Trabajo Fin de Carrera

Securización de sistemas Linux

Alumno: Miguel Montero Rodríguez

Profesor: Helena Rifá Pous

Consultor: Jordi Massaguer Pla

Securización de sistemas Linux

INTRODUCCIÓN

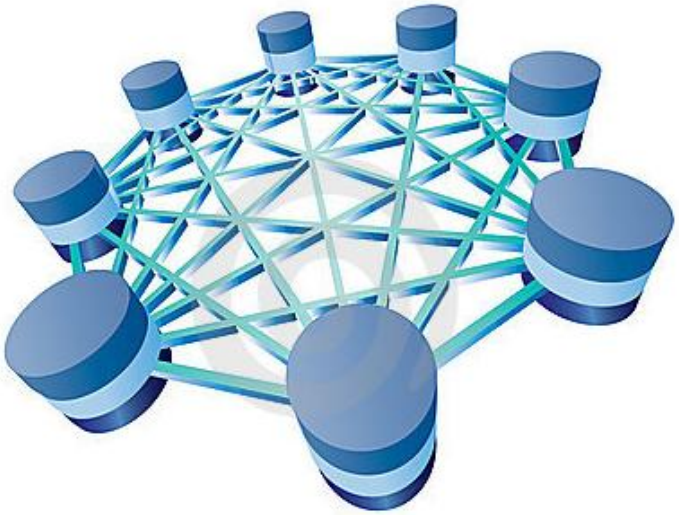
Universitat Oberta de Catalunya

www.uoc.edu

¿POR QUÉ PREOCUPARSE DE LA SEGURIDAD?

La pérdida de los activos de la empresa:

- Datos sensibles
- Servicios



IMPLICA

Pérdidas económicas

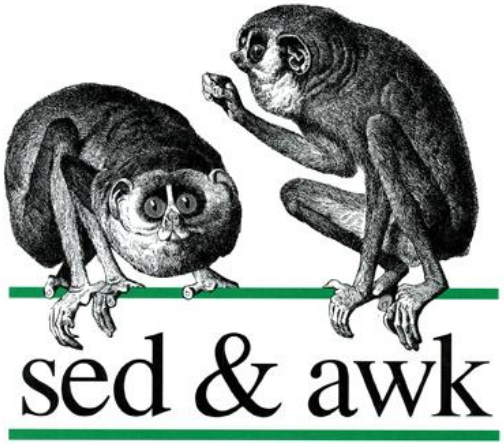
Implicaciones legales

SEGURIDAD EN LA EMPRESA

- La seguridad es el equilibrio entre riesgo y medidas establecidas para paliarlo.
- Los recursos utilizados para mitigar las amenazas no pueden ser más costosos que la información que se desea proteger.

HERRAMIENTAS

- Bastionado de SUSE Linux Enterprise Server 11 SP1, aporta la potencia de Linux con interesantes mecanismos de seguridad. Muy utilizado en entorno empresarial.
- Uso de *Shell scripting* implementar las políticas de seguridad, con el apoyo de *sed* y *awk.*
- Plataforma SUSE Studio para generar el LiveCD.



Securización de sistemas Linux

POLÍTICAS DE SEGURIDAD

POLÍTICAS DE SEGURIDAD: DEFINICIÓN

Cada una de las directivas del sistema que establece una configuración del objeto al que afecta.

POLÍTICAS DE SEGURIDAD I

Identificación y autenticación

Prevenir el ingreso en el sistema de personas no autorizadas.

- Gestión de las cuentas de usuario.
- Fortalecimiento de la política de contraseñas de usuario.
- Control de permisos.
- Banner de acceso.

POLÍTICAS DE SEGURIDAD II

Control de acceso y autorización

Derechos de acceso sobre recursos.

