Taller de Seguridad

Securizando un servidor

Daniel Marcos Martín

GUL UC3M

04/03/2010

Parte I

Introducción

Justificación

¿Es necesario securizar una máquina?

- ¿A quién le interesa mi máquina?
- ¿Esfuerzo?
- ¿Dinero?
- ¿Número y tipo de ataques?

Tipos de ataque

- Locales / Remotos
- Automáticos
  - Poca cualificación (en general)
  - Fáciles de defender
- Dirigidos
  - Alta cualificación
  - Más dificiles de defender

Introducción

Pasos a seguir

- Diseño
- Actualización del sistema
- Reducción de la superficie de ataque
- Securización de las comunicaciones
- Protección frente a ataques locales
- Cuando todo falla

Parte II

Diseño

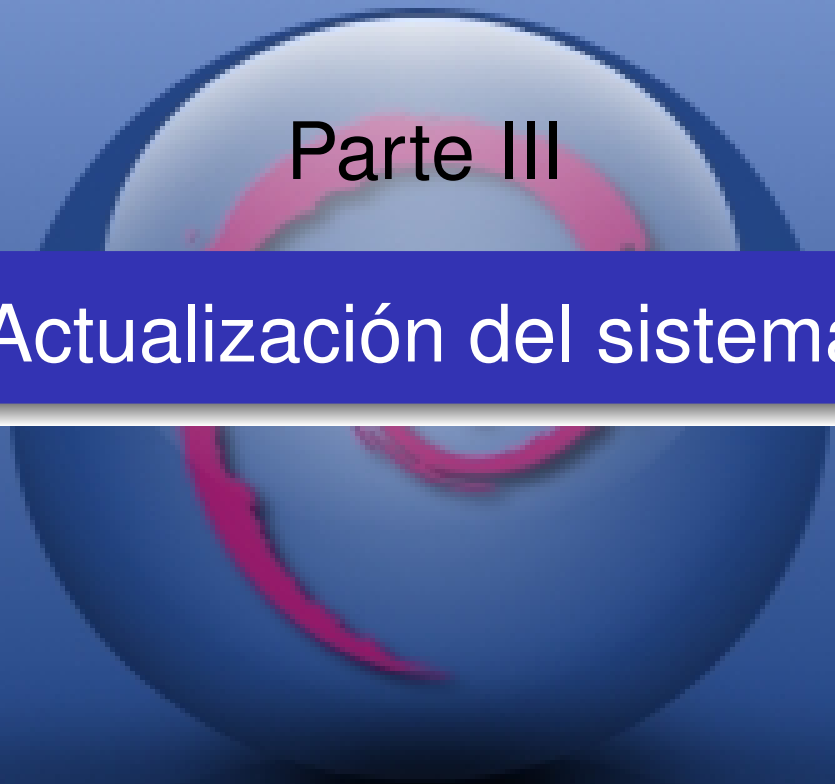
Diseño

Elección del sistema operativo

- Windows / Linux / FreeBSD
- Distribución
  - Debian
  - Ubuntu
  - Fedora
  - etc.
- Versión
  - stable
  - unstable
  - testing

Elección de los servicios

- Sólo los imprescindibles
- ¿En qué máquina?



Parte III

Actualización del sistema

Actualización del sistema

Mantener el sistema actualizado

- Recibir notificaciones
- System-icon-notifier
- cron-apt
  - Recibir correo cuando hay notificaciones
  - Descarga actualizaciones
  - Tarea programada
  - Disponible en Debian (herramientas similares en otros sistemas)

Mantenerse informado

- Contramedidas hasta que salga la actualización
- Listas de correo genéricas
  - una-al-día
  - full-disclosure
- Listas de correo específicas de cada distribución

Parte IV

Reducción de la superficie de ataque

Reducción de la superficie de ataque

Servicios

- Procesos ejecutándose
  - ps auxw
- Puertos abiertos
  - netstat -nlp
  - nmap, nessus
  - cups, ip6tables

Permisos

- Archivos con suid y sguid
  - find / -type f \(-perm -4000 -o -perm -2000 \) -exec ls -l {} \;
- Permisos en directorios
  - rw para otros y todos
  - find / -type d \(-perm -g+w -o -perm -o+w \) -not -perm -a+t -exec ls -lad {} \;
- Aplicaciones propias

