Securización de sistemas Linux

Trabajo fin de carrera [UOC]

Alumno: Miguel Montero Rodríguez
Profesor: Helena Rifá Pous
Consultor: Jordi Massaguer Pla

ESTA PÁGINA HA SIDO DEJADA INTENCIONALMENTE EN BLANCO

VERSIÓN DEL DOCUMENTO

Versión	Fecha	Páginas	Procesador	Cambios
0.1	24/10/2011	17	MS Word 2010	Versión inicial
0.2	21/12/2011	37	MS Word 2010	Modificado 5.4.6 (Establecimiento de la máscara por defecto). El usuario root por defecto no dispone de esos ficheros y coge los globales (los que se encuentran en /etc), por lo que se operará únicamente sobre éstos. Añadidos los puntos 9. Generación del LiveCD y 10. Ejecución del LiveCD. Añadido el código asociado a cada política de securización (en caso de que tenga script asociado). Añadido índice de tablas y figuras.
0.3	08/01/2012	37	MS Word 2010	Modificado 4.6.1 (Política de contraseñas de usuario). Añadidas restricciones de complejidad de contraseña. Modificado el código. Modificada figura 7: Opciones generales (se han añadido dos usuarios con el propósito de realizar una demo con ellos). Modificadas las figuras 14, 15 y 16: se ha actualizado a la versión 1.0.0 (previamente aparecía 0.0.1).
1.0	11/01/2012	39	MS Word 2010	Añadido el capítulo de conclusiones. Añadido el capítulo de bibliografía. Añadido logotipo de la UOC.

ÍNDICE

1. OBJETO 8
2. ALCANCE 9
3. OPERATIVA 10
4. IDENTIFICACIÓN Y AUTENTICACIÓN 11
4.1. IDENTIFICACIÓN DE USUARIOS 11
4.2. BLOQUEO DE CUENTAS INACTIVAS 11
4.3. ELIMINACIÓN DE CUENTAS INNECESARIAS 11
4.4. BLOQUEO DE CUENTAS DE SISTEMA 11
4.5. SECURIZACIÓN DE LOS ACCESOS PRIVILEGIADOS 11
4.6. FORTALECIMIENTO DE LA POLÍTICA DE CUENTAS 12
4.6.1. POLÍTICA DE CONTRASEÑAS DE USUARIO 12
4.6.2. POLÍTICA DE BLOQUEO DE CUENTAS DE USUARIO 13
4.7. NO PERMITIR APAGAR O REINICIAR EL EQUIPO A USUARIOS NORMALES 13
4.8. NO PERMITIR CTRL+ALT+SUPR 13
4.9. BANNER 13
5. CONTROL DE ACCESO Y AUTORIZACIÓN 15
5.1. DESHABILITAR EL ACCESO REMOTO A ROOT 15
5.2. PROTECCIÓN DEL MODO MONOUSUARIO CON CONTRASEÑA 15
5.3. RESTRICCIÓN DEL USO DE CRON Y AT 15
5.4. PROTECCIÓN DEL SISTEMA DE FICHEROS 16
5.4.1. PARTICIONAMIENTO 16
5.4.2. PROTECCIÓN DE LOS PUNTOS DE MONTAJE 16
5.4.3. RESTRICCIÓN DEL ACCESO A UTILIDADES ADMINISTRATIVAS 16
5.4.4. PERMISOS SUID EN PROGRAMAS EJECUTABLES 17
5.4.5. PERMISOS DE ESCRITURA GLOBALES 17
5.4.6. ESTABLECIMIENTO DE LA MÁSCARA POR DEFECTO 18
5.4.7. FORTALECIMIENTO DE LA VARIABLE PATH DE ROOT 18
5.4.8. DIRECTORIO DE LOS USUARIOS 18
5.4.9. DESHABILITAR LOS FICHEROS CORE 19
5.4.10. DESINSTALACIÓN DE LOS COMPILADORES 19
6. SEGURIDAD DE RED 20
6.1. CONFIGURACIÓN MANUAL DE LOS PARÁMETROS DE RED 20
6.2. ACTIVACIÓN DEL FIREWALL 20
6.3. SECURIZACIÓN DEL ACCESO VÍA SSH 20
6.4. SECURIZACIÓN DE LA PILA DE PROTOCOLOS TCP/IP 21
6.4.1. DESHABILITACIÓN DEL ENCAMINAMIENTO DE PAQUETES 21
6.4.2. DESHABILITACIÓN DEL ENCAMINAMIENTO FUENTE O DE ORIGEN 21
6.4.3. PROTECCIÓN FRENTE A INUNDACIONES SYN 21
6.4.4. PROTECCIÓN FRENTE A IP SPOOFING 21
6.4.5. PROTECCIÓN CONTRA ATAQUES SNMP 21
7. INTEGRIDAD DEL SISTEMA 23
7.1. ACTUALIZACIÓN DEL SISTEMA 23
7.1.1. IDENTIFICACIÓN DE PARCHES, ACTUALIZACIONES DE SISTEMA E INSTALACIÓN DE ACTUALIZACIONES CRÍTICAS 23
7.2. ESTABLECIMIENTO DE LOS SERVICIOS MÍNIMOS NECESARIOS 23
7.3. PROTECCIÓN DE LA ARQUITECTURA DEL SISTEMA 24

7.3.1. SEGURIDAD DE DISPOSITIVOS 24
8. MECANISMOS DE AUDITORÍA 25
8.1. SYSLOG-NG 25
8.2. AUDIT 25
9. GENERACIÓN DEL LIVECD 26
9.1. ACCESO A SUSE STUDIO 26
9.2. CREACIÓN DE UN NUEVO APPLIANCE 26
9.3. CONFIGURACIÓN DEL APPLIANCE 27
9.3.1. SOFTWARE 27
9.3.2. CONFIGURACIONES DE LA MÁQUINA 28
9.3.2.1. GENERAL 28
9.3.2.2. PERSONALIZACIÓN DE LA APARIENCIA 29
9.3.2.3. NIVEL DE INICIO DEL APPLIANCE 29
9.3.2.4. OPCIONES POR DEFECTO 30
9.4. INTEGRACIÓN DEL SCRIPT DE SECURIZACIÓN 30
9.4.1. CARGA DEL FICHERO DE SECURIZACIÓN EN LA MÁQUINA 30
9.4.2. SCRIPT DE INICIO 31
9.5. CONSTRUCCIÓN DEL APPLIANCE 32
10. EJECUCIÓN DEL LIVECD 33
11. CONCLUSIONES 37
11.1. POLÍTICAS DE SEGURIDAD 37
11.2. LÍNEAS FUTURAS 37
12. BIBLIOGRAFÍA 38
13. ANEXOS 39
13.1. LISTAS DE DISTRIBUCIÓN RECOMENDAS 39
13.2. PARCHES 39
13.3. NORMATIVA Y CERTIFICACIÓN 39

LISTA DE TABLAS Y FIGURAS

Tabla 1: [code] 4.4. Bloqueo de cuentas del sistema 11
Tabla 2: [code] 4.6.1. Bloqueo de cuentas del sistema 13
Tabla 3: [code] 4.6.2. Política de bloqueo de cuentas de usuario 13
Tabla 4: [code] 4.8. No permitir CTRL + ALT + SUPR 13
Tabla 5: [code] 4.9. Banner 14
Tabla 6: [code] 5.1. Deshabilitar el acceso remoto a *root* 15
Tabla 7: [code] 5.2. Protección del modo monousuario con contraseña 15
Tabla 8: [code] 5.3. Restricción del uso de *cron* y *at* 15
Tabla 9: [code] 5.4.3. Restricción del acceso a utilidades administrativas 16
Tabla 10: [code] 5.4.4. Permisos SUID en programas ejecutables 17
Tabla 11: [code] 5.4.5. Permisos de escritura globales 17
Tabla 12: [code] 5.4.6. Establecimiento de la máscara por defecto 18
Tabla 13: [code] 5.4.7. Fortalecimiento de la variable PATH de root 18
Tabla 14: [code] 5.4.8. Directorios de los usuarios 18
Tabla 15: [code] 5.4.9. Deshabilitar los ficheros *core* 19
Tabla 16: [code] 5.4.10. Desinstalación de los compiladores 19
Tabla 17: [code] 6.3. Securización del acceso SSH 21
Tabla 18: [code] 6.4. Securización de la pila de protocolos TCP/IP 22
Tabla 19: [code] 7.2. Establecimiento de los servicios mínimos necesarios 24
Tabla 20: [code] 7.3.1. Evitamos que los usuarios monten unidades extraíbles 24
Tabla 21: [code] Ejecución de *securiza.sh* 31

Figura 1: Acceso a SUSE Studio 26
Figura 2: Creación del appliance 26
Figura 3: Eligiendo la plantilla base 26
Figura 4: Eligiendo la arquitectura y nombre del appliance 27
Figura 5: Buscando el programa *audit* para instalarlo 27
Figura 6: Añadiendo *audit* a nuestra máquina 27
Figura 7: Opciones generales 28
Figura 8: Personalizando la apariencia 29
Figura 9: Nivel de inicio 29
Figura 10: Cargando el fichero que contiene el *script* de securización 30
Figura 11: Edición de los permisos del fichero que contiene el *script* 30
Figura 12: Detalles del fichero que contiene el *script* 31
Figura 13: *Script* de ejecución de *securiza.sh* 31
Figura 14: Configuración del LiveCD 32
Figura 15: Construcción del appliance 32
Figura 16: Descarga del appliance 32
Figura 17: Grub 33
Figura 18: Bootsplash 33
Figura 19: Novell Software License Agreement 34
Figura 20: *Banner* 34
Figura 21: Salida de la ejecución del *script securiza.sh* 35

Figura 22: escrituraGlobal.txt 35
Figura 23: suidfiles.txt 36

1. OBJETO

El objeto del presente documento es proporcionar una serie de directrices de configuración de seguridad para sistemas operativos Suse Linux Enterprise Server 11. Este sistema operativo proporciona un conjunto interesante de mecanismos de seguridad que permiten alcanzar un nivel de seguridad aceptable.

Mediante la aplicación de las directrices expuestas en este documento, se podrá garantizar una configuración adecuada del sistema operativo Suse Linux Enterprise Server 11 en lo relativo a la seguridad lógica.

El bastionado del sistema operativo debería realizarse antes de conectar la máquina a la red de comunicaciones.

2. ALCANCE

El presente documento tiene como alcance los sistemas basados en Suse Linux Enterprise Server 11, así como aquellas personas responsables de su administración.

3. OPERATIVA

Esta guía de securización se ha desarrollado para que pueda aplicarse a aquellas plataformas que cuenten con Suse Linux Enterprise Server 11 como sistema operativo.

Pese a que existe la opción de utilizar YaST para aplicar algunas labores de securización, se va a proceder a aplicar el bastionado de forma manual (así podremos aplicarlo al LiveCD mediante *scripts* a través de SUSE Studio).

Es necesario realizar cada uno de los puntos de esta guía respetando el orden en que aparecen.