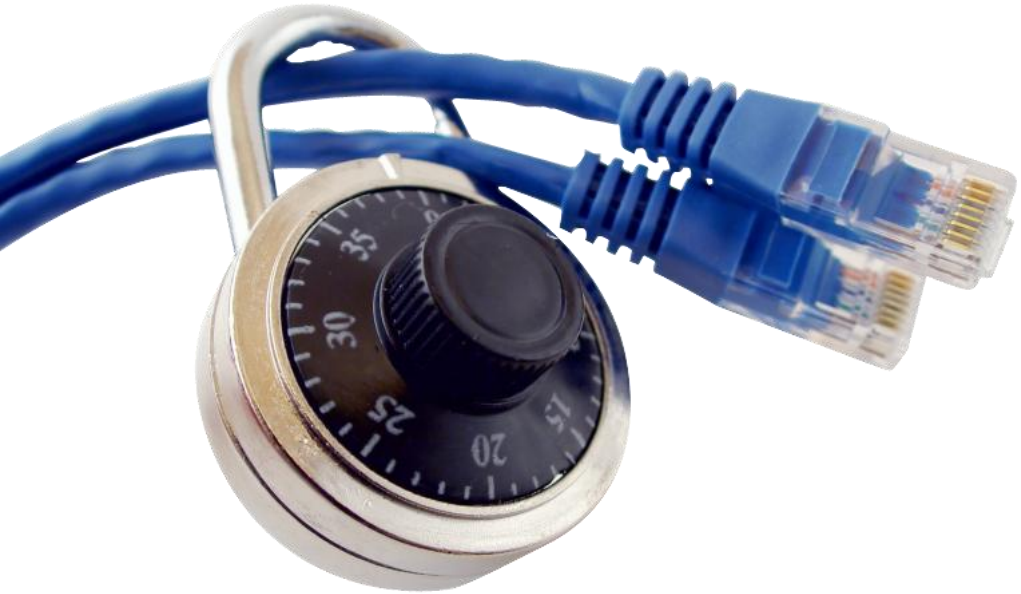
- Acceso a directorios y ficheros.
- Permisos SUID/SGID y de escritura global.
- Protección de los niveles de ejecución.
- Restricción de *cron* y *at*.

POLÍTICAS DE SEGURIDAD III

Seguridad de red

Bastionado de la interconexión del sistema con el exterior.

- Configuración de parámetros de red.
- Securización de los accesos vía SSH.



- Pila TCP/IP.
- Firewall.

POLÍTICAS DE SEGURIDAD IV

Integridad del sistema

Bastionado de la interconexión del sistema con el exterior.

- Actualización del sistema.
- Establecimiento de los servicios mínimos necesarios.
- Seguridad de dispositivos.

POLÍTICAS DE SEGURIDAD V

Mecanismos de auditoría

Registro de eventos que otorgan información de las actividades de los usuarios y del funcionamiento del sistema.

- Syslog-ng.
- Audit.

Securización de sistemas Linux

Ejecución del LiveCD

Universitat Oberta de Catalunya
www.uoc.edu

LiveCD: Arranque

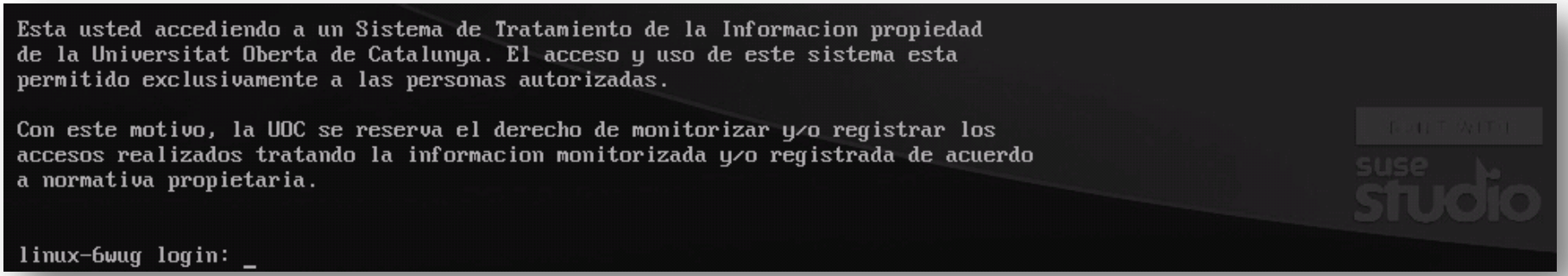
En primer lugar Grub que se encargará de cargar el sistema operativo:

LiveCD: Ejecución del *script*

Ejecución del *script* durante el inicio:

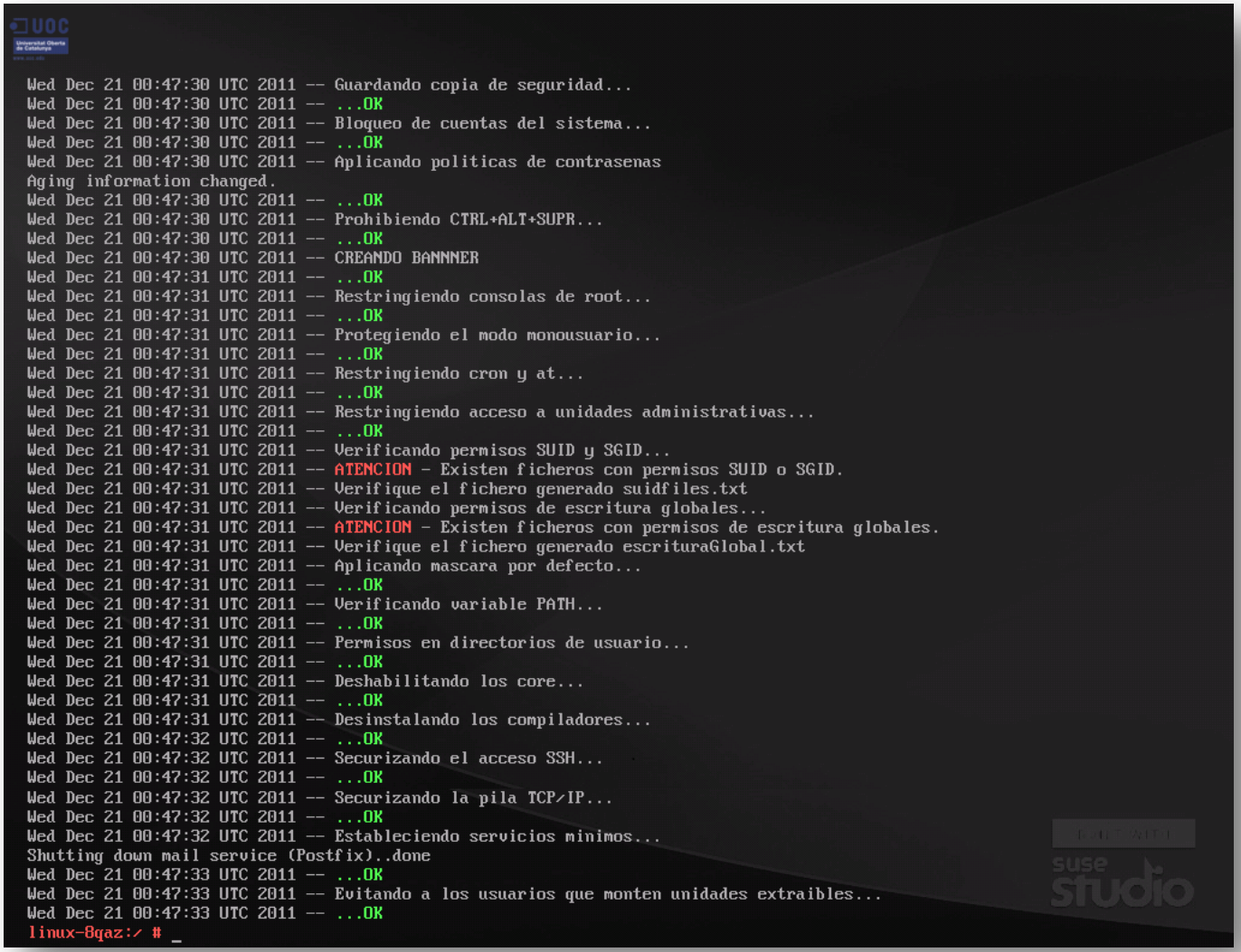
```
if [ -f /etc/init.d/suse_studio_firstboot ]
then

# Accedemos al directorio raíz donde se encuentra el fichero securiza.sh
cd /

# Ejecutamos el script y redireccionamos la salida al fichero securizacion.log
./securiza.sh >> securizacion.log

fi
```

Aparecerá el *banner* de acceso al sistema que hemos creado:



LiveCD: Salida del *script*

La salida del *script* se encuentra en el fichero *securizacion.log*:



Gracias

Alumno: Miguel Montero Rodríguez

Profesor: Helena Rifá Pous

Consultor: Jordi Massaguer Pla