-- ASEGURAR-SISTEMA --

OJO Cualquier aplicación que quiera ponerse a la escucha en un puerto bajo (menor al 1024) debe correr con privilegios de root.

---------------------- >
Editaremos el archivo /etc/pam.d/su y buscaremos las líneas que dicen
auth required pam_wheel.so
lograremos que solo quien pertenezca al grupo root pueda escalar a superusuario con el comando su.
addgroup --system wheel (creamos el grupo whell con permisos de sistem)
y luego en /etc/pam.d/su dejamos la linea del siguiente modo(descomentamos):
auth required pam_wheel.so group=wheel
Luego agreguemos al grupo wheel a los usuarios que deseamos que escalen a superusuario con su.

------------------ >
/ETC/PASSWD
Usuarios de sistema, en debian se caracterizan por tener un UID menor que 1000, que tienen como interprete de comandos a */bin/sh, eso está mal, esos usuarios no deberían poder ejecutar ordenes de consola. Si bien esos usuarios no pueden hacer login, ya que en/etc/shadow hay un * donde debería estar el hash de su password, les quitaremos el shell para estar seguros ya que no lo necesitan, para eso
utilizaremos la utilidad chsh (change shell)
chsh -s /bin/false daemon
chsh -s /bin/false bin
...
chsh -s /bin/false nobody

-------------------- >
GRUB
Si estamos utilizando grub podríamos querer asegurarnos que nadie pueda modificar los parámetros que se envía al kernel durante el arranque, a eso lo lograremos colocando un password al grub.
(OJO)Solo si instalamos el sistema separando la partición /boot
mount -t ext3 /dev/hda1 /boot
$ grub-md5-crypt
Password:
Retype password:
1XPXwl$59U9fEc5VgKjVzN.cinQ31
Editemos ahora el archivo /boot/grub/menu.lst
Buscamos: password ['--md5'] passwd
y debajo añadimos asi nuestro passwd generado:
password --md5 1XPXwl$59U9fEc5VgKjVzN.cinQ31
Busquemos ahora la línea que dice lockalternative y dejémosla así:
should update-grub lock alternative automagic boot options
e.g. lockalternative=true
lockalternative=false
lockalternative=true
IMPORTANTE: No debe descomentar la línea lockalternative, solo debe reemplazar false por true.
También modificaremos los permisos de /boot/grub/menu.lst para evitar que los usuarios no privilegiados accedan al hash: chmod 600 /boot/grub/menu.lst

------- >

```
# ARCHIVO /ETC/SYSCTL.CONF
# Podemos descomentar esta línea si deseamos evitar que klogd envíe los
# mensajes a consola, esto logrará que no aparezca en pantalla algo
# trivial como cuando se conecta un cable de red pero omitirá información
# importante como por ejemplo un Out_Of_Memory
#kernel.printk = 4 4 1 7
#
# Ignorar la tecla petición de sistema, esto nos impedirá hacer un cierre
# limpio del sistema en caso de cuelgue
#kernel.sysrq=0
#
# Protección básica contra ataques de Spoof, a un paquete se lo aceptará solo si
# la dirección IP de origen es alcanzable desde la interfaz por la cual ingresó.
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
#
# Ignorar ICMP broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
#
# Ignorar ICMP que informan errores en paquetes que nosotros no hemos
transmitido.
net.ipv4.icmp_ignore_bogus_error_responses = 1
#
# No aceptar redirección de ICMPs
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
#
# Ni tampoco enviarlos
net.ipv4.conf.all.send_redirects = 0
# No aceptar información de source route (no somos un router)
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
#
# Un paquete marciano es justamente eso, un paquete que parece venido de
# otro mundo, por
# ejemplo: si mi interfaz de red esta configurada con una IP
  200.100.53.9/255.255.255.224
# ¿Como carajos me ha llegado un paquete cuya trama ethernet tiene mi
  dirección MAC
# pero la IP de destino es 10.0.0.5? Bueno, no tengo la menor idea, eso es un
  marciano.
# Loguear paquetes marcianos puede ser deseable
  net.ipv4.conf.all.log_martians = 1
  Para lograr que el kernel tome la nueva configuración:
# sysctl -p

# -------------- >
CERRAR SESION EN TERMINALES POR INACTIVIDAD A LOS 5 MINUTOS
Si es solo para root es en su .bashrc, si es para todos en /etc/profile le añadimos
esta línea:
readonly TMOUT=300

# ---------------- >
QUITAR EL SUID A DIRECTORIOS PELIGROSOS (rws------)(quitar privilegios a
usuarios)
/usr/bin/passwd: para que los usuarios puedan cambiar su password.no es muy
importante
```

/usr/bin/chsh: para que los usuarios puedan cambiar su shell por defecto.
/usr/bin/newgrp y /usr/bin/gpasswd: cambiar de grupo y cambiar el password a un grupo, es una funcionalidad poco conocida de Linux, se comporta analogo a lo que son passwd y su pero a nivel de grupos. gpasswd permite asignar password a los grupos para que, mediante newgrp, un usuario pueda cambiar su identificador de grupo, previa autenticación. Si lo cree conveniente puede quitar el bit SUID a estos programas.
/usr/bin/gpg: en ciertas versiones no esta activo el bit de SUID.
/usr/sbin/exim4: puede que no este instalado
/bin/su: para poder escalar/degradar privilegios. Seguramente no desee quitar el bit SUID a este comando
si esta en su equipo de trabajo, para un servidor si vale, habría que logearse en tty como root
/bin/mount y /bin/umount: para poder montar y desmontar dispositivos como usuario no privilegiado.
/bin/ping, /bin/ping6 y /bin/traceroute.lbl Para hacer ping

Quitemos esos permisos entonces, para hacerlo basta con ejecutar
chmod -s archivo_ejecutable
update-grub

------------------ >
ASEGURARNOS CONTRA ATAQUES "FORK" (bucle infinito para agotar el sistema)
agregando una línea como ésta en el archivo /etc/security:
/limits.conf :
* hard nproc (número de procesos que deseamos poner como máximo, por ej 500).

------------------ >
DESHABILITANDO EL cTL+aLT+sUPR
/etc/inittab y busquemos donde dice:
What to do when CTRL-ALT-DEL is pressed.
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
ca es el id, donde dice 12345 se refiere a los runlevels en los cuales, tras el evento ctrlaltdel se llevará a cabo la acción /sbin/shutdown -t1 -a -r now.
Entonces las alternativas son:
* Podemos comentar la línea para que no se realice ninguna acción tras presionar Ctl+Alt+Supr.
* Podemos dejar solo el numero 1 en la columna de runlevels para que la característica se mantenga si hemos ingresado en modo single user.
* Podemos quitar el 2 de la columna runlevels para que la característica se mantenga en los demás runlevels pero no en el runlevel por defecto.
* Podemos leer el man de shutdown y sorprendernos al saber que la opción a significa que si existe el archivo /etc/shutdown.allow la orden shutdown solo se respetará si root a algún usuario listado en dicho archivo está logueado en alguna tty.
Dejaremos /etc/inittab como está y haremos:
echo root > /etc/shutdown.allow
funciona en el momento.

-------------------- >
CRONTAB Y AT (tareas programadas)
Si queremos que nadie pueda programar tareas excepto root crearemos:
/etc/crontab.allow
/etc/at.allow

------------------------ >
CAMBIAR EL NOMBRE A ROOT [Básico].

```
usermod -l pernambuco root

# ------------------------ >
Almacenar logs remotamente [Critico] (leer el manual)
```