Seguridad y Linux
(v3.0)

David Fernández Vaamonde
davidfv@alfa21.com

IV Jornadas sobre el Sistema Operativo Linux
Universidade da Coruña
Facultade 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
- Un ejemplo práctico: Seguridad doméstica mínima
- Consejos de seguridad en servicios de red y Linux.
- Esqueleto de una intrusión.
- 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)

Una 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**
- **...**

Honey Pots

- Chroot clásico
- User Mode Linux como HoneyPot
- Productos "prefabricados"
  - Tiny Honey Pot
  - Labrea
  - IISEmulator

Criptografía

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

Criptografía (y II)

- **FreeSwan (o IPsec nativo)**
  - **Parche para el kernel**
  - **Implementación de IPSec**
  - **VPN (Redes Privadas virtuales)**
- **OpenVPN**
  - **Sistema servidor de tuneles muy sencillo.**

Criptografía (y III)

- **Sistemas de ficheros criptográficos**
  - **Parches para el kernel**

CryptoAPI

  - **PPDD**
  - **CFS**

Analisis Forense

- **The Coroners Kit**
  - **Lazarus, urm, inode-cat, pcat.**
- **SleuthKit+Autopsy**

Un caso práctico

Seguridad mínima o doméstica con Linux

- **Caso práctico de protección de un ordenador doméstico con Linux y conectado a internet**

- **Se podría tomar como una metodología sencilla de seguridad.**

Un caso práctico (y II)

Pasos a dar:

- **¿Qué tenemos activo en el sistema?**
  - **Examinar /etc/inetd.conf**
  - **Usar netstat: netstat -ltu**
  - **Usar nmap desde fuera: nmap -sU -P0 maquina**
  - **Usar ps: ps aux**
- **Eliminar todo lo superfluo**
  - **Comentar en inetd.conf**
  - **Desinstalar paquetes que no se usan**
  - **Filtrar todo lo posible.**

Un caso práctico (y III)

- ¿Queremos filtrar algo?
  - Sencillo: tcpwrappers
    - host.allow, host.deny
    - Solo servidos por inetd
  - Más elaborado: firewall (iptables)
    - Política por defecto (-P) denegar todo.
    - Realizar aperturas selectivas

Un caso práctico (y IV)

- ¿Que versiones tenemos?
  - Ordenador propio:
    - Lista de paquetes
    - uname -a
  - Ordenador externo:
    - nmap -O -sV maquina
    - telnet
  - ¡Actualizar a las últimas versiones!

Consejos de seguridad en servicios de red

Consejos generales:

- **Uso de SSH y comunicaciones encriptadas:**

Previene el "sniffing"

- **Uso de firewalls que limiten los servicios:**
  - **Denegación por defecto**
  - **Políticas lo más estrictas posibles sin asfixiar.**
- **Uso de servicios actualizados (¡Vital!).**
- **Revisión habitual de logs.**

Consejos de seguridad en servicios de red (y II)

Servidor web: Apache

- **Mayor peligro: Scripts (CGI, PHP...)**
  - **Ejecutar como un usuario normal (no root)**
  - **Examinar el código con detenimiento:**
    - **Prevenir ejecuciones en el sistema**
    - **Prevenir inyección SQL**
    - **Prevenir accesos a ficheros.**
- **Protección del arbol web.**
  - **No situar en el path ficheros de claves.**
- **Uso de encriptación: SSL, Certificados.**
- **No permitir "browsing" (Indexes)**
- **Ejecutarlo en una DMZ**

Consejos de seguridad en servicios de red (y III)

Servidor DNS: Bind

- **Intentar no ejecutarlo como root.**
- **Posible ejecución en un chroot.**
- **No permitir transferencias de zona ("zone-transfer")**
- **Limitar las consultas al servidor ("allow-querys")**
- **Filtrar con firewall.**

Consejos de seguridad en servicios de red (y IV)

Servidor de correo: Postfix, Sendmail, Qmail, Exim

- **Limitar el relay de correo (SPAMSPAMSPAM!)**
- **Limitar tamaños de correo y máximo de conexiones (Evita DoS)**

Consejos de seguridad en servicios de red (y V)

Servidor de FTP: (wuftp, proftp)

- **Intentar correr en un chroot y sin permisos de root.**
- **Limitar ftps anónimos en lo posible.**
- **Limitar uploads si es posible.**
- **Establecer filtros en las acciones a ejecutar (limite de caracteres, etc étera).**

Consejos de seguridad en servicios de red (y IV)

Resumen

- Dar los mínimos permisos sin quitar funcionalidad
- Actualizar a las últimas versiones
- Backup, Backup, Backup...

Esqueleto de una intrusión:

- 1) Búsqueda de puertos abiertos (escaneo de puertos)
  - Solución: Detección de intrusos (SNORT, LogCheck), Firewall (iptables)
- 2) Intento de "explotar" una vulnerabilidad
  - Solución: Detección de intrusos, actualización periódica.
- Si se ha conseguido penetrar en el sistema:
- 3) Puertas traseras, loggers o rootkits para conseguir contraseñas y asegurarse el acceso.
  - Solucción: Detectores de rootkits (chkrootkit), Pruebas de integridad de ficheros (AIDE), Criptografía...
- 4) Saltos a otras máquinas.

Ejemplo de una intrusión reciente:

- **Compromiso de algunos servidores Debian:**
  - **Espionaje de la comunicación para obtener una password local.**
  - **Explotan un fallo del kernel (do_brk) y obtienen root en la máquina.**
  - **Se instala un rootkit para velar la intrusión (suckit)**
- **Tratamiento desde Debian:**
  - **Se detecta la intrusión (AIDE, Oops del kernel)**
  - **Se aislan los servidores y se realizan copias de los discos a fichero.**
  - **Se analizan las copias dando con la vulnerabilidad.**
  - **Se anuncia la vulnerabilidad y los pasos dados en un ejemplo de claridad.**

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 sistemas internos más "vulnerables"**
    - **Firewall de separación en DMZ**
    - **Bastión hosts**
    - **...**

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**
    - **...**
  - **Comienzan 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.**

- **Honeynet Project**
  - **Modus operandi de blackhats**
  - **Herramientas libres:**
    - **Snort (Detector de intrusos)**
    - **Sebek (Modulo del kernel)**
    - **Bash Path (Modificación de Bash)**
  - **Gracias a posibilidad de modificación.**

Grandes proyectos de seguridad (y III)

- ¿Necromantux?
  - Distribución live basada en Metadistros
  - Añade funciones de seguridad en una live:
    - Analisis de tráfico de red (iptraf, sniffit)
    - Funcionamiento como firewall (iptables)
    - Detección de rootkits (chkrootkit)
    - Auditoria de red (nmap)
    - Comprobación de integridad
    - Servidor de VPNs (OpenVPN, IPsec nativo)
    - Analisis Forense (tct)
  - Futuras funcionalidades
    - ¿Antivirus? (Clamav)
    - HoneyPot (TinyHoneyPot, labrea, iisemulator)
  - Todo productos de software libre.

Conclusión

- La seguridad deriva del conocimiento del sistema
- Hemos de estar actualizados
- Mayor problema de seguridad: Inexistencia de backups
- Un sistema es potencialmente inseguro
- En Linux hay muy buenas herramientas de seguridad, y proyectos prometedores (hasta Necromantux ;))
- Hay un 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**
- **project.honeynet.org**
- **www.tracking-hackers.com**
- **www.snort.org**
- **www.amavis.org**
- **www.davidfv.net/ponencias/**
- **www.debian.org ;)**

¡Gracias por asistir!