La operativa se realizará durante el arranque del sistema.

4. IDENTIFICACIÓN Y AUTENTICACIÓN

La compartición de cuentas por varias personas supone la imposibilidad de establecer mecanismos de auditoría que permitan identificar de forma adecuada al autor de las acciones realizadas sobre el sistema. Por ello, es obligatorio que todos los accesos a las máquinas se realicen utilizando cuentas asignadas unívocamente a una persona.

En este proyecto se aplicarán medidas a nivel local, pues no disponemos de ningún servicio de directorio con el que integrarlo. En un principio existirá el superusuario local *root* (que no tendrá acceso remoto).

4.1. IDENTIFICACIÓN DE USUARIOS

Se debe implementar un mecanismo de identificación personal, que permita otorgar a cada individuo únicamente los accesos que requiera para desarrollar sus funciones, así como auditar su actividad.

Se debe asignar un identificador único a cada usuario; garantizándose en cualquier caso una relación unívoca entre el usuario y su identificador en el sistema.

4.2. BLOQUEO DE CUENTAS INACTIVAS

Todas las cuentas inactivas deberán ser eliminadas. El periodo de inactividad será de cuarenta días. Este procedimiento se realiza automáticamente una vez configurada la política de contraseñas.

4.3. ELIMINACIÓN DE CUENTAS INNECESARIAS

Por lo general, durante la instalación del sistema, se crean una serie de cuentas que no son necesarias. Se deberán borrar los usuarios y grupos que no sean estrictamente necesarios.

4.4. BLOQUEO DE CUENTAS DE SISTEMA

Se deberá impedir que se puedan realizar *logins* interactivos en las cuentas de demonios y servicios del sistema (su UID es inferior a 1000). Para ello se asignará a estas cuentas */bin/false* como *shell* por defecto. Adicionalmente se bloquearán las cuentas para no poder realizar inicio de sesión interactivo.

```
[code]
for NOMBRE_USER in `cut -d: -f1 /etc/passwd`; do
       ID_USER=`id -u $NOMBRE_USER`
       if [ $ID_USER -lt 1000 -a $NOMBRE_USER != 'root' ]; then
              usermod -s /bin/false $NOMBRE_USER &>/dev/null
              usermod -L $NOMBRE_USER &>/dev/null
       fi
       if [ $ID_USER -gt 999 -a $NOMBRE_USER != 'admin' ]; then
              usermod -L $NOMBRE_USER &>/dev/null
       fi
done
[/code]
```

Tabla 1: [code] 4.4. Bloqueo de cuentas del sistema

4.5. SECURIZACIÓN DE LOS ACCESOS PRIVILEGIADOS

La cuenta *root* no debe eliminarse nunca, pero tampoco debe utilizarse de manera remota. En su lugar se utilizará el comando *sudo* para realizar las operaciones necesarias. De esta forma se definirán roles de administración y se auditará toda acción privilegiada ejecutada en la máquina.

4.6. FORTALECIMIENTO DE LA POLÍTICA DE CUENTAS

4.6.1. POLÍTICA DE CONTRASEÑAS DE USUARIO

Se establecerá una política de contraseñas robustas. Las contraseñas constituyen la primera barrera de defensa contra posibles ataques a los sistemas, además de ser especialmente importantes desde el punto de vista normativo. En este sentido, es preciso establecer controles que garanticen la protección del acceso mediante la implantación de una política de contraseñas adecuada.

Se deberán aplicar las siguientes medidas:

- Prohibir el uso de contraseñas en blanco, requiriendo un mínimo de 7 caracteres.
- Forzar el cambio periódico de contraseña con una frecuencia máxima de 40 días.
- No permitir que se cambien las contraseñas inmediatamente después del cambio de contraseña, durante un periodo de cómo mínimo un día.
- Se avisará que la contraseña está a punto de caducar, con una antelación de 10 días.
- Forzar el empleo de contraseñas complejas: mínimo deberá diferenciarse de la anterior contraseña en 3 caracteres (difok=3), una longitud mínima de 7 caracteres (minlen=7), deberá contener al menos dos caracteres numéricos (dcredit=-2), un carácter numérico en mayúsculas (ucredit=-1) y uno en minúsculas (lcredit=-1). Se deberá utilizar además un carácter distinto de alfanumérico (un símbolo por ejemplo, ocredit=-1).
- Activar el mantenimiento de un histórico de contraseñas, de forma que el sistema no acepte la reutilización de la misma cadena de caracteres durante al menos 5 cambios consecutivos.
- El fichero /etc/passwd no contendrá contraseñas. Para tal fin se hará uso del fichero /etc/shadow. Este fichero sólo tendrá permisos de lectura para *root*.

```
[code]
awk '($1 ~ /^PASS_MAX_DAYS/) { $2="40" }
($1 ~ /^PASS_MIN_DAYS/) { $2="1" }
($1 ~ /^PASS_WARN_AGE/) { $2="10" }
($1 ~ /^PASS_MIN_LEN/) { $2="7" }
($1 ~ /^LOGIN_RETRIES/) { $2="3" }
{ print } ' /etc/login.defs.bak > /etc/login.defs
# Protegemos el fichero login.defs
chown root:root /etc/login.defs
chmod 640 /etc/login.defs
printf "/etc/login.defs \troot.root\t640\n" >> \
/etc/permissions.local
# Aplicamos la politica de contrasenas a los usuarios ya creados
for NAME in `cut -d: -f1 /etc/passwd`; do
uid=`id -u $NAME`
if [ $uid -ge 500 -a $uid != 65534 ]; then
chage -m 7 -M 90 -W 28 -I 7 $NAME
fi
done
# Creamos el fichero que controlara el historial de las contrasenas
touch /etc/security/opasswd
chown root:root /etc/security/opasswd
chmod 600 /etc/security/opasswd
# Politicas de contrasenas fuertes
cat <<- _EOF > /etc/pam.d/common-password
# Anadido por el script de securizacion
password  required  pam_cracklib.so     retry=3 difok=3 minlen=7 dcredit=-2
ucredit=-1 lcredit=-1 ocredit=-1
password  required  pam_pwhistory.so    remember=5
```

```
password  required  pam_unix.so        use_authtok nullok shadow md5
_EOF
[/code]
```

Tabla 2: [code] 4.6.1. Bloqueo de cuentas del sistema

4.6.2. POLÍTICA DE BLOQUEO DE CUENTAS DE USUARIO

Se debe activar el mecanismo de bloqueo de cuentas de usuario tras 5 intentos de acceso fallidos al sistema.

```
[code]
touch /var/log/faillog
chown root:root /var/log/faillog
chmod 600 /var/log/faillog
cat <<- _EOF >> /etc/pam.d/common-auth
# Añadido por el script de securización
auth    required        pam_tally.so    onerr=fail deny=4 unlock_time=900
_EOF
[/code]
```

Tabla 3: [code] 4.6.2. Política de bloqueo de cuentas de usuario

4.7. NO PERMITIR APAGAR O REINICIAR EL EQUIPO A USUARIOS NORMALES

Se impedirá que los usuarios sin privilegios puedan apagar, detener o reiniciar el equipo ejecutando los comandos *poweroff*, *halt* o *reboot*.

Nota: por defecto Suse Linux Enterprise Server 11 no permite realizar esta operativa a usuarios no privilegiados.

4.8. NO PERMITIR CTRL+ALT+SUPR

Se deberá prohibir el uso de CTRL+ALT+SUPR, de tal forma que no se pueda reiniciar el servidor por usuarios no autorizados que accedan físicamente al lugar donde esté situado el servidor.

```
[code]
# Comentamos la linea donde se encuentra la cadena ctrlaltdel
sed '/ctrlaltdel/s/^/#/' /etc/inittab.bak > /etc/inittab
[/code]
```

Tabla 4: [code] 4.8. No permitir CTRL + ALT + SUPR

4.9. BANNER

Con el objetivo de asemejar el bastionado a un sistema real, se generará un *banner* que se mostrará cuando un usuario realice un inicio de sesión, informándole sobre el uso del sistema y las acciones en caso de uso no autorizado.

Se incluirá el siguiente texto:

“”

Está usted accediendo a un Sistema de Tratamiento de la Información propiedad de la Universitat Oberta de Catalunya. El acceso y uso de este sistema está 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.

“”

```
[code]
function create_banner() {
    do_log "CREANDO BANNNER"

    cat > /etc/issue.net <<-_EOF


Esta usted accediendo a un Sistema de Tratamiento de la Informacion 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 informacion monitorizada y/o registrada de acuerdo
a normativa propietaria.


_EOF
}

create_banner

# Establecemos el propietario y los permisos
chown root:root /etc/issue.net
chmod 644 /etc/issue.net
cp /etc/issue.net /etc/issue
echo "Banner /etc/issue.net" >> /etc/ssh/sshd_config
# Necesitamos tambien incluirlo en el fichero de backup
echo "Banner /etc/issue.net" >> /etc/ssh/sshd_config.bak
tmp=`service sshd restart`
[/code]
```

Tabla 5: [code] 4.9. Banner

5. CONTROL DE ACCESO Y AUTORIZACIÓN

5.1. DESHABILITAR EL ACCESO REMOTO A ROOT

No se permitirá el acceso remoto a *root*. Cualquier tipo de acceso que requiera un inicio de sesión directo al sistema como *root* se restringirá a la consola local.

Se comentarán todas las líneas del fichero */etc/securetty*, a excepción de *vc/1* y *tty1*, para evitar que el usuario *root* inicie sesión en más de un terminal virtual.

```
[code]
awk '$1 ~ /^#?*tty[0-9]?[2-9]/ { $1 = "#"$1; print; next };
       $1 ~ /^#?*vc\/[0-9]?[2-9]/ { $1 = "#"$1; print; next};
      {print}' /etc/securetty.bak > /etc/securetty
# Protegemos el fichero /etc/securetty
chown root:root /etc/securetty
chmod 400 /etc/securetty
printf "/etc/securetty \troot.root\t400\n" >> \
/etc/permissions.local
[/code]
```

Tabla 6: [code] 5.1. Deshabilitar el acceso remoto a *root*

5.2. PROTECCIÓN DEL MODO MONOUSUARIO CON CONTRASEÑA

Se establecerá una contraseña de tal forma que no se permita que un usuario malintencionado arranque el sistema en el nivel de ejecución (*runlevel*) 1 y se convierta en *root*.

```
[code]
sed -e '/id:3:initdefault:/ a ~~:S:wait:/sbin/sulogin' /etc/inittab.bak >
/etc/inittab
[/code]
```

Tabla 7: [code] 5.2. Protección del modo monousuario con contraseña

5.3. RESTRICCIÓN DEL USO DE CRON Y AT

Se deberá restringir el acceso a *cron* y *at* únicamente a los usuarios que necesiten ejecutar tareas programadas.

En estos ficheros se especificarán los usuarios autorizados a ejecutar dichas aplicaciones, que en general, será únicamente el superusuario *root*.

