UNIX/LINUX HOST SECURITY

Vers. 1.3 del 20/12/2005

Premessa

Questo documento contiene alcune raccomandazioni che l'Amministratore di Sistema dovrebbe tenere presente al momento della installazione e amministrazione di sistemi operativi Unix/Linux. Le indicazioni riportate si riferiscono in particolare alle distribuzioni Linux RedHat, Scientific Linux e Fedora, ma possono essere estese ad altre distribuzioni o sistemi Unix proprietari.

Le misure di sicurezza qui indicate sono da considerare come misure di sicurezza "minime". Spetta all'amministratore, con la sua conoscenza delle esigenze dell'Unità Operativa a cui fa riferimento la decisione finale sull'opportunità o meno di certe misure.

Se l'host fornisce un servizio centralizzato (ad esempio è un server WWW, FTP, BIND o altro) si raccomanda inoltre la lettura del documento specifico dedicato alla sicurezza di tali sistemi [ref. 1].

Installazione e configurazione

La fase di installazione e configurazione di sistemi operativi Unix/Linux deve essere coordinata con i Servizi di Calcolo presenti nell'Unità Operativa, secondo le modalità stabilite dai Servizi stessi.
I Servizi, ove possibile, dovrebbero predisporre un sistema di installazione semiautomatica (ad es. tramite *kickstart)*, in modo da armonizzare le politiche di sicurezza. Un esempio di kickstart è riportato in Appendice.

I principi generali da seguire durante la fase di installazione sono i seguenti:

- evitare di collegare alla rete sistemi preinstallati o dei quali non si conosce in dettaglio la configurazione
- scegliere, dove possibile, versioni del sistema operativo recenti e stabili
- rimuovere il software non necessario, disattivare i servizi e chiudere le porte inutili
- subito dopo l'installazione applicare tutti gli aggiornamenti e le patch di sicurezza disponibili.

Se la macchina opererà in un ambiente dove hanno libero accesso studenti o altre persone non soggette alla politica di sicurezza informatica dell'INFN, si consiglia di disabilitare il *boot* da floppy o CD, impostare una password al BIOS e all'accesso in modalità *single-user*.

Gestione operativa

Aggiornamento

Il sistema deve essere mantenuto il più possibile aggiornato. I pacchetti di cui sono note vulnerabilità gravi devono essere immediatamente aggiornati o disinstallati. I Servizi, ove possibile, possono predisporre dei sistemi di aggiornamento automatici, di mirroring delle distribuzioni linux più diffuse o di notifica degli aggiornamenti disponibili.

Il servizio di "Security alert" via e-mail del GARR-CERT fornisce informazioni tempestive sulle vulnerabilità più gravi; in generale però si raccomanda di visitare periodicamente il sito della distribuzione installata per verificare la presenza di altre *patch* o aggiornamenti.

Account e password

La gestione degli account e l'impostazione delle password dovrebbe in generale seguire alcuni principi di sicurezza di base:

- ogni account deve essere riferito ad una sola persona
- ogni account deve essere protetto da una password.

Inoltre:

- se possibile usare le *shadow password* e *md5*
- eseguire periodicamente *John the Ripper* o *crack* sui file di password per scoprire quali sono facilmente indovinabili
- rimuovere gli account e i gruppi di default non necessari:
  - `userdel adm, lp, shutdown, halt, news, mail, uucp, operator, games, gopher, ftp`
  - `groupdel adm, lp, news, mail, uucp, games, dip`
- disabilitare gli account speciali (ad es. *bin*) mettendo */bin/false* come shell in */etc/passwd*
- disabilitare immediatamente gli account utente non più necessari
- controllare periodicamente che gli account vengano usati e disabilitarli in caso contrario; in alternativa, creare gli account con una data di scadenza
- gli account sono personali: se è necessario condividere file, utilizzare i gruppi
- limitare ai casi strettamente necessari l'uso dell'account di *root;* disabilitare il login tranne che da console *(*tramite */etc/ttys* o */etc/ttytab*), utilizzando invece ssh e su
- verificare che il PATH non contenga **.** (la directory corrente)
- controllare che tutti i file eseguiti durante il login e da cron siano di *root* e non siano scrivibili da tutti.

