Seguridad en Sistemas Informáticos (SSI)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

Laboratorio: AIDE

Carlos Pérez Conde

Departament d'Informàtica

Escola Técnica Superior d'Enginyeria

Universitat de València

AIDE

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Objetivos:**
  - aprender a detectar modificaciones no autorizadas en un sistema protegido con *aide*
- **Actividades a realizar**
  - Arrancar “base.example.net” y copiar /etc en /tmp/etc (cp -a /etc /tmp/etc).
  - Copiar el fichero de configuración original (/etc/aide.conf) en /root
  - Configurar AIDE (/etc/aide.conf) para que detecte cualquier tipo de alteración en /tmp/etc e ignore cambios en cualquier otra parte del sistema
  - Inicializar la base de datos de AIDE
  - Mover la base de datos al lugar oportuno
  - Comprobar la integridad de /tmp/etc (no deberían aparecer cambios)

AIDE (II)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Actividades a realizar (cont.):**
  - Intercambiar el ordenador con otro grupo
  - Realizar diferentes tipos de acceso sobre el directorio /tmp/etc (lectura, modificación, sustitución de ficheros...) anotando qué se hace
  - Volver al ordenador original
  - Comprobar la integridad de /tmp/etc
  - Identificar los cambios realizados por el otro equipo
  - Basándose en esta prueba previa, preparar un fichero de configuración para un servidor web con las siguientes características:
    - el directorio en el que se alojan las páginas web es /var/www
    - existe un administrador del web con cuenta propia a la que accede con SSH
    - no existen más cuentas
    - no se ofrecen servicios adicionales (sólo HTTP y SSH)