Se eliminarán las entradas de *crontab* en */var/spool/cron* para todos los usuarios, exceptuando aquellos estrictamente necesarios.

```
[code]
echo "root" > /etc/cron.allow
echo "root" > /etc/at.allow
[/code]
```

Tabla 8: [code] 5.3. Restricción del uso de *cron* y *at*

5.4. PROTECCIÓN DEL SISTEMA DE FICHEROS

5.4.1. PARTICIONAMIENTO

***NOTA**: esto es una recomendación, no se implantará en el LiveCD debido a que no podremos intervenir en el sistema de ficheros.*

Se debería crear, como mínimo, las siguientes particiones, cuyo tamaño dependerá de la función que desempeñe el servidor:

- /
- /home
- /opt
- /tmp
- /usr
- /var
- swap

De esta forma se consiguen evitar determinados ataques de denegación de servicio que pretenden llenar directorios y que podrían inutilizar el sistema.

5.4.2. PROTECCIÓN DE LOS PUNTOS DE MONTAJE

***NOTA**: esto es una recomendación, no se implantará en el LiveCD debido a que no podremos intervenir en el sistema de ficheros.*

Se debería modificar el fichero */etc/fstab* para reforzar la protección del sistema de ficheros de la siguiente forma:

- Montar el directorio */usr* como sólo lectura. El sistema se deberá montar como lectura-escritura cuando se actualice el sistema o se instalen nuevas aplicaciones
- Prevenir la activación de ficheros con SUID o ficheros de dispositivos de unidades removibles tal como cdroms, etc.
- El directorio */home* deberá tener activadas las opciones de nosuid y nodev
- Desactivar el hecho de que se monten unidades automáticamente (ver apartado 7.3.1)

5.4.3. RESTRICCIÓN DEL ACCESO A UTILIDADES ADMINISTRATIVAS

Se restringirá el acceso a las utilidades administrativas del sistema de tal forma que no puedan ser ejecutadas por usuarios sin privilegios. Estas utilidades se encuentran en los siguientes directorios:

/sbin

/usr/sbin

Se deberán quitar los permisos de lectura, escritura y ejecución a los usuarios y grupos que no sean dueños de los ficheros en dichos directorios.

```
[code]
chmod o-wx /sbin/*
chmod o-wx /usr/sbin/*
chmod g-wx /sbin/yast2
[/code]
```

Tabla 9: [code] 5.4.3. Restricción del acceso a utilidades administrativas

5.4.4. PERMISOS SUID EN PROGRAMAS EJECUTABLES

Es necesario auditar los programas *suid* y *sgid* para determinar qué programas no necesitan tener estos bits activos. Los programas con estos bits activos deberán ser los estrictamente necesarios, pues suponen un riesgo grave de seguridad.

Es importante auditar e identificar los programas con *suid* activo antes de ejecutar el mandato, la ejecución de este comando podría provocar que ciertos programas dejaran de funcionar.

```
[code]
result=`find / -xdev \( -perm -04000 -o -perm -02000 \) -type f -print`
echo "$result" > suidfiles.txt
if [ "$result" = "" ]; then
        do_log "${VERDE}...OK${NC}"
        rm suidfiles.txt
else
        do_log "${ROJO}ATENCION${NC} - Existen ficheros con permisos SUID o SGID."
        do_log 'Verifique el fichero generado suidfiles.txt'
fi
[/code]
```

Tabla 10: [code] 5.4.4. Permisos SUID en programas ejecutables

5.4.5. PERMISOS DE ESCRITURA GLOBALES

Se auditará el sistema en busca de ficheros con permisos de escritura para todos los usuarios. Estos ficheros pueden ser modificados o eliminados por cualquier usuario del sistema. Pueden ser síntoma de problemas en algún *script* o aplicación, que pueden ser una causa potencial de problemas más graves.

```
[code]
# Busca ficheros con o+w y sin tener activo el sticky bit
result=`find / -xdev \( -perm -0002 -a ! -perm -1000 \) -type f -print`
echo "$result" > escrituraGlobal.txt
if [ "$result" = "" ]; then
        do_log "${VERDE}...OK${NC}"
        rm escrituraGlobal.txt
else
        do_log "${ROJO}ATENCION${NC} - Existen ficheros con permisos de escritura
globales."
        do_log 'Verifique el fichero generado escrituraGlobal.txt'
fi
[/code]
```

Tabla 11: [code] 5.4.5. Permisos de escritura globales

5.4.6. ESTABLECIMIENTO DE LA MÁSCARA POR DEFECTO

Será necesario modificar la máscara (UMASK) para todos los usuarios, ya que por defecto se dispone de permisos de lectura para todo el mundo.

```
[code]
for FILE in /etc/profile /etc/csh.login /etc/csh.cshrc /etc/bash.bashrc;
do
        if ! egrep -q 'umask.*77' $FILE ; then
                echo "umask 077" >> $FILE
        fi
        # Protegemos el fichero
        chown root:root $FILE
        chmod 444 $FILE
        printf "/etc/$FILE \troot.root\t444\n" >> \
        /etc/permissions.local
done
[/code]
```

Tabla 12: [code] 5.4.6. Establecimiento de la máscara por defecto

5.4.7. FORTALECIMIENTO DE LA VARIABLE PATH DE ROOT

No debe existir "." En la variable $PATH de *root*.

```
[code]
echo $PATH > /tmp/pathfile.tmp
result=`grep "\." /tmp/pathfile.tmp`
if [ "$result" = "" ]; then
       do_log "${VERDE}...OK${NC}"
else
       do_log "${ROJO}ATENCION${NC} - La variable PATH contiene"
       do_log 'el directorio "."'
fi
rm /tmp/pathfile.tmp
[/code]
```

Tabla 13: [code] 5.4.7. Fortalecimiento de la variable PATH de root

5.4.8. DIRECTORIO DE LOS USUARIOS

Los directorios de los usuarios deberán tener como mínimo permisos 750, especificados por la máscara por defecto que se definió anteriormente.

```
[code]
for DIR in `awk -F: '($3 >= 500) { print $6 }' /etc/passwd`; do
       chmod g-w $DIR
       chmod o-rwx $DIR
done
[/code]
```

Tabla 14: [code] 5.4.8. Directorios de los usuarios

5.4.9. DESHABILITAR LOS FICHEROS CORE

Se deberá deshabilitar la creación de ficheros *core*.

```
[code]
function deshabilitaCore(){
      #Adicion al  fichero /etc/security/limits.conf
      cat <<- _EOF >> /etc/security/limits.conf
# Anadido por el script de securizacion
* soft core 0
* hard core 0
_EOF
}
[/code]
```

Tabla 15: [code] 5.4.9. Deshabilitar los ficheros *core*

5.4.10. DESINSTALACIÓN DE LOS COMPILADORES

Con el objetivo de que el servidor realice el trabajo únicamente para el que se haya establecido, se deberán desinstalar los compiladores si no van a utilizarse.

```
[code]
rpm -e gcc &>/dev/null
rpm -e gcc3 &>/dev/null
rpm -e gcc3-c++ &>/dev/null
rpm -e gcc3-g77 &>/dev/null
rpm -e gcc3-java &>/dev/null
rpm -e gcc3-objc &>/dev/null
rpm -e gcc-c++ &>/dev/null
rpm -e gcc-chill &>/dev/null
rpm -e gcc-g77 &>/dev/null
rpm -e gcc-java &>/dev/null
rpm -e gcc-objc &>/dev/null
rpm -e bin86 &>/dev/null
rpm -e dev86 &>/dev/null
rpm -e nasm &>/dev/null

result=`find /home -type f -name "*gcc*"  -o -name "*bin86*" -o -name "*dev86*" -o
-name "*nasm*"`
echo "$result" > compiladores.txt
if [ "$result" = "" ]; then
        do_log "${VERDE}...OK${NC}"
        rm compiladores.txt
else
        do_log "${ROJO}ATENCION${NC} - Se han encontrado indicios de compiladores."
        do_log 'Verifique el fichero generado compiladores.txt'
fi
[/code]
```

Tabla 16: [code] 5.4.10. Desinstalación de los compiladores

6. SEGURIDAD DE RED

6.1. CONFIGURACIÓN MANUAL DE LOS PARÁMETROS DE RED

En un entorno empresarial la configuración de los parámetros de red (dirección IP, máscara de red, *gateway*, servidores DNS, etc.) se debería realizar de forma manual, no permitiéndose la configuración mediante protocolos de configuración automática (DHCP).

En nuestro caso vamos a dejar DHCP activo, para disponer de acceso a red desde LiveCD.

6.2. ACTIVACIÓN DEL FIREWALL

Se deberá habilitar el cortafuegos para impedir todo tipo de acceso al servidor, exceptuando los servicios para los que se haya configurado. En principio aplicaremos la configuración desde SUSE Studio y abriremos el puerto 22 de SSH.

6.3. SECURIZACIÓN DEL ACCESO VÍA SSH

Se configurará el demonio SSH (*sshd*) de tal forma que se cumplan los siguientes puntos:

- Se utilizará exclusivamente la versión 2 del protocolo.
- El demonio escuchará exclusivamente en las interfaces necesarias.
- No se permitirá encapsular las X en una sesión.
- No se permitirá la autenticación basada en hosts.
- Se ignorarán los hosts remotos definidos en .rhosts o .shosts.
- No se permitirá que el usuario root se conecte vía ssh.
- No se permitirán contraseñas vacías.
- Se establecerá un periodo de inactividad, tras el cual finalizará la sesión. Dicho periodo de inactividad será de cinco minutos.
- Se establecerá que el banner apunte al configurado previamente.

```
[code]
IPGEST=`/sbin/ifconfig eth0 | grep inet | awk {'print $2'} | sed 's/addr://'`

awk -v ipgestion=$IPGEST '/^#? *Protocol/ { print "Protocol 2"; next };
/^#? *ListenAddress [0-9]\.[0-9]\.[0-9\.[0-9]/ { if (ipgestion == "") print $0;
else print "ListenAddress "ipgestion ; next };
/^#? *X11Forwarding/ { print "X11Forwarding no"; next };
/^#? *IgnoreRhosts/ { print "IgnoreRhosts yes"; next };
/^#? *HostbasedAuthentication/ { print "HostbasedAuthentication no"; next };
/^#? *PermitRootLogin/ { print "PermitRootLogin no"; next };
/^#? *PermitEmptyPasswords/ { print "PermitEmptyPasswords no"; next };
/^#? *ClientAliveInterval / { print "ClientAliveInterval  300"; next };
/^#? *ClientAliveCountMax / { print "ClientAliveCountMax  3"; next };
/^#? *Banner/ { print "Banner /etc/issue.net"; next };
{print}' /etc/ssh/sshd_config.bak > /etc/ssh/sshd_config

tmp=`/etc/init.d/sshd restart 2> sshErrors.txt`
if [[ -s sshErrors.txt ]]; then
        do_log "${ROJO}ERROR${NC} La configuracion de SSH ha fallado."
        do_log "Se restaura la configuracion anterior."
        do_log "Verifique el fichero sshErrors.txt para ver los errores."
        recover /etc/ssh/sshd_config
        /etc/init.d/sshd restart &>/dev/null
else
```

```
        rm sshErrors.txt
        do_log "${VERDE}...OK${NC}"
fi
[/code]
```

Tabla 17: [code] 6.3. Securización del acceso SSH

6.4. SECURIZACIÓN DE LA PILA DE PROTOCOLOS TCP/IP

Los parámetros que se describen a continuación se deben especificar en el fichero */etc/sysctl.conf.* Dicho fichero deberá tener permisos de lectura y escritura para *root* exclusivamente.