Password

Molte password sono facilmente indovinabili in pochi tentativi e non tutti i programmi segnalano sui log di sistema i tentativi falliti (ad es. alcune versioni di **pop3**).
Gli utenti tendono ad avere la stessa password su tutti i sistemi, quindi una compromissione di una macchina spesso porta alla compromissione di tutte le altre a cui l'utente ha accesso.

Il file di password (specie se non si usano le *shadow password*) può essere facilmente letto da un estraneo, che lo può poi analizzare con comodo con uno dei tanti programmi esistenti (ad es. **John the Ripper**).
Alcuni sistemi venivano distribuiti con account senza password o con password standard, che non sempre vengono modificate durante l'installazione.

Per rendere le password un po' più difficili da indovinare si consiglia di rispettare le regole seguenti:

- utilizzare almeno 6 caratteri (meglio 8), comprendendo almeno un numero e un carattere speciale (. , - _ $ %)
- non utilizzare nomi o date in nessuna lingua
- cambiare periodicamente le password
- evitare di utilizzare la stessa password su diversi host
- impedire il login dopo un certo numero di tentativi di accesso falliti.

Accesso al sistema

L'accesso al sistema può essere controllato (impedito, limitato e/o monitorato) in diversi modi:

- il controllo dell'accesso a servizi e risorse da parte di host specifici viene configurato mediante *tcp_wrapper* (ovvero tramite i file */etc/hosts.allow* e */etc/hosts.deny*) e *xinetd*
- il controllo dell'accesso a servizi e risorse da parte di specifici utenti o applicazioni viene configurato tramite le librerie PAM (ref [2], capitolo 4)
- il controllo dell'accesso a porte o servizi da rete può inoltre essere configurato tramite *ipchains* o *iptables*.

Accesso come root

L'accesso come root dovrebbe in generale essere utilizzato solo in casi di assoluta necessità e comunque mai da remoto. E' possibile impedire il collegamento remoto attraverso i file */etc/ttys*, */etc/ttytab* e */dev/default/login*.

Gli amministratori di sistema potranno collegarsi da remoto utilizzando il proprio login e facendo successivamente *su*, in modo da lasciare traccia di chi abbia compiuto eventuali operazioni.

Accesso in single-user

Accedendo al sistema in modalità *single-user* non viene chiesta la password. Se al pc linux possono aver accesso non controllato persone diverse, è meglio disabilitare questa caratteristica, poiché basta un semplice reboot perché chiunque possa aver accesso al sistema come root.
Una possibilità è inserire in */etc/inittab* la richiesta che, al momento dello startup in single-user, venga richiesta la password di root:

```
id:3:initdefault:
~~:S:wait:/sbin/sulogin
```

File System

Per quanto riguarda la sicurezza dei file-system, si consiglia di seguire perlomeno le misure di sicurezza qui elencate:

- script setuid: non ne esistono di sicuri, usate *super* o *sudo*
- settate il *bit sticky* sulle directory pubbliche (chmod o+t)
- gli utenti non devono poter cancellare e rinominare i file di altri utenti
- in particolare */tmp* deve essere di root:system
- settate il bit setgid sulle directory pubbliche (chmod g+s)
- il gid dei nuovi file è quello della directory
- controllate che i file con i bit suid o sgid siano legittimi.
- controllate file e directory scrivibili dal gruppo e dal mondo
    - `find / -type f \( -perm -2 -o -perm -20 \) - exec ls -lg {} \;`
      `find / -type g \( -perm -2 -o -perm -20 \) - exec ls -lg {} \;`
- controllate gli umask: quello di root deve essere almeno 0x22.
- quando possibile montate i file system non-setuid e read-only.

