

Trabajo Fin de Carrera

Securización de sistemas Linux

Alumno: Miguel Montero Rodríguez

Profesor: Helena Rifá Pous

Consultor: Jordi Massaguer Pla



**Universitat Oberta
de Catalunya**

www.uoc.edu

Securización de sistemas Linux

INTRODUCCIÓN



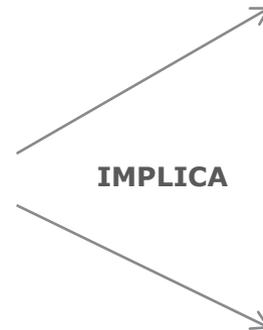
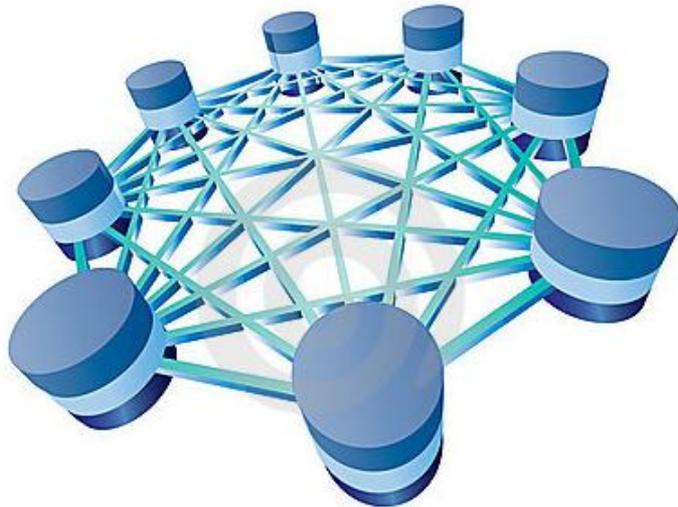
Universitat Oberta
de Catalunya

www.uoc.edu

¿POR QUÉ PREOCUPARSE DE LA SEGURIDAD?

La pérdida de los activos de la empresa:

- Datos sensibles
- Servicios



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



Universitat Oberta
de Catalunya

www.uoc.edu

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*.