6.4.1. DESHABILITACIÓN DEL ENCAMINAMIENTO DE PAQUETES

Se deberá deshabilitar el encaminamiento de paquetes en aquellos sistemas que no actúen como *gateways*. Para ello se establecerá el siguiente parámetro:

net.ipv4.ip_forward = 0

6.4.2. DESHABILITACIÓN DEL ENCAMINAMIENTO FUENTE O DE ORIGEN

Se deberá deshabilitar el encaminamiento fuente. Para ello se establecerá el siguiente parámetro:

net.ipv4.conf.all.accept_source_route = 0

6.4.3. PROTECCIÓN FRENTE A INUNDACIONES SYN

Se deberán configurar los siguientes parámetros:

net.ipv4.tcp_max_syn_backlog = 4096

net.ipv4.tcp_syncookies = 1

6.4.4. PROTECCIÓN FRENTE A IP SPOOFING

Se deberá configurar el siguiente parámetro:

net.ipv4.conf.all.rp_filter = 1

6.4.5. PROTECCIÓN CONTRA ATAQUES SNMP

Se deberán configurar los siguientes parámetros:

- No permitir que se puedan mandar paquetes de redirección ICMP:

  net.ipv4.conf.all.send_redirects = 0

- No permitir que se acepten paquetes de redirección ICMP:

  net.ipv4.conf.all.accept_redirects = 0

  net.ipv4.conf.default.accept_redirects = 0

```
[code]
# Definimos la funcion securizarPilaTCP()
function securizarPilaTCP() {
       #Adición al  fichero /etc/sysctl
       cat <<- _EOF >> /etc/sysctl.conf
# Añadido por el script de securización
net.ipv4.ip_forward = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.tcp_max_syn_backlog = 4096
```

```
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
_EOF
}
# Ejecutamos la funcion
securizarPilaTCP
# Protegemos el fichero sysctl.conf
chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf
printf "/etc/sysctl.conf\troot.root\t600\n" >> \
/etc/permissions.local
[/code]
```

Tabla 18: [code] 6.4. Securización de la pila de protocolos TCP/IP

7. INTEGRIDAD DEL SISTEMA

7.1. ACTUALIZACIÓN DEL SISTEMA

7.1.1. IDENTIFICACIÓN DE PARCHES, ACTUALIZACIONES DE SISTEMA E INSTALACIÓN DE ACTUALIZACIONES CRÍTICAS

Se deberá tener el sistema actualizado con los últimos parches de seguridad instalados, de tal forma que se mitiguen los riesgos derivados de la existencia de vulnerabilidades del sistema operativo y de sus componentes.

***NOTA**: esto es una recomendación, no se implantará en el LiveCD.*

7.2. ESTABLECIMIENTO DE LOS SERVICIOS MÍNIMOS NECESARIOS

En la instalación de SLES, se deberán elegir únicamente los paquetes estrictamente necesarios. Se deberán deshabilitar los servicios que no se vayan a utilizar.

De esta forma se aumentará la seguridad del sistema, puesto que cuantos menos servicios estén activos, menor será el alcance de posibles ataques. A su vez, se aumentará el rendimiento del sistema, pues se necesitarán menos recursos.

Debido a su carácter inseguro, los siguientes servicios deberán desinstalarse en caso de estar instalados:

- *telnetd*
- *wu-ftpd*
- *rlogin, rsh, rexec*
- *tftp*

```
[code]
# Nos aseguramos de deshabilitar los servicios de xinetd
for FILE in $(ls /etc/xinetd.d/); do
  if [ $FILE != "cba8" -a $FILE != "pds2" ]; then
          chkconfig -set $FILE off &>/dev/null;
  fi
done;
chkconfig -set aaeventd off # Notificación y reporte de AppArmor
chkconfig -set autoyast off # Instalaciones automáticas
chkconfig -set boot.apparmor off # AppArmour
chkconfig -set acpid off # Control del funcionamiento de la BIOS
chkconfig -set fbset off # Configuración del frame buffer
chkconfig -set lm_sensors off # Control de temperaturas y velocidad de ventilador
chkconfig -set microcode off # Actualización del microcódigo de la CPU de Intel
chkconfig -set nfsboot off # Servicio que permite arrancar un equipo a través de la
red
chkconfig -set postfix off # Relay de correo
chkconfig -set powersaved off # Optimización del consumo de energía
chkconfig -set slpd off # Búsqueda de servicios en la red
chkconfig -set splash off # Servicio para modificar la pantalla de arranque
chkconfig -set splash_early off # "Mata" la aplicación cuando la red se levanta
chkconfig -set xdm off # Gestor de las X

service aaeventd stop
service autoyast stop
service boot.apparmor stop
service acpid stop
service fbset stop
service lm_sensors stop
```

```
service microcode stop
service nfsboot stop
service postfix stop
service powersaved stop
service slpd stop
service splash stop
service splash_early stop
service xdm stop
[/code]
```

Tabla 19: [code] 7.2. Establecimiento de los servicios mínimos necesarios

7.3. PROTECCIÓN DE LA ARQUITECTURA DEL SISTEMA

7.3.1. SEGURIDAD DE DISPOSITIVOS

Se deberá impedir el montaje automático de todo tipo de unidades, tales como *cdroms*, dispositivos *usb*, etc.

```
[code]
cat /etc/fstab |
sed 's|\( /media/[fc].* *auto .*[ ,]\)user\([,]\)|\1nouser\2|' |
sed 's|\( /media/[fc].* *auto .*[ ,]\)users\([,]\)|\1nouser\2|' > /etc/fstab
[/code]
```

Tabla 20: [code] 7.3.1. Evitamos que los usuarios monten unidades extraíbles

8. MECANISMOS DE AUDITORÍA

Se utilizarán las opciones por defecto que nos aporta tanto *Syslog-ng* como *Audit*.

8.1. SYSLOG-NG

Syslog-ng es un demonio que implementa el estándar de facto para el registro de eventos y dispone de interesantes prestaciones y gran flexibilidad.

8.2. AUDIT

Audit dispone de varios componentes, contribuyendo cada uno de ellos con una funcionalidad concreta. El módulo de auditoría del *kernel* intercepta las llamadas al sistema y registra los eventos relevantes. El demonio *auditd* escribe reportes de auditoría al disco.

9. GENERACIÓN DEL LIVECD

El objetivo de disponer de un LiveCD securizado servirá como prueba de concepto de la seguridad aplicada. Para obtenerlo, realizaremos la siguiente operativa:

9.1. ACCESO A SUSE STUDIO

Para acceder a SUSE Studio deberemos disponer de alguna de las siguientes cuentas:

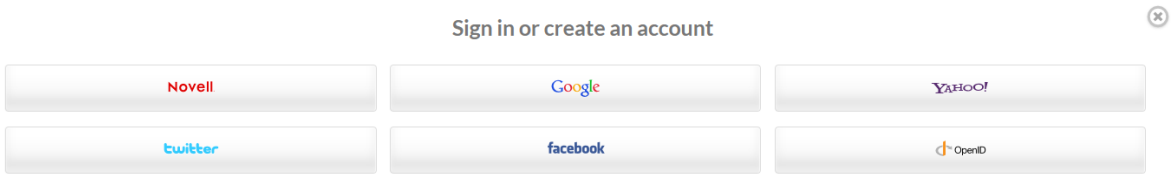

Figura 1: Acceso a SUSE Studio

9.2. CREACIÓN DE UN NUEVO APPLIANCE

Una vez accedemos al sistema, deberemos crear nuestro nuevo appliance, para ello, pulsamos en el siguiente enlace:

Figura 2: Creación del appliance

La siguiente pantalla nos solicita que elijamos una plantilla base, la arquitectura y el nombre del appliance. En nuestro caso, elegiremos las siguientes opciones:

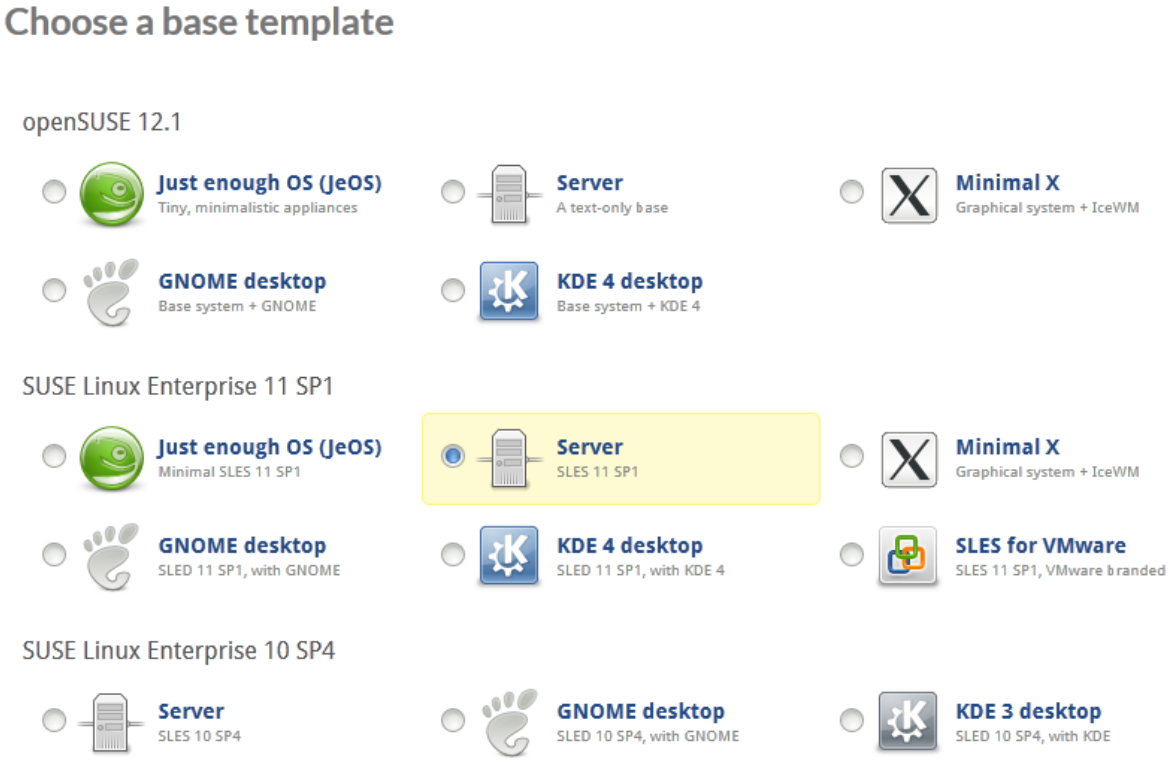

Figura 3: Eligiendo la plantilla base

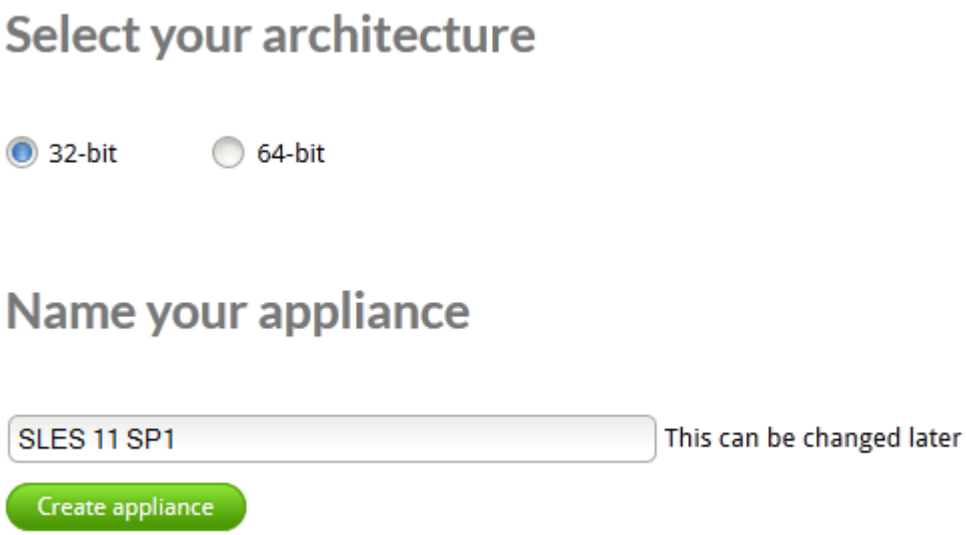

Figura 4: Eligiendo la arquitectura y nombre del appliance

9.3. CONFIGURACIÓN DEL APPLIANCE

9.3.1. SOFTWARE

Deberemos añadir *audit* ya que no viene instalado por defecto, para ello accederemos a la pestaña "Software" y lo buscaremos en el campo "*Search for software*":

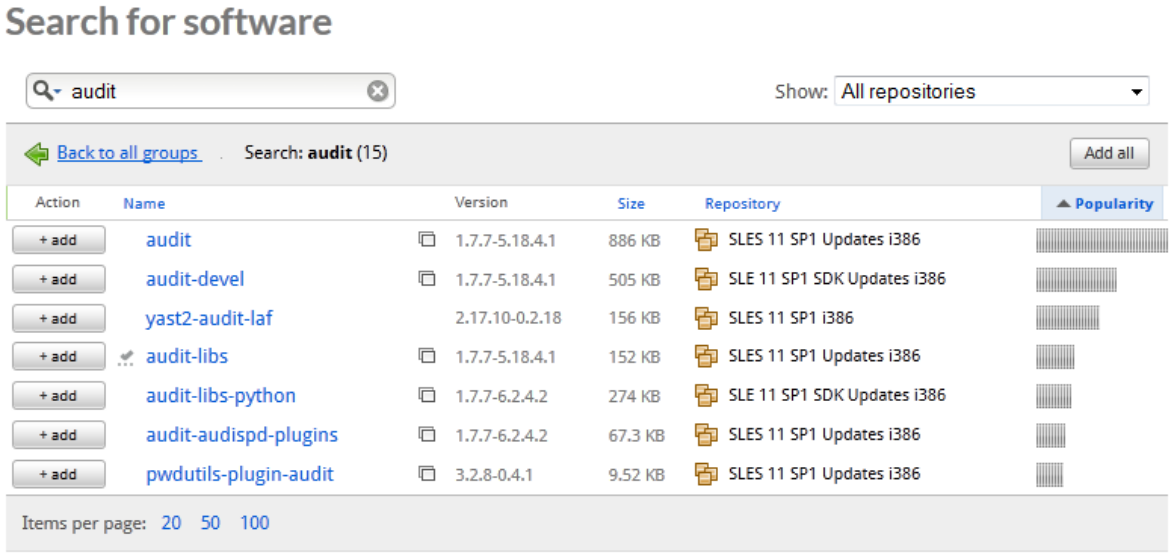

Figura 5: Buscando el programa *audit* para instalarlo

Añadiremos entonces *audit* a nuestro equipo pulsando sobre el botón "+ *add*":

Figura 6: Añadiendo *audit* a nuestra máquina

9.3.2. CONFIGURACIONES DE LA MÁQUINA

Encontraremos estas opciones en la pestaña "Configuration".

9.3.2.1. General

En este punto configuraremos las locales del sistema, la zona horaria, red, Firewall y usuarios y grupos. Se encuentra bajo la subpestaña "General":

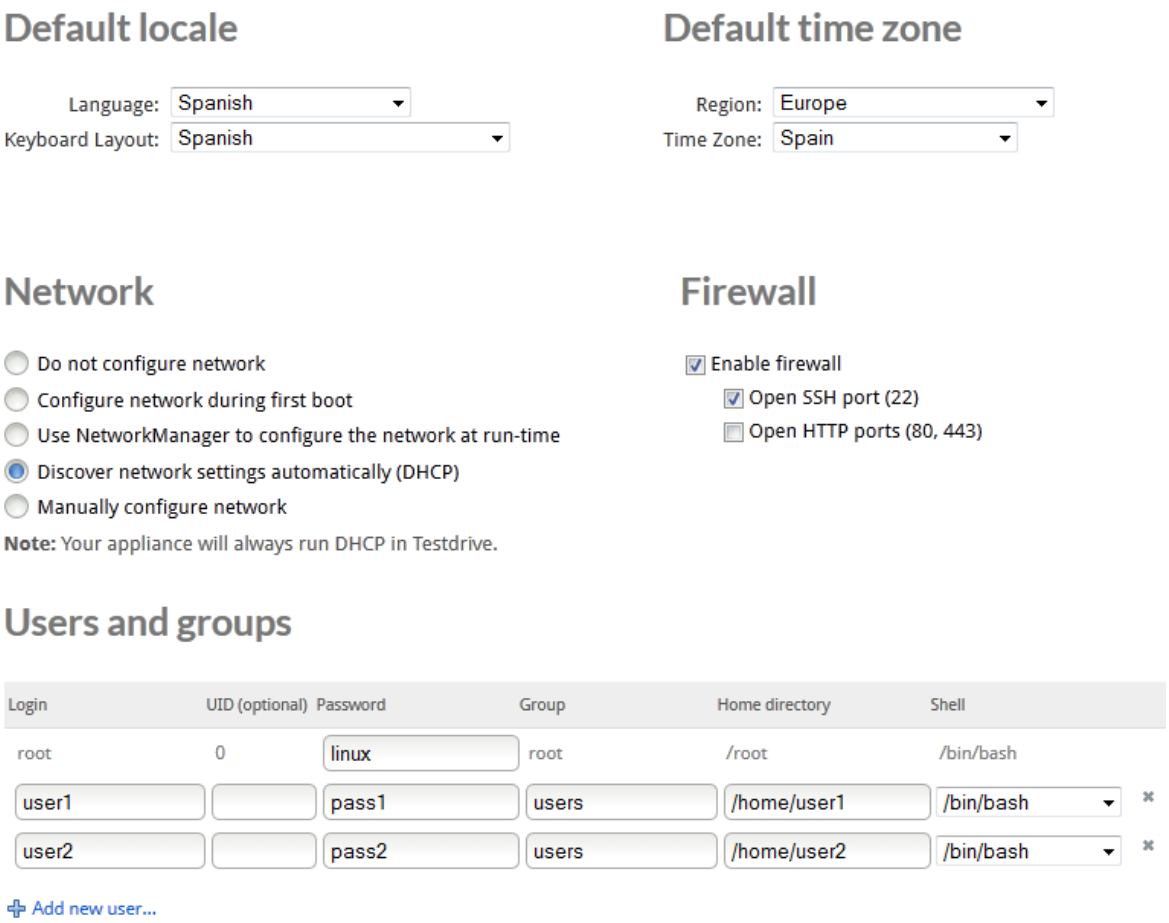

Figura 7: Opciones generales

9.3.2.2. Personalización de la apariencia

Cargaremos el logo de la UOC y elegiremos el fondo de pantalla del appliance:

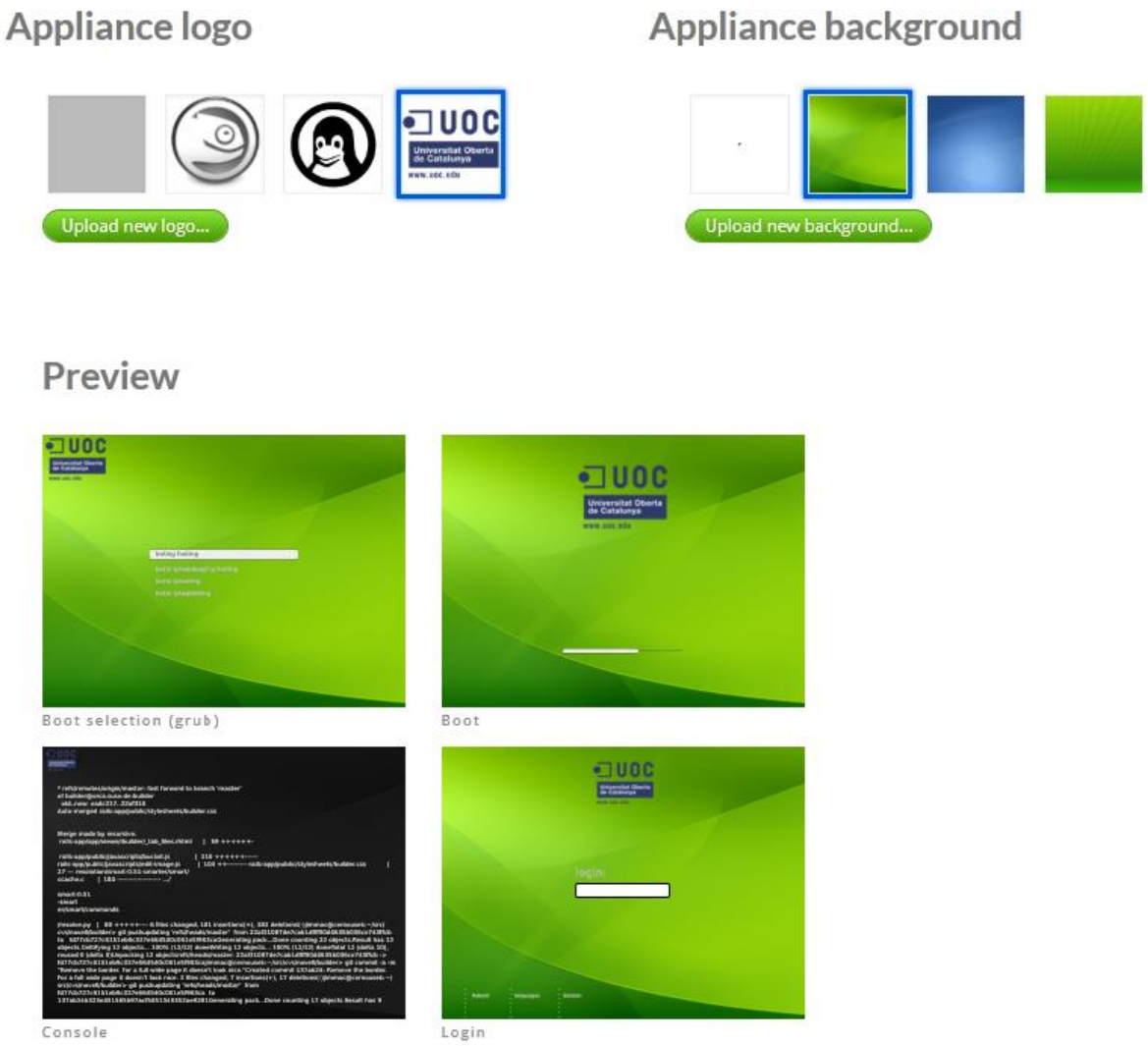

Figura 8: Personalizando la apariencia

9.3.2.3. Nivel de inicio del appliance

Se configurará para que el nivel de inicio (*runlevel*) sea la consola (*3: Normal console*).