Condivisione di file-system: nfs

Si tratta di un servizio intrinsecamente insicuro, poiché è basato su UID e GID dell'utente remoto. Se è necessario usarlo, si raccomanda di configurarlo correttamente impostando alcune restrizioni:

- in */etc/exports* evitate wildcards, impedite l'accesso a root e, dove possible, montate il file-system in read-only:
    - `/dir-da-esportare  host.amico.xx (ro, root_squash)`
- mai esportare un filesystem al mondo!
- controllate la vostra situazione con: *showmount -e* (e *-a*)
- attenzione a cosa importate *(/etc/fstab* o */etc/amd.conf*): usate nosuid, se potete
- filtrate le porte 111 e 2049 (TCP e UDP)
- inserite il servizio portmapper fra quelli controllati da tcp_wrapper in */etc/hosts.allow* e */etc/hosts.deny*

Macchine "fidate"

Per semplificare i processi di autenticazione e autorizzazione, alcuni servizi e applicazioni permettono di configurare macchine remote come macchine "fidate", dalle quali è possibile accedere direttamente al servizio o applicazione anche in modo non interattivo. La configurazione di queste relazioni di fiducia è in generale sconsigliata.
Se è necessario utilizzarle si consiglia di:

- usare i *tcp_wrappers* (o *xinetd*)
- cercare di ridurre al minimo le macchine da cui si accetta il login senza autorizzazione (comandi r* o anche ssh), in ogni caso mai esterne alla LAN
- utilizzare */etc/hosts.equiv* e proibite l'uso di *~/.rhosts* (anche per root!)
    - controllate che *hosts.equiv* non contenga +
    - *hosts.equiv* deve essere di root e con permesso 600
    - non esistono caratteri di commento in questi file!
- verificare periodicamente che non esistano file *.rhosts*
    - `find / -name .rhosts -ls`
- non usare *.netrc*
- filtrare le porte 512, 513 e 514 (TCP).

Servizi r*

Col nome generico *servizi r** si indicano i servizi **rsh**, **rlogin**, **rexec** (*shell*, *login* e *exec*, rispettivamente), che consentono di collegarsi ad una macchina remota, in qualche caso senza necessità di digitare una password.
Considerare una macchina "fidata" (ad es. inserendola in **.rhosts**) è doppiamente pericoloso, sia se viene compromessa, sia se viene impersonata dall'attaccante (ad es. tramite *ip-spoofing*).
Non sempre il loro uso viene registrato e/o disabilitato dopo qualche tentativo falllito: sono quindi meccanismi ideali per provare combinazioni di user e password.

Se possibile evitare quindi l'accesso al sistema tramite i servizi r* e controllare periodicamente la presenza di file *.rhosts, .forward, .netrc, hosts.lpd, hosts.equiv* e il loro contenuto (ad esempio, un segno + nei file).

rpc, portmapper (porta 111) è il punto di accesso "ufficiale", ma i servizi possono essere contattati direttamente saltando i controlli di sicurezza: è sufficiente **rpcinfo** per conoscere le porte su cui ascoltano.
Alcuni implementazioni di questi servizi, anche recenti, hanno vulnerabilità ben note. Tra i più diffusi: **rexd**, **statd** (o **status**), **mountd**.
Controllate i servizi attivi (via *portmapper*):

```
$ rpcinfo -p
program  vers    proto   port
100000   2       tcp     111  rpcbind
100000   2       udp     111  rpcbind
100024   1       udp     815  status
100024   1       tcp     817  status
100021   1       tcp     821  nlockmgr
100020   1       udp   1048 llockmgr
100068   5       udp   1051
100005   1       udp   899   mountd
100003   2       udp   2049  nfs
```

Eliminate i servizi che non servono, in particolare:

- *rexd* (sempre!)
- *statd* (o *status*) e *mountd* (se non usate NFS)

X11

I display X11 e i caratteri battuti sulla tastiera, se non protetti opportunamente, possono essere visti anche da un'altra macchina.
Non permettete accessi X11 dall'esterno:

- Bloccate le porte 6000-6030 sul router di accesso alla LAN e usate X11 solo in tunnelling ssh
- Controllate periodicamente le macchine sulla vostra LAN (ad es. con nmap e xscan) per verificare che le protezioni di accesso siano corrette.

