Seguridad y Linux

David Fernández Vaamonde
davidfv@gpul.org

III Jornadas sobre el sistema operativo Linux

Universidad de La Coruña
Facultad de Informática

Guión

- Introducción
- Seguridad y software libre
- Seguridad y distribuciones
- Seguridad y software
  - Seguridad en el operativo
  - Firewalls
  - Sistemas de deteccion de intruso
  - Software de auditorias sobre equipos
  - Criptografía
- Linux como asegurador de sistemas heterogeneos.
- Grandes proyectos de seguridad en Linux

Introducción

- Seguridad informática:
  - Muy importante a dia de hoy
  - Aumenta en importancia con la interconexión de los sistemas
  - Aspecto importante en cualquier implantación y desarrollo
    - Por tanto también en software libre y Linux
    - El software libre tiene características que lo hacen especial para la seguridad.

Seguridad y Software Libre (I)

Linux y sus aplicaciones son Software libre:

- Han de ser distribuidas con el código
  - Fuente al alcance de quien quiera
- Puede ser modificado libremente
  - Se distribuyen las modificaciones con la misma licencia (GPL).
  - Se puede modificar para realizar funciones específicas.

Seguridad y Software libre (y II)

Derivado de estas dos características:

- Acceso al código fuente:
  - Búsqueda de vulnerabilidades (Auditoría de código)
  - No hay "troyanos" o "puertas traseras"
  - Crackers -> Pruebas de caja negra
  - Evita "security through obscurity"

Seguridad y Software libre (y III)

- Se puede modificar libremente:
  - Rapida aparición de parches ante fallos.
  - Mucha gente lo usa, y mucha gente lo puede arreglar
  - No se dejará de dar soporte
  - Solución de muchos productos comerciales:
    - "Service Pack"

Seguridad y distribuciones

- Kernel+Paquetes de software+Modos de instalación de todo ello
- Paquetes software: .deb, .rpm
- Principal canal de difusión de linux
- Se encuentran en CDs y pueden ser descargadas de internet
- Han de incluir algún tipo de seguridad.

Seguridad y distribuciones (y II)

Paquetes .deb (Debian, CorelLinux, Progeny...):

- Firmado con claves PGP (GPG) de los paquetes de código fuente
- Futuro firmado con PGP(GPG) de paquetes de binarios.
- Sumas MD5 para los ficheros
- ISOS firmadas con PGP(GPG)
- FTP con actualizaciones de seguridad
  - ftp://security.debian.org
- Informes y seguimiento de fallos
  - http://bugs.debian.org

Seguridad y distribuciones (y III)

Paquetes .rpm (RedHat, Mandrake, SuSe...):

- Firmado de todos los paquetes con PGP(GPG)
  - --sign, --resign, --addsign
- Sumas MD5 de todos los ficheros a manejar
  - El del primer fichero instalado
  - El del fichero actual
  - El de la posible actualización
- Informes de todos los fallos en listas de correo y webs

Software y seguridad en Linux

- Seguridad en el propio sistema operativo
  - Sistemas de permisos (ficheros, IPCs)
  - Sistema de logs y accounting
  - Mecanismos genéricos de autenticación: PAM
  - Seguridad en el kernel:
    - Parches GRSEC
    - Sistemas de ficheros criptográficos
    - ...

Firewalls

- ipfwadm (2.0.X)
- ipchains(2.2.X)
- iptables(2.4.X)
  - Filtrado por puerto, direccion, protocolo,flags tcp,mac
  - Estado temporal de las conexiones: limit
  - Filtrado por UID y GID del generador de paquetes: owner
  - Filtrado por estado de las conexiones: state
  - Filtrado por TOS y TTL
  - NAT en Origen y Destino
  - Muy modular y extensible

Firewalls (y II)

Carencia en los firewalls linux libres:

- Analisis de protocolos

Comienzan a surgir alternativas:

- ZORP
  - Examina protocolos usuales:FTP, HTTP, TELNET...
  - Gran herramienta junto con iptables.

Sistemas de detección de intrusos

- SNORT
  - Basado en red
- LogCheck
  - Basado en logs
- AIDE
  - Basado en sistema de ficheros
- FCHECK, COAST IDS, SHADOW...

Software de auditorías sobre equipos

- Nessus
  - Modelo cliente/servidor
  - Pasa pruebas de vulnerabilidades (actualizables)
  - Lenguaje de scripting para programar vulnerabilidades (NASL)
  - Informes en muchos formatos, muchos clientes.
  - El propio programa es seguro.
- Nmap
  - Scanner de puertos
  - Escanear redes de máquinas
  - Muchos tipos de scaneos
- Crack/Jhon the ripper
  - Ataques con diccionario

Software de auditorías sobre equipos (y II)

- Whisker
  - Escaneo de vulnerabilidades habituales en CGIs
  - libwhisker (perl) -> Nikto, Formaline...
- TIGER
- SARA
- SAINT
- ...

Criptografía

- GPG o PGP
  - Encriptación con llave publica
- SSH
  - Secure Shell
  - Sesiones interactivas y transmisiones de ficheros seguras
  - Tuneles encriptados

Criptografía (y II)

- FreeSwan
  - Parche para el kernel
  - Implementación de IPSec
  - VPN (Redes Privadas virtuales)
- Sistemas de ficheros criptográficos
  -
  - Parches para el kernel
  - CryptoAPI
  - PPDD
  - CFS

Linux como asegurador de Sistemas

Linux da seguridad a otros sistemas:

- Samba
  - Control de ficheros en el server
    - Control de virus
    - Control de corrupcion de archivos
    - Sistema CIFS robusto
- Firewall
  - Permite control de la red
  - Protege sistema internos más "vulnerables"

Linux como asegurador de Sistemas (y II)

- Filtrado
  - Filtrado de virus en correos (AMAVIS, mailscanner,sanitizer..)
  - Filtrado de virus en proxies
- ...

Grandes proyectos de seguridad

- Trinux
  - Minidistribución:
    - Auditoría de seguridad
    - Equipos heterogéneos
    - ...
  - Comiënzan a surgir distribuciones live
  - Modificación en base a software libre
- GRSEC
  - Agrupaciones de parches de seguridad del kernel
  - Añaden comportamiento seguro al kernel
  - Modificacion de software libre (el kernel de linux)

Grandes proyectos de seguridad (y II)

- LSAP
  - Linux Security Audit Project
  - Filosofía "OpenBSD"
  - Auditoría de código -> Software libre
  - Gracias a la visibilidad del código.
- Denominador común que los hace todos posibles:

¡ Son Software Libre !

The End

Algunas URLs de seguridad y Linux:

- www.securityfocus.com
- www.linuxsecurity.com
- www.nessus.org
- www.nmap.org
- www.jollycom.ca/iptables-tutorial/iptables-tutorial.html
- www.amavis.org
- www.openantivirus.org
- www.debian.org ;)