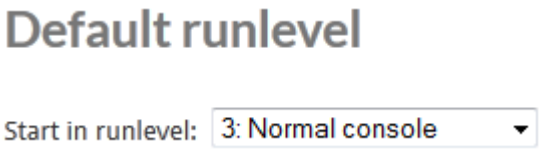

Figura 9: Nivel de inicio

9.3.2.4. Opciones por defecto

Dejaremos las siguientes funcionalidades por defecto:

- Servidor de PostgreSQL y/o MySQL: deshabilitado.
- Identificación automática de usuario: deshabilitado.
- Opciones físicas del appliacnes (espacio de disco duro para imágenes virtuales, partición swap…): valores por defecto.

9.4. INTEGRACIÓN DEL SCRIPT DE SECURIZACIÓN

En este punto disponemos del appliance con la configuración necesaria. Únicamente falta integrar el trabajo realizado relativo a la securización.

9.4.1. CARGA DEL FICHERO DE SECURIZACIÓN EN LA MÁQUINA

Lo primero que deberemos realizar es cargar el script en la máquina. Para ello, accederemos a la pestaña "*Files*" y cargaremos el fichero "*securiza.tar.gz*":

Pulsamos sobre "*Upload file…*" y elegimos el fichero. Una vez realizado esto, veremos lo siguiente:

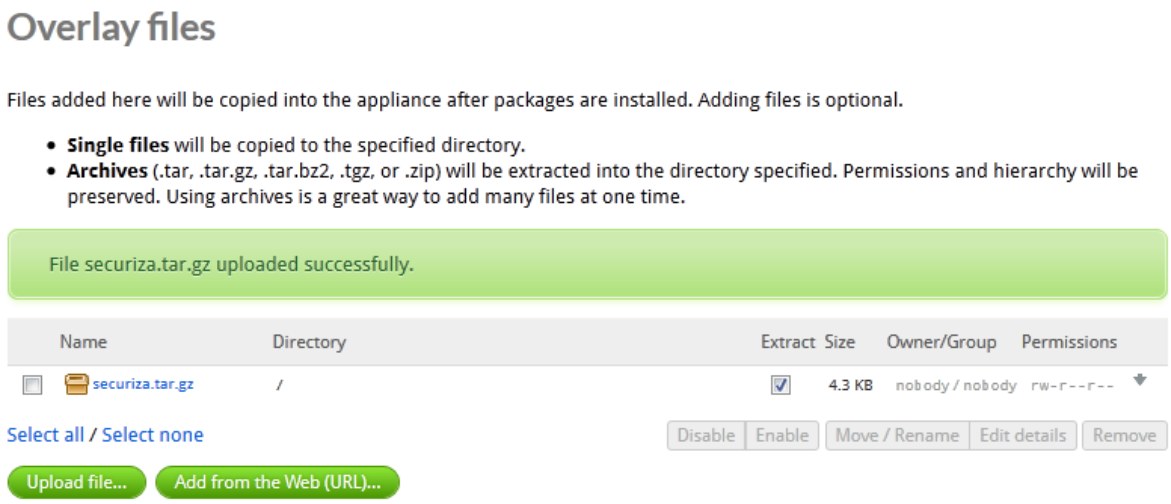

Figura 10: Cargando el fichero que contiene el *script* de securización

Como el *script* deberá ejecutarlo el usuario *root*, procederemos a dejar la configuración como se indica a continuación (seleccionamos el fichero y pulsamos "*Edit details*"):

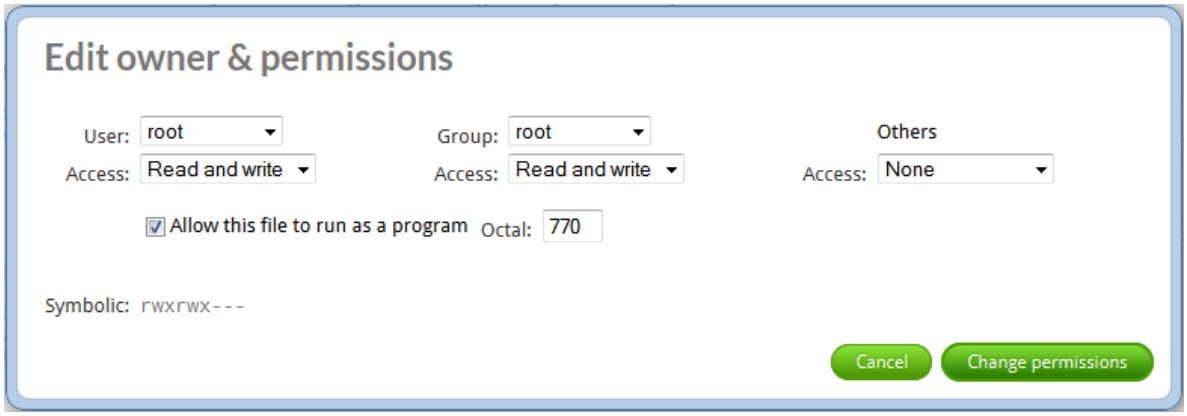

Figura 11: Edición de los permisos del fichero que contiene el *script*

Dejaremos también habilitada la opción "Extract". Quedará, por tanto, de la siguiente forma:

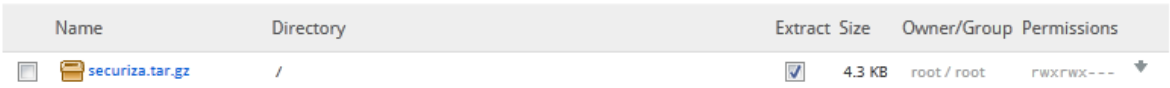

Figura 12: Detalles del fichero que contiene el *script*

9.4.2. SCRIPT DE INICIO

Para iniciar el *script* que acabamos de cargar, será necesario ejecutar ciertos comandos la primera vez que el appliance arranque.

Con este objetivo accederemos a "*Configuration*", subpestaña "*Scripts*". En este punto habilitaremos la opción "*Run script whenever the appliance boots*" y escribiremos el *script* de ejecución del fichero de securización:

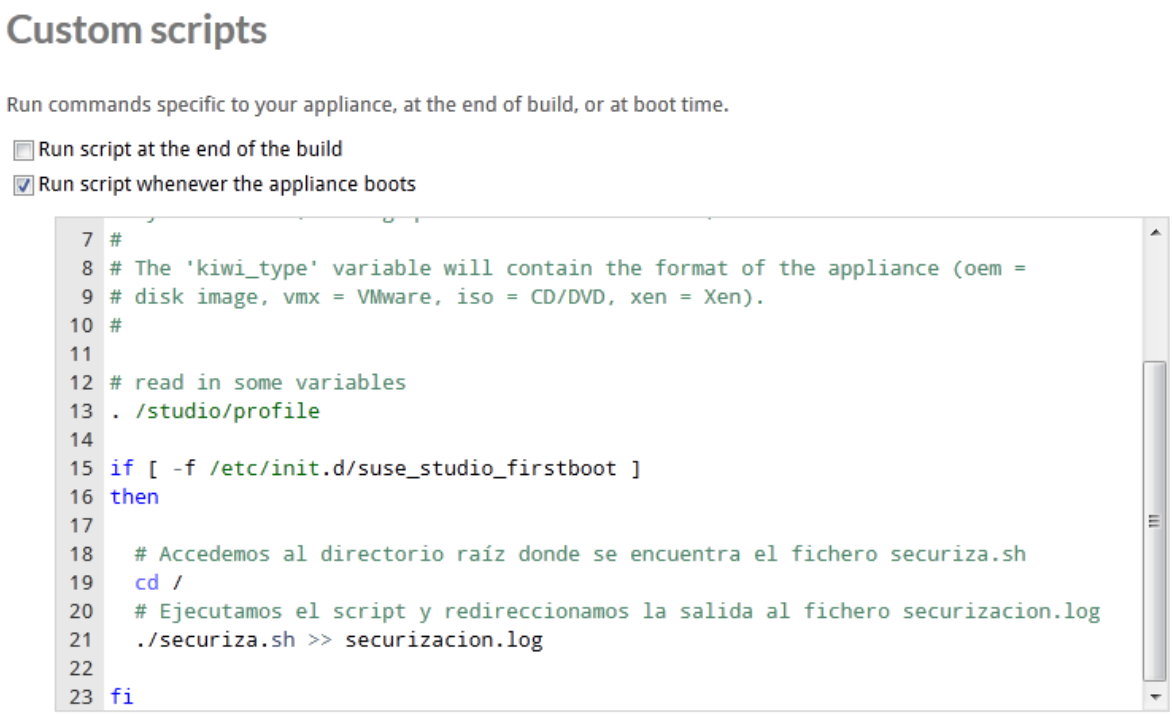

Figura 13: *Script* de ejecución de *securiza.sh*

```
[code]
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
[/code]
```

Tabla 21: [code] Ejecución de *securiza.sh*

9.5. CONSTRUCCIÓN DEL APPLIANCE

Procederemos a crear el appliance para poder descargarlo. Accederemos a la pestaña "Build", elegiremos la versión y el formato, el cual será LiveCD/DVD (.iso), (se ha probado también el formato VMware / VirtualBox / KVM):