Varie

- Preparatevi una copia delle più importanti utility (*ls, find, du, ps, netstat, lsof*, ecc.) linkate staticamente e conservatele in un posto sicuro.
- Controllate periodicamente che l'interfaccia ethernet non sia in modo promiscuo.
- Devices
    - */dev/mem* e */dev/kmem* non devono essere leggibili dal mondo
    - quasi tutti i device devono essere di root (eccezione i terminali)

    - attenzione ai file normali in /dev!
- Se usate inetd, commentate in /etc/inetd.conf tutte le righe tranne quelle indispensabili. In particolare, oltre a quelle già discusse:
    - *echo*, *chargen* (attacchi DoS)
    - *finger* (o al massimo sostituitelo con *safe-finger*), *who*, *systat*
    - *uucp*

Monitoraggio

Eseguire, previo accordo con i Servizi di Calcolo locali, port-scanning (ad es. con nmap) per controllare l'elenco delle porte e dei servizi aperti, ed effettuare un controllo incrociato con la lista delle porte e dei servizi autorizzati dal firewall/router della LAN.

Per controllare l'integrità dei file di sistema si consiglia di installare un programma di controllo come *tripwire*.

Verificare la presenza dei seguenti programmi, alcuni dei quali sono affetti da gravi vulnerabilità o sono intrinsecamente insicuri:

- **finger**, **systat**, **netstat**, **rusers**, **rwho** forniscono informazioni preziose: chi sta lavorando al momento, da quanto tempo non ha fatto login, dove sono le home directory, ecc.

Controllare periodicamente la presenza di file con il bit SUIG/SGID abilitato:

- `find / -type f \( -perm -04000 -o -perm -02000 \) -exec ls -l {} \;`

Controllare l'eventuale presenza di file con il nome insolito, come ad esempio "..." (tre punti) o ".. " (punto punto spazio) o "..^G" (punto punto control-G):

- `find / -name ".. " -print -xdev`
- `find / -name ".*" -print -xdev | cat -v`

Controllare l'eventuale presenza di file e directory scrivibili al mondo:

- `find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg {} \;`
- `find / -type d \( -perm -2 -o -perm -20 \) -exec ls -ldg {} \;`

Controllare anche l'eventuale presenza di file che non appartengono a nessuno (tralasciando ciò che viene riportato eventualmente dalla directory /dev):

- `find / -nouser -o -nogroup`

Controllare periodicamente la presenza di file .rhosts; se è necessario che esistano, verificare perlomeno che non contengano wildcards o righe di commento.

Controllare infine:

- cron files scrivibili
- /*tmp* con permessi sbagliati

Vulnerabilità

Una lista "ufficiale" delle maggiori vulnerabilità viene mantenuta dal SANS Institute [ref 4].
La maggior parte di queste vulnerabilità può essere affrontata seguendo due semplici principi:

1. Evitare di mettere in rete un nodo linux o unix acquistato preistallato: potrebbero essere stati attivati servizi pericolosi o non necessari e il sistema potrebbe essere non aggiornato o patchato, presentando e bachi o vulnerabilità.
2. Utilizzare il più possibile le versioni stabili e aggiornate del sistema operativo e delle applicazioni, avendo cura di verificare al termine dell'installazione l'eventuale esistenza di nuovi aggiornamenti o patch.

File di log

Il mantenimento e l'analisi periodica dei file di log rappresentano pratiche che possono aiutare a risolvere problemi di sicurezza oltre che di malconfigurazione dei sistemi.
Si raccomanda quindi di valutare e adeguare il livello di logging di ogni macchina, la durata della permanenza dei log nei dischi e la loro rotazione secondo la criticità del sistema.