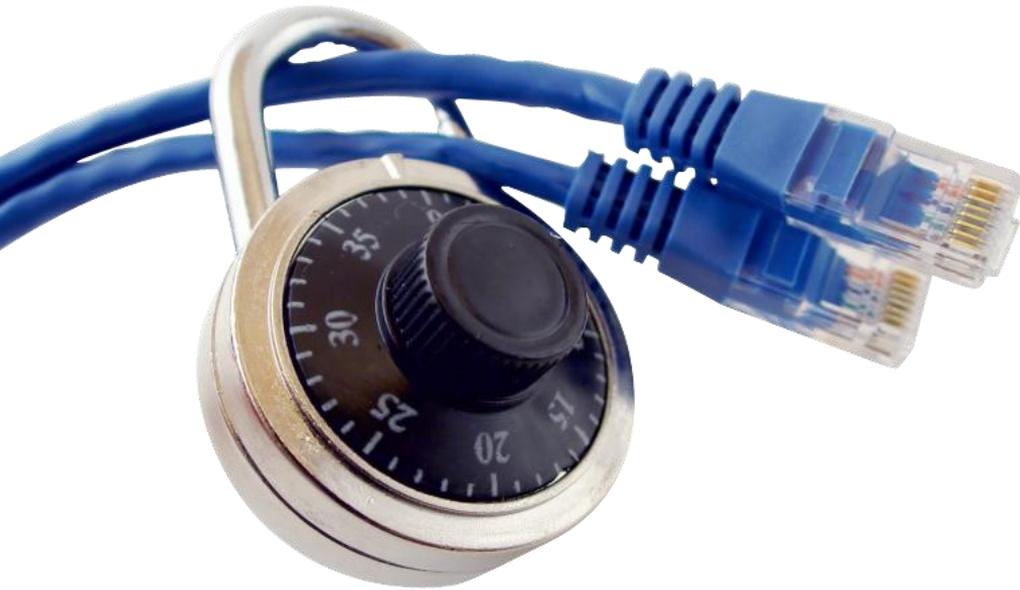


POLÍTICAS DE SEGURIDAD III

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

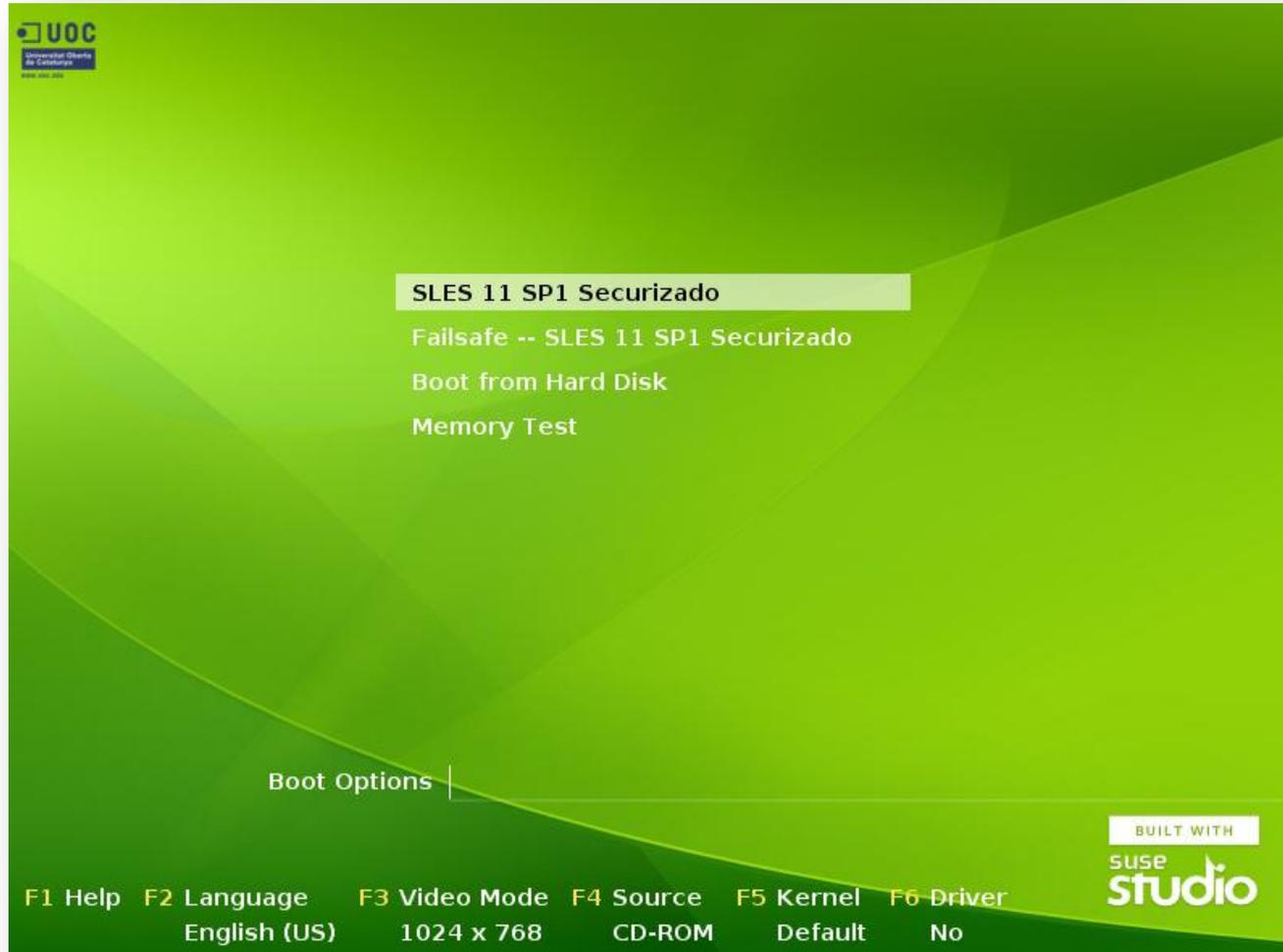


Universitat Oberta
de Catalunya

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:

Esta usted accediendo a un Sistema de Tratamiento de la Información propiedad de la Universitat Oberta de Catalunya. El acceso y uso de este sistema esta permitido exclusivamente a las personas autorizadas.

Con este motivo, la UOC se reserva el derecho de monitorizar y/o registrar los accesos realizados tratando la información monitorizada y/o registrada de acuerdo a normativa propietaria.

linux-6wug login: _



LiveCD: Salida del *script*

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

```
UOC
Universitat Oberta de Catalunya

Wed Dec 21 00:47:30 UTC 2011 -- Guardando copia de seguridad...
Wed Dec 21 00:47:30 UTC 2011 -- ...OK
Wed Dec 21 00:47:30 UTC 2011 -- Bloqueo de cuentas del sistema...
Wed Dec 21 00:47:30 UTC 2011 -- ...OK
Wed Dec 21 00:47:30 UTC 2011 -- Aplicando politicas de contraseñas
Aging information changed.
Wed Dec 21 00:47:30 UTC 2011 -- ...OK
Wed Dec 21 00:47:30 UTC 2011 -- Prohibiendo CTRL+ALT+SUPR...
Wed Dec 21 00:47:30 UTC 2011 -- ...OK
Wed Dec 21 00:47:30 UTC 2011 -- CREANDO BANNNER
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Restringiendo consolas de root...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Protegiendo el modo monousuario...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Restringiendo cron y at...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Restringiendo acceso a unidades administrativas...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Verificando permisos SUID y SGID...
Wed Dec 21 00:47:31 UTC 2011 -- ATENCION - Existen ficheros con permisos SUID o SGID.
Wed Dec 21 00:47:31 UTC 2011 -- Verifique el fichero generado suidfiles.txt
Wed Dec 21 00:47:31 UTC 2011 -- Verificando permisos de escritura globales...
Wed Dec 21 00:47:31 UTC 2011 -- ATENCION - Existen ficheros con permisos de escritura globales.
Wed Dec 21 00:47:31 UTC 2011 -- Verifique el fichero generado escrituraGlobal.txt
Wed Dec 21 00:47:31 UTC 2011 -- Aplicando mascara por defecto...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Verificando variable PATH...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Permisos en directorios de usuario...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Deshabilitando los core...
Wed Dec 21 00:47:31 UTC 2011 -- ...OK
Wed Dec 21 00:47:31 UTC 2011 -- Desinstalando los compiladores...
Wed Dec 21 00:47:32 UTC 2011 -- ...OK
Wed Dec 21 00:47:32 UTC 2011 -- Securizando el acceso SSH...
Wed Dec 21 00:47:32 UTC 2011 -- ...OK
Wed Dec 21 00:47:32 UTC 2011 -- Securizando la pila TCP/IP...
Wed Dec 21 00:47:32 UTC 2011 -- ...OK
Wed Dec 21 00:47:32 UTC 2011 -- Estableciendo servicios minimos...
Shutting down mail service (Postfix)..done
Wed Dec 21 00:47:33 UTC 2011 -- ...OK
Wed Dec 21 00:47:33 UTC 2011 -- Evitando a los usuarios que monten unidades extraibles...
Wed Dec 21 00:47:33 UTC 2011 -- ...OK
Linux-8qaz:~ #
```

Gracias

Alumno: Miguel Montero Rodríguez

Profesor: Helena Rifá Pous

Consultor: Jordi Massaguer Pla



**Universitat Oberta
de Catalunya**

www.uoc.edu