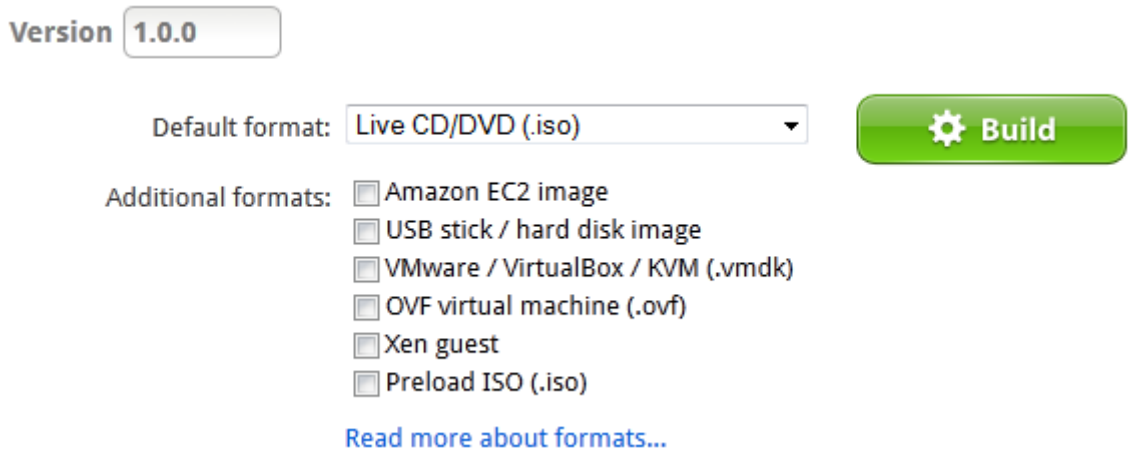

Figura 14: Configuración del LiveCD

Una vez seleccionadas las opciones, pulsamos el botón "Build" y se generará nuestro appliance:

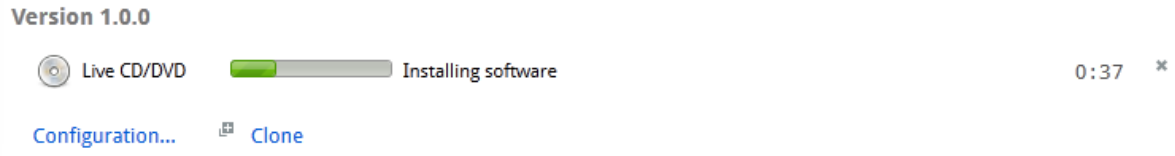

Figura 15: Construcción del appliance

Procederemos entonces a descargarlo pulsando en el botón "Download":

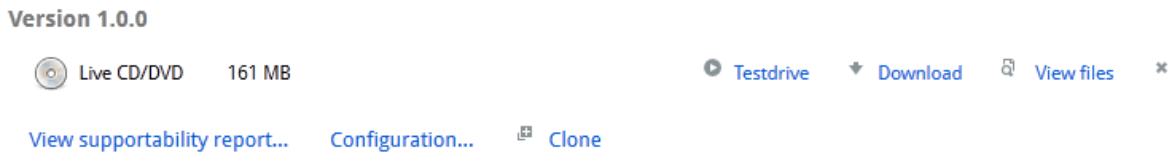

Figura 16: Descarga del appliance

10. EJECUCIÓN DEL LIVECD

En este apartado veremos unos pantallazos del arranque del LiveCD:

Grub

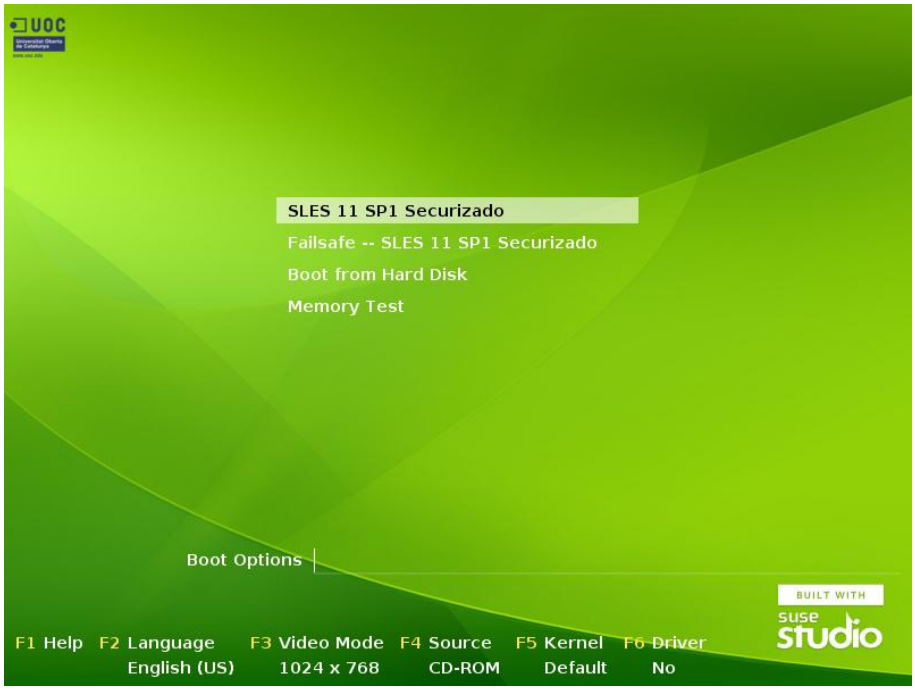

Figura 17: Grub

Bootsplash

Figura 18: Bootsplash

Novell Software License Agreement

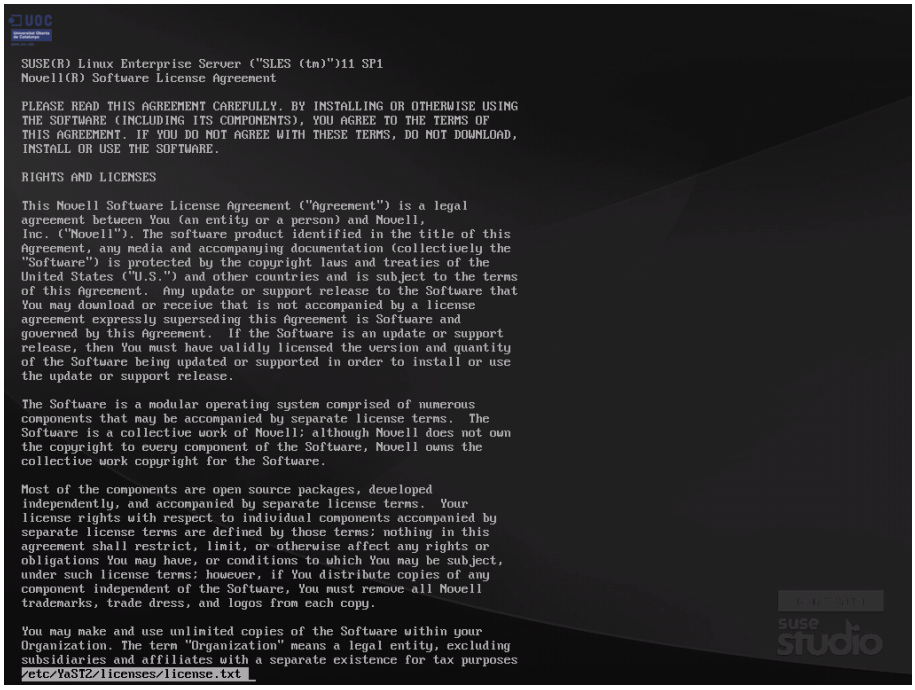

Figura 19: Novell Software License Agreement

Banner creado por nosotros

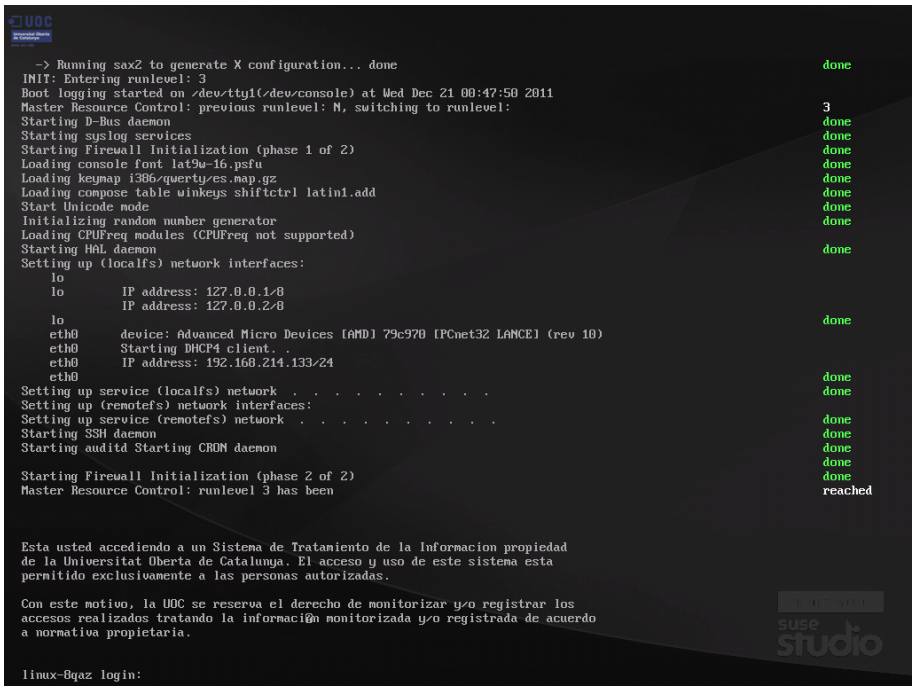

Figura 20: *Banner*

Salida del *script* se securización (*securizacion.log*, ver con el comando *more*)

