Bisoños Usuarios de Linux de Mallorca y Alrededores | Bergantells Usuaris de Linux de Mallorca i Afegitons

Kernel Linux − Aumentando la seguridad del sistema

Por **Carlos Cortes Cortes**, ***carcoco*** (http://bulmalug.net/~carcoco/)
Creado el 25/11/2001 18:15 y modificado por última vez el 25/11/2001 18:15

Existen multitud de proyectos orientados a aumentar la **seguridad** del ya de por sí (aunque parece que no suficiente) **seguro sistema operativo Linux**, la mayoría son mejoras y parches del propio **kernel** ...

Como la practica totalidad tienen **licencia GPL**, no sería de extrañar que las mejoras más significativas fueran paulatinamente absorbidas y añadidas al propio **kernel**, de forma que las tendriamos de serie en el núcleo , tal y como está ocurriendo con los sistemas **journalist**: reiserfs, ext3 ya incluidos y XFS, JFS que se incluirán muy pronto.

Aquí teneís la relación de estos proyectos:

- **Medusa DS9**
- **NSA Linux SE**
- **Linux grsecurity**
- **Linux Intrusion Detection System**
- **HP secure OS software for Linux**
- **Rule Set Based Access Control for Linux**
- **Capsel**
- **OpenWall (Kernel 2.2.x)**
- **HAP−Linux Kernel Patches (Kernel 2.2.x)**
- **VXE − Virtual eXecuting Environment**
- **...**

Medusa DS9
Medusa DS9 is used to increase Linux's security. It consists of two major parts, Linux kernel changes and the user−space daemon. Kernel changes do the monitoring of syscalls, filesystem actions, and processes, and they implement the communication protocol. The security daemon communicates with the kernel using the character device to send and receive packets. It contains the whole logic and implements the concrete security policy. That means that Medusa can implement any model of data protection; it depends only on configuration file, which is in fact a program in the internal programming language, somewhat similiar to C.
http://medusa.terminus.sk/(1)

NSA Linux SE
NSA Security−enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control architecture into the major subsystems of the kernel. It provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications. It includes a set of sample security policy configuration files designed to meet common, general−purpose security goals.
http://www.nsa.gov/selinux/(2)

Linux grsecurity
*grsecurity is a set of security patches for Linux 2.4 that contain all the features of Openwall and HAP−Linux, among many other patches for 2.2, and other OSes. It features the Openwall non−executable stack, PaX, the Oblivion ACL system, /proc restrictions, chroot restrictions, linking and FIFO restrictions, exec and set*id logging, secure file descriptors, trusted path execution, randomized IP IDs, randomized PIDs, randomized TCP source ports, altered ping ids, randomized TTL, better IP stack randomness, socket restrictions, fork−bomb protection, sysctl support on nearly*

all options, secure keymap loading, stealth networking enhancements, signal logging, failed fork logging, time change logging, and others.
http://www.grsecurity.net/(3)

LIDS
The Linux Intrusion Detection System (LIDS) is a patch which enhances the kernel's security by implementing a reference monitor and Mandatory Access Control (MAC). When it is in effect, chosen file access, all system/network administration operations, any capability use, raw device, memory, and I/O access can be made impossible even for root. You can define which programs can access specific files. It uses and extends the system capabilities bounding set to control the whole system and adds some network and filesystem security features to the kernel to enhance the security. You can finely tune the security protections online, hide sensitive processes, receive security alerts through the network, and more.
http://www.lids.org/(4)

hp secure OS software for Linux
HP announces a secure server platform for Linux as an enhancement to the HP Netaction software suite. The new product, HP Secure OS Software for Linux, will help businesses secure their Linux environments by offering intrusion prevention, real−time protection against attacks, and damage containment. HP is first to market with this business−critical security solution for Linux. HP Secure OS Software for Linux provides high reliability, performance, availability, flexibility and scalability. Additionally, it is easy to install and manage, making it attractive to businesses that don't have large IT organizations. HP Secure OS Software for Linux provides users with a secure environment that offers intrusion prevention, real−time attack protection and damage containment.:

- Prevention: A virtual compartment prevents unauthorized communication between programs, networks and files. This feature offers users the ability to host different company−sensitive applications and data on the same machine.
- Detection: The auditing feature detects hacking attempts.
- Containment: If the system is penetrated, the containment feature locks the program, thereby preventing damage to internal systems and preventing the system from launching other attacks.
- Installation: HP Secure OS Software for Linux is easy to install during a standard Linux installation.

http://www.hp.com/security/products/linux/(5)

Rule Set Based Access Control (RSBAC) for Linux
Rule Set Based Access Control (RSBAC) is an open source security extension for current Linux kernels. It is based on the Generalized Framework for Access Control (GFAC) by Abrams and LaPadula and provides a flexible system of access control based on several modules. All security relevant system calls are extended by security enforcement code. This code calls the central decision component, which in turn calls all active decision modules and generates a combined decision. This decision is then enforced by the system call extensions.
http://www.rsbac.org/(6)

Capsel
Capsel is a Linux kernel module designed to increase system security with many useful features. It works with Linux capabilities and allows you to decrease number of SUID binaries and root−privileged daemons on a system. It performs additional security checks before executing new binaries to prevent users from taking control of their execution. It also protects against the latest ptrace kernel bugs.
http://cliph.linux.pl/capsel/(7)

VXE − Virtual eXecuting Environment
Main problem with UNIX security is that superuser can do with system anything he wants. There are programs (daemons) which work with superuser privilegies, for example popd, sendmail, and accessible from network (Internet/Intranet). There could be bugs in any program, so intruder connects to such programs via network, exploit existing bugs in it and get a control over all host. VXE (Virtual eXecuting Environment) protects UNIX servers from such intruders, hacker attacks from network and so on. It protects software subsystems, such as: SMTP, POP, HTTP and any other subsystem, already installed on the server. There is no need to change configuration of existing software − just PROTECT it. VXE is FREE for non−commercial use.
http://www.intes.odessa.ua/vxe/(8)

Kernel 2.2

OpenWall
"Owl" (or "Openwall GNU//Linux"; please, note that only the "O" is capitalized in either case) is a security−enhanced operating system with Linux and GNU software as its core, compatible with other major distributions of GNU/*/Linux. It is intended as a server platform.*
http://www.openwall.com/Owl/(9)

HAP−Linux Kernel Patches
HAP−Linux is a collection of my favorite security−related patches that are floating around, plus a few non−security, but "required" patches to the 2.0.x and 2.2.x Linux kernels. The current patches are against 2.2.20 and 2.2.19. There was/still is a 2.0.38 version, but it's frozen; I won't release another 2.0.x version except for drastic bug−fixing. Anyone still running 2.0.x should be at 2.0.39 at least due to the execve/ ptrace race fixes; email me to prod me into releasing 2.0.39−hap if you need it, or I'll never get around to it since I have no such boxes any more.
http://www.theaimsgroup.com/~hlein/hap−linux/(10)

Por último comentar la existencia de **TrustedBSD**, un proyecto cuyo objetivo es mejorar la segidad de los sistemas **FreeBSD**:
http://www.trustedbsd.org/(11)

−−
Carlos Cortes(aka carcoco)
http://bulmalug.net/todos.phtml?id_autor=132 (12)

Lista de enlaces de este artículo:

1. http://medusa.terminus.sk/
2. http://www.nsa.gov/selinux/
3. http://www.grsecurity.net/
4. http://www.lids.org/
5. http://www.hp.com/security/products/linux/
6. http://www.rsbac.org/
7. http://cliph.linux.pl/capsel/
8. http://www.intes.odessa.ua/vxe/
9. http://www.openwall.com/Owl/
10. http://www.theaimsgroup.com/~hlein/hap−linux/
11. http://www.trustedbsd.org/
12. http://bulmalug.net/todos.phtml?id_autor=132

E−mail del autor: carcoco _ARROBA_ grupobbva.net
Podrás encontrar este artículo e información adicional en: http://bulmalug.net/body.phtml?nIdNoticia=1023