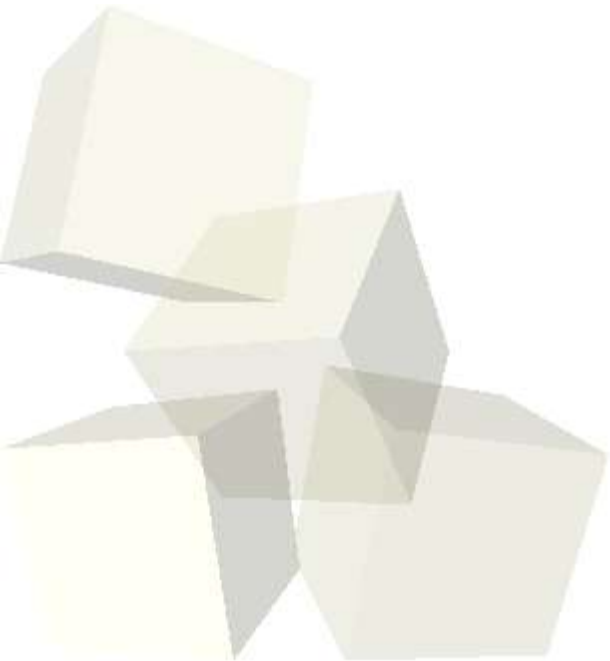
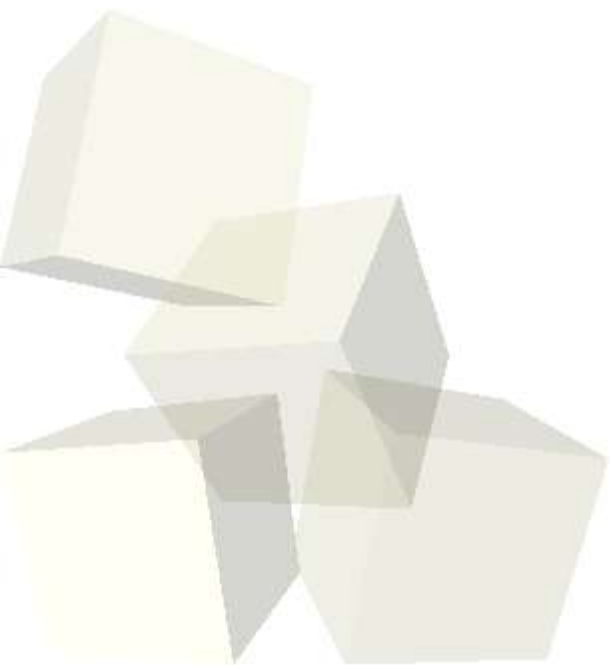


Seguridad y Linux



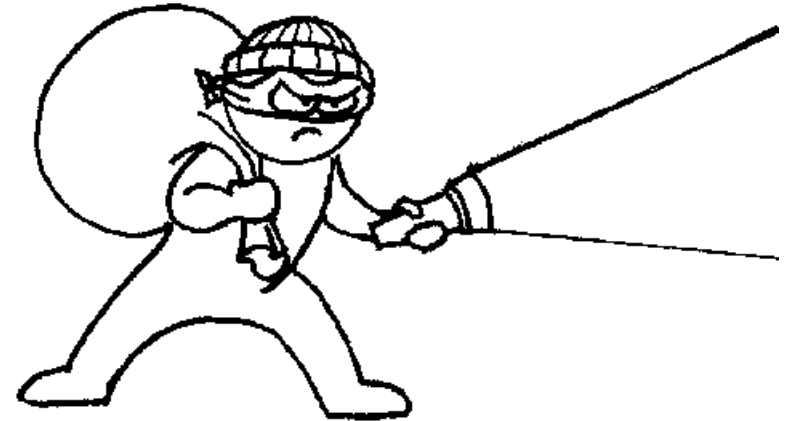
- La seguridad no es un problema técnico
- Un sistema no es seguro por si mismo
- Como en una cadena, un sistema es tan seguro como su eslabón más débil