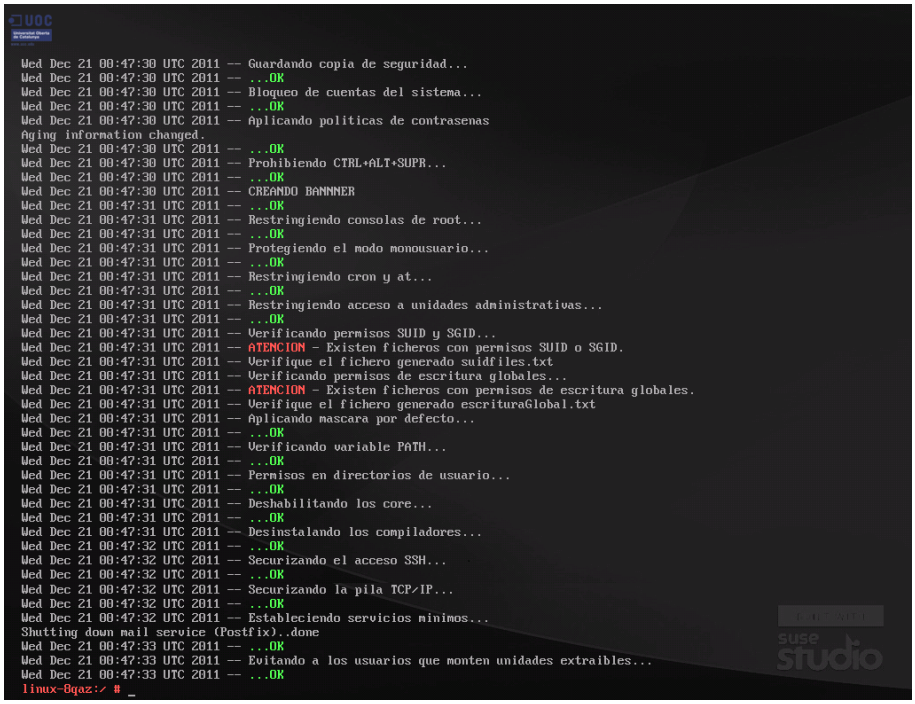

Figura 21: Salida de la ejecución del *script securiza.sh*

Como puede observarse hay ficheros con permisos SUID o SGID y ficheros con permisos de escritura globales, podemos ver la salida de estos dos ficheros a continuación:

escrituraGlobal.txt

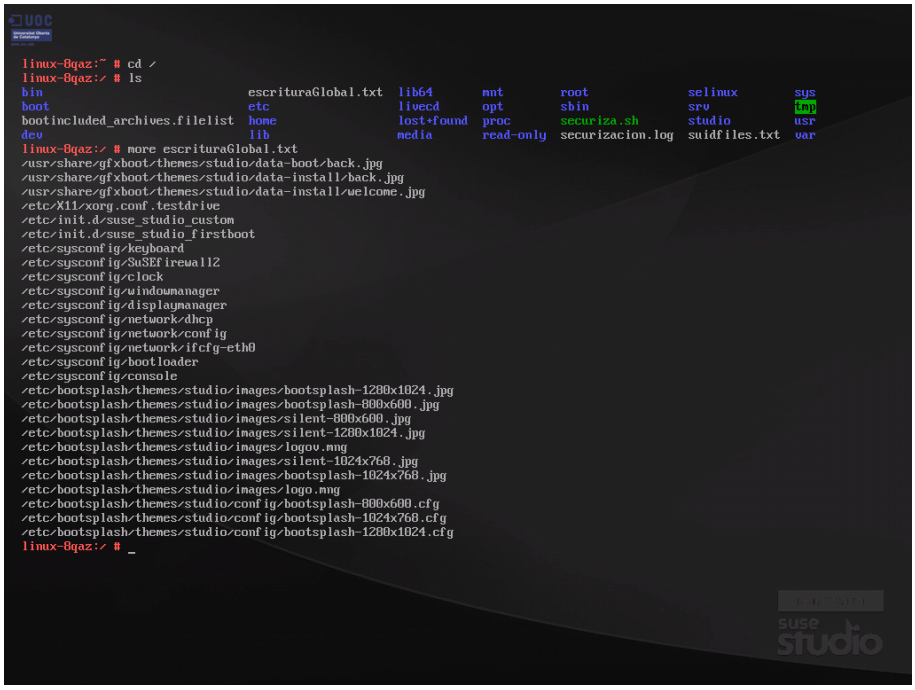

Figura 22: escrituraGlobal.txt

suidfiles.txt

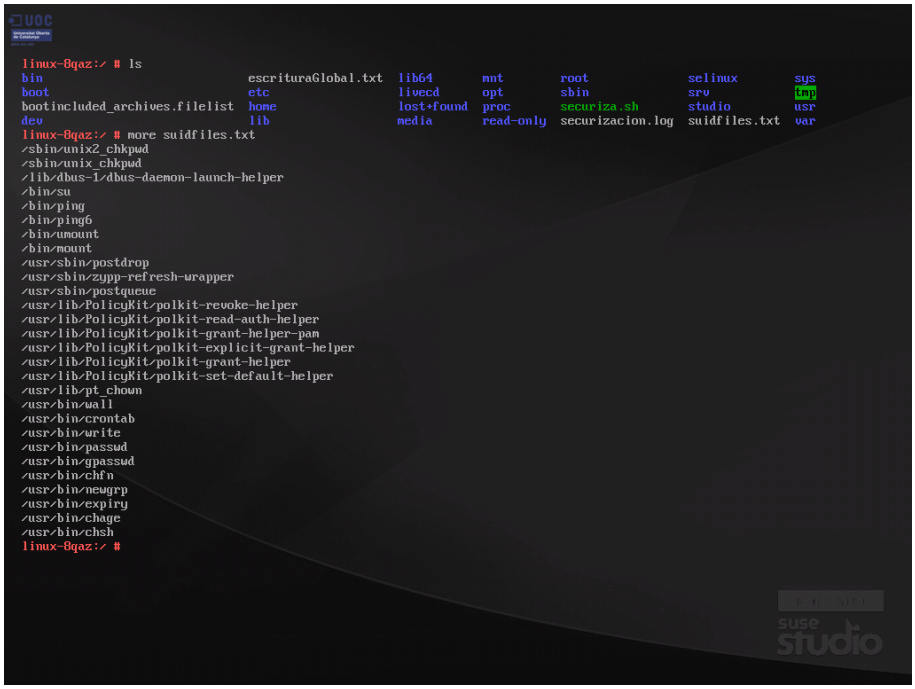

Figura 23: suidfiles.txt

11. CONCLUSIONES

De acuerdo con los objetivos y propósitos establecidos al inicio del proyecto, se han definido un conjunto de políticas de seguridad para aplicarlas a sistemas operativos Suse Linux Enterprise Server. Para poner en práctica estas medidas de seguridad se ha creado un *script* de *bash* para Linux que las implementa.

El producto final consiste en un LiveCD el cual ejecuta durante el arranque este *script* aplicando la securización al sistema operativo. Este CD ha sido generado mediante la herramienta de Novell denominada SUSE Studio la cual permite crear una distribución SUSE a nuestra medida.

Se han logrado objetivos complementarios a la obtención del producto final. En primer lugar se han asentado los conocimientos de seguridad obtenidos durante la carrera. Además, se ha conseguido profundizar en los conocimientos de sistemas operativos Linux, ya que trabajar en su seguridad te permite ahondar en el funcionamiento interno del mismo. Por otro lado, ha sido un reto enfrentarse al *Shell scripting*, donde se han utilizado tecnologías de procesamiento de datos basados en texto muy potentes tales como *awk y sed*.

De esta forma, podemos confirmar que se consigue el objetivo principal: obtener un sistema operativo Suse Linux Enterprise Server bastionado.

El trabajo fin de carrera cumple un papel importante para completar la formación que como Ingeniero Informático he recibido en el periodo de formación universitaria.

11.1. POLÍTICAS DE SEGURIDAD

Para llevar a cabo la definición de las políticas de seguridad, en primera instancia se llevó a cabo un estudio de la literatura. En este estudio se pudo comprobar que es un ámbito complejo debido a la diversidad de factores a tener en cuenta.

En segundo término se profundizó en los distintos elementos a los que íbamos a proceder a bastionar: identificación y autenticación, control de acceso y autorización, seguridad de red, integridad del sistema y mecanismos de auditoría.

La definición de estas políticas se ha desarrollado de tal forma que sean útiles para cualquier sistema operativo Linux.

11.2. LÍNEAS FUTURAS

El trabajo del bastionado de sistemas operativos no debería terminar aquí.

En primer lugar será necesario realizar un *script* lo más genérico posible. Esto permitirá ir adaptándolo a otras distribuciones y obtener versiones estables para cada una de ellas.

Sería interesante profundizar en la configuración de los mecanismos de auditoría. Es un campo de gran valor ya que ofrece información que puede ser inspeccionada para descubrir brechas de seguridad en nuestros sistemas.

En este trabajo nos hemos centrado en el entorno local, por lo que siendo tan común que en el entorno empresarial los servidores pertenezcan al dominio corporativo, sería interesante trabajar en la adaptación a éste. Algunos cambios que podrían implementarse:

- El método de autenticación debería ser acorde al dominio (*Kerberos*, por ejemplo).
- La política de contraseñas vendría definida en dicho dominio, por lo que no sería necesario implementarlo en el *script* de securización.

Los ficheros de auditoría deberán enviarse a un servidor de centralización de *logs* externo a las máquinas, para llevar un control centralizado de todas ellas.

12. BIBLIOGRAFÍA

GITE, Vivek.: Linux Shell Scripting Tutorial (LSST) v2.0 [en línea] 301 p. Escrito por Vivek Gite. Disponible en Web: <http://nixcraft.com/shell-scripting/13583-pdf-download-linux-shell-scripting-tutorial-v2-0-a.html>

1. CISECURITY, the CENTER for INTERNET SECURITY: Center for Internet Security SUSE Linux Enterprise Server Benchmark [en línea]. <http://benchmarks.cisecurity.org/tools2/linux/CIS_SUSE_Linux_Benchmark_v2.0.pdf>

2. NUSEPAS, Blackhold: Securizando los accesos a un sistema GNU/Linux [en línea]. <http://blackhold.nusepas.com/2011/02/securizando-los-accesos-a-un-sistema-gnulinux/>

3. NOVELL: SLES 11 Administration Guide [en línea] 552 p. <http://www.novell.com/es-es/documentation/sles11/pdfdoc/book_sle_admin/book_sle_admin.pdf>

4. NOVEL: Linux Audit Quick Start [en línea] 6 p. <http://www.novell.com/es-es/documentation/sles11/pdfdoc/art_auditquick/art_auditquick.pdf>

5. NOVEL: SLES 11 Security guide [en línea] 458 p. <http://www.novell.com/es-es/documentation/sles11/pdfdoc/book_security/book_security.pdf>

6. SOFTLAYER: Enabling and Disabling Services within SLES [en línea]. <http://knowledgelayer.softlayer.com/questions/446/Enabling+and+Disabling+Services+within+SLES>

13. ANEXOS

13.1. LISTAS DE DISTRIBUCIÓN RECOMENDAS

- SecurityFocus: http://www.securityfocus.com
  - bugtraq@securityfocus.com: lista de distribución de bugs para distintos entornos.
  - vuln-dev@securityfocus.com: lista de distribución de vulnerabilidades para distintos entornos.
  - focus-linux@securityfocus.com: vulnerabilidades sobre entornos Microsoft
- Novell: los usuarios suscritos a las listas podrán consultar información como cuál es el problema, a qué producto afecta, cómo protegerse de la vulnerabilidad, etc. Para subscribirse a cualquiera de las listas, se debe acceder a:

  https://secure-www.novell.com/center/regadmin/jsps/notification_app.jsp (se requiere estar registrado).

13.2. PARCHES

Para poder descargar y consultar los últimos parches se deberá tener una suscripción con Novell.

13.3. NORMATIVA Y CERTIFICACIÓN

El estándar ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Disponer de un SGSI y obtener la certificación de ISO/IEC 27001, permitirá a una compañía ofertar a sus clientes el tratamiento de su información de manera segura.

El hecho de seguir el procedimiento de bastionado descrito anteriormente garantiza el cumplimiento de aspectos fundamentales del estándar ISO/IEC 27001, tales como control de acceso y auditoría.