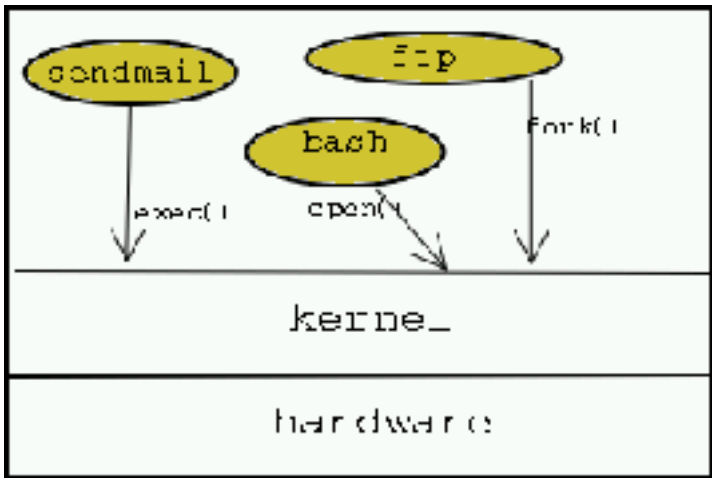
Un fallo en un programa, compromete todo

- desbordamiento de buffer
- seguridad basada en usuarios
- el root tiene demasiados privilegios
- herencia de privilegios

¿Se puede mejorar seguridad en Linux?

Modo supervisor, modo usuario

- los programas se ejecutan en modo usuario
- usan memoria paginada
- acceden a los recursos mediante llamadas al sistema
- las llamadas al sistema comprueban permisos



Por tanto "sólo" hay que cambiar dónde se comprueba EUID 0

MAC frente a DAC

Definición: existe una política de seguridad a la que está sujetos todos los usuarios, incluidos los administradores y que sólo el responsable de seguridad puede cambiar.

Conceptos claves:

- sujetos, objetos, etiquetas
- MAC y DAC pueden convivir

Varios modelos de políticas:

- MLS: Bell y La Padula
- Roles
- DTE

Implementaciones en Linux

Lomac (muy simple, dos niveles, script kiddies)

LIDS

- OpenWall

RSBAC

SELinux

Medusa

Un módulo de seguridad: LSM

- Sólo políticas restrictivas

Orange Book. CC (Common Criteria)

Trusted IRIX

LIDS: características (I)

Relativamente sencillo
- Engarde Linux y Debian

ACLs a nivel de ejecutables
- permisos de acceso,lectura,añadir,escritura
- tanto ficheros como árboles de directorios
- permite ocultar ficheros y procesos
- permiso para matar un proceso

ACLs por defecto no se heredan

parámetro de tiempo

dominios

LIDS: características (II)

capabilities
- por procesos
- detalle de puertos
- globales: sellado

detección de instrusiones
logs
- evita repeticiones
- puede enviar vía red

cambiar o no desde red

LIDS: funcionamiento

subjects: ejecutables

objects: ficheros, directorios, procesos, capab.

se usan inodos

configuración en /etc/lids

lidsadm

- Herramienta de línea de comandos
- similar a ipchains
- su propio password
- comandos para fijar configuración, clave, inodos
- comando para actualizar
- comandos para activar/desactivar

SELinux

Desarrollado por la NSA, SCC, Universidad Utha y NAI
Predecesor para Matcha (DTMatch, luego DTOS)
Multipolítica, se puede reiniciar en vivo
Arquitectura Flask

Muy actualizado. Primero en usar LSM
Nuevas llamadas al sistema
DTE, Roles, MLS

Enlaces

Kernel

- http://www.kernel.org/pub/linux/kernel/ Kernel oficial

MAC

- http://opensource.nailabs.com/lomac/
- http://lsm.immunix.org/ LSM (Linux Security Module)
- http://www.nsa.gov/selinux/
- http://www.lids.org/
- http://www.rsbac.org/
- http://medusa.terminus.sk/

Enlaces (II)

Parches

- http://www.openwall.com/
- http://www.grsecurity.net/
- http://trustees.sourceforge.net/
- http://www.solucorp.qc.ca/miscprj/s_context.hc

Miscelanea

- http://www.engardelinux.com/
-

http://linuxtoday.com/news_story.php3?ltsn=2001-04-09-007-20-

- http://www.linuxsecurity.com/
- http://lwn.net/ (seguridad y kernel)