- Defectos de diseño
 - ◆ Acceso a recursos sin restricción
 - ◆ Seguridad por ocultamiento
 - ◆ Diseños monolíticos de aplicaciones críticas
- Errores de programación
 - ◆ buffer overflows
 - ◆ scripting pass through



- Acceso a información
 - ◆ cookies
 - ◆ trafico de red
 - ◆ archivos
- Acceso a niveles de privilegio mayores
- Control total de la máquina



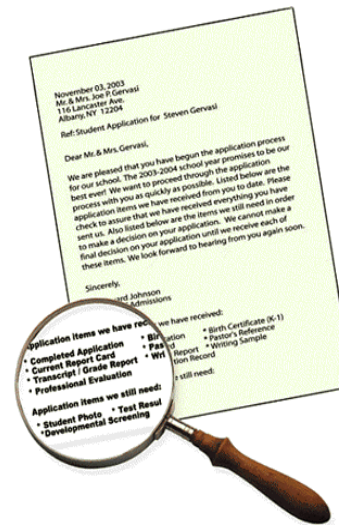
- Mala selección de passwords
- Aplicaciones con defectos instaladas
- Servicios con defectos publicados
- Configuraciones por omisión poco seguras
- Puertas traseras que “nadie conocerá”



- Puede garantizar que cuenta con un determinado nivel de seguridad
- El código abierto es mas fácil de auditar para alguien interesado en el tema
- No es necesario esperar a que “alguien haga algo” para solucionar un problema
- Todo esto NO es suficiente

- Una distribución es un conjunto de aplicaciones
- Cada aplicación está compuesta por paquetes
- Cada distribución tiene una empresa y/o comunidad tras ella:
 - ◆ Debian
 - ◆ Ubuntu
 - ◆ SuSE
 - ◆ RedHat

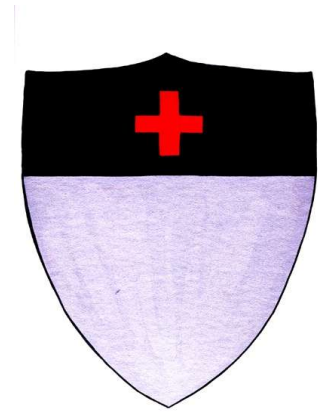
- Los paquetes se auditan y corrigen en forma independiente
- Las correcciones se publican tan pronto como sea posible
- La instalación de paquetes corregidos se puede automatizar



- Cada paquete se encuentra en una versión específica
- Las distribuciones ocupan distintos criterios para seleccionar versiones
 - ◆ RedHat EL/Fedora/Rawhide
 - ◆ Debian: stable, testing, experimental
 - ◆ Ubuntu: stable, development
- Las versiones estables ofrecen versiones por varios años, a las que se aplican backports de las correcciones

- Uso de mecanismos de protección del hardware:
 - ◆ kernel corre en ring 0
 - ◆ el resto corre en user space
 - ◆ bit NX
- Sistema de archivos con atributos de seguridad
- Restricciones para publicar servicios TCP

- Exec Shield
 - ◆ Desarrollado por RedHat
 - ◆ Permite evitar buffer overflows
 - ◆ Usa bit NX o emulación en donde no está soportado
- Security Enhanced Linux (SELinux)
 - ◆ Desarrollado por National Security Agency(NSA)
 - ◆ Evita que fallas en las aplicaciones o en el kernel comprometan el sistema



- Si hubiese mas gente usando Linux, sería más inseguro
 - ◆ La seguridad es independiente de los usuarios
- El código abierto facilita encontrar defectos
 - ◆ Se encuentran mas defectos aplicando fuerza bruta
- En Linux hay Virus
 - ◆ Difícil propagación
 - ◆ Requieren cooperación
 - ◆ Los que existen son inviábiles

- Como las encuestas, todo depende de quien los financia
- Normalmente presentan una visión parcial de las variables de seguridad
 - ◆ No consideran nivel de peligrosidad
 - ◆ No consideran facilidad de abuso
 - ◆ No consideran rapidez de corrección
- Comparan los miles de paquetes de un sistema Linux, frente a las decenas de “otros sistemas”

Preguntas