Parte V

Filtrado de las comunicaciones

Securización de las comunicaciones

Cortafuegos

- Filtrar conexiones entrantes
- Filtrar conexiones salientes (troyanos)
- Evitar escaneo de puertos (router)
- Iptables
  - Por defecto no permitir nada
  - HTTP (apt-get), IMAP(cron-apt), etc.
- Interfaz gráfica para Iptables
  - FireStarter
  - UFW / GUFW

Port Knocking

- Puertos cerrados
- Se abren los puertos con combinación

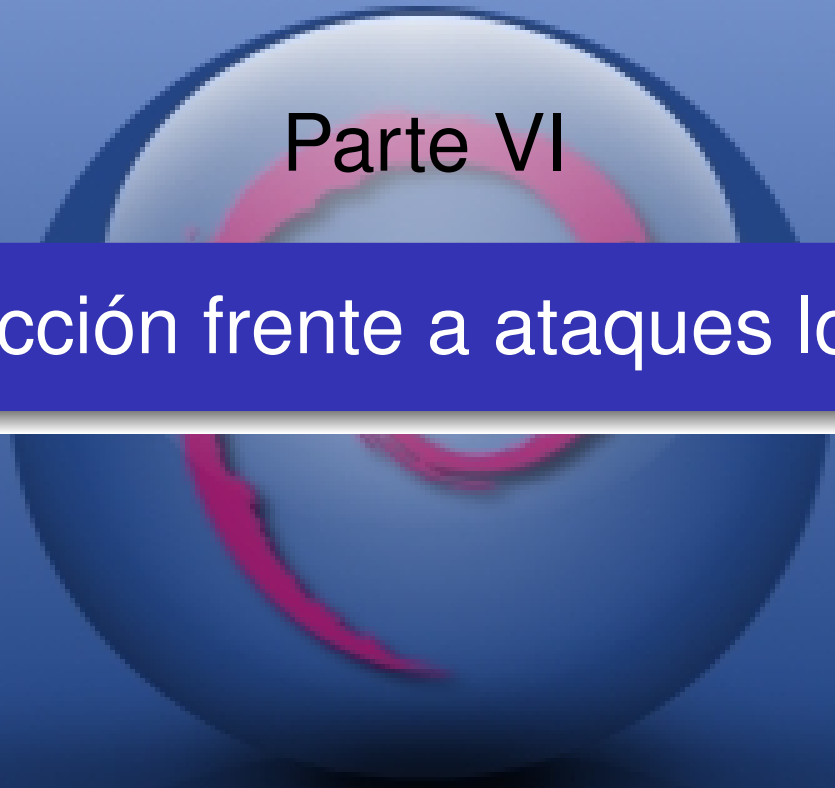
Securización de las comunicaciones

IDS

- Snort
  - Monitoriza las comunicaciones
  - Reglas para filtrar/avisar
  - Otra máquina, router (Linksys)

HIDS

- Host Intrusion Detection System
  - Monitorizar cambios en archivos importantes
    - /etc/passwd
    - Binarios del sistema
  - Detectar ataques desde otros hosts (combinado con IDS)
  - Controlar el uso de recursos
  - Buscar troyanos, rootkits, etc.
  - Guardar logs en servidor remoto
  - Dificil proteger ataques via web
    - shells en php



Parte VI

Protección frente a ataques locales

Protección frente a ataques locales

Protección frente a rootkits

- rkhunter
  - rkhunter -c
  - rkhunter -update
- chkrootkit

Evitar elevación de privilegios

- Ninja
  - Detecta cuando un proceso se ejecuta con permisos que no debería
  - Whitelist
  - Detecta cuando un proceso se ejecuta con uid de root

Protección frente a ataques locales

Entornos restringidos

- chroot
  - Entorno restringido para los usuarios
  - Apache, bases de datos, ftp
  - Usuario restringido a su home
  - No puede navegar por el sistema de archivos

Parte VII

Todo en uno

Todo en uno

Bastille

- Securizar sistema entero
- Conjunto de scripts
- Configuración mediante diálogos

SELinux

- Módulos de seguridad para el núcleo de Linux

Parte VIII

Cuando todo falla

Cuando todo falla

Logs

- En servidor remoto
- Si se guarda en local *only append*
  - chattr +a /var/log/secure

Análisis Forense

- Montar el sistema como sólo lectura
- Realizar copia del sistema atacado
- Analizar copia realizada

Parte IX

Referencias

Enlaces

Referencias

- http://www.chkrootkit.org/
- http://www.netfilter.org/
- https://help.ubuntu.com/community/Security
- http://www.debian.org/doc/manuals/securing-debian-howto/index.en.html
- http://www.gentoo.org/doc/en/security/security-handbook.xml