Logging remoto: dove possibile, si raccomanda di mantenere una copia dei messaggi su di un'altra macchina (*loghost* nell'esempio seguente)

```
*.info;mail.none;authpriv.none /var/log/messages
*.info;mail.none;authpriv.none @loghost
authpriv.*                     /var/log/secure
authpriv.*                     @loghost
mail.*                         /var/log/maillog
*.emerg                        *
*.emerg                        @loghost
```

Backup

Effettuare regolari backup di sistema e, periodicamente, prove di *restore* da backup.

Riferimenti

[1] "Servizi Centralizzati"

[2] "Securing & Optimizing Linux: The Ultimate Solution", http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-The-Ultimate-Solution-v2.0.pdf

[3] Linux Documentation Project, http://www.tldp.org/guides.html

[4] "SANS TOP20 vulnerabilities, http://www.sans.org/top20/

Bibliografia

- xscan: http://www.xfocus.org/programs/
- sudo: http://www.courtesan.com/sudo/
- super: http://www.ucolick.org/~will/
- Simson Garfinkel, Gene Spafford, Practical Unix and Internet Security, 2nd Ed. O'Reilly & Associates (1996)
- Joel Scambray, Stuart McClure e George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, 3rd Ed., Osborne/McGraw-Hill (2001)
- CERT: Unix configuration guidelines http://www.cert.org/tech_tips/unix_configuration_guidelines.html

Appendice. Esempio di kickstart per Scientific Linux

Quello che segue è un estratto dello script di kickstart utilizzato nella Sezione INFN di Bologna. È stato anche riportato uno script per la configurazione dei tcp_wrapper e del logging remoto che viene lanciato automaticamente dal kickstart al termine dell'installazione.

Alla fine dell'installazione usare il comando *redhat-config-xfree86* (da root) per configurare la grafica.

```
#######################################################
#  COPIARE QUESTO FILE SU UN FLOPPY DOS, COL NOME ks.cfg
# Bootstrappare da cd
# Al prompt boot: linux ks=floppy
#######################################################
# Per lingua di default italiana
#lang it_IT
lang en_US
langsupport en_US
#langsupport it_IT --default en_US
keyboard us
install
cdrom
# Per installazione da rete commentare la riga precedente e scommentare la seguente
#nfs --server lnxsrv.bo.infn.it --dir /linux/scientific/305/i386
network  --bootproto static --ip 131.154.10.xxx --netmask 255.255.255.0 --gateway
131.154.10.9 --nameserver 131.154.10.4 --hostname pctest.bo.infn.it
zerombr yes
clearpart --all --drives=hda
# Per piu' dischi eide: hda,hdb,...
#part /home --size 100 --grow --ondisk hdb
# Per piu' dischi scsi: sda,sdb,...
#part /home --size 100 --grow --ondisk sda
# Per fare un check dei settori delle partizioni del disco:
#part --badblocks /boot ...
#
part swap  --size 2000 --ondisk hda
part /boot --size  100  --ondisk hda
part /usr  --size 7000  --ondisk hda
part /var  --size 2000  --ondisk hda
part /tmp  --size  500  --ondisk hda
part /     --size 2000  --ondisk hda
part /home --size  100  --grow --ondisk hda
mouse
#mouse genericps/2 --emulthree
#
# If you would like to have your system's hardware clock set to use GMT/UTC,
#  add the --utc option the timezone line.
#timezone --utc Europe/Rome
timezone Europe/Rome
#### xconfig --monitor Generic06 --vsync "50-90" --startxonboot
#### xconfig --startxonboot
# xconfig --depth=32 --resolution=1024x768 --defaultdesktop=GNOME --startxonboot
skipx
rootpw --iscrypted RONl3M9P1.IUw
#firewall --high
auth --useshadow --enablemd5
bootloader
#reboot
%packages
@ X Window System
@ GNOME Desktop Environment
@ Editors
@ Engineering and Scientific
@ Graphical Internet
@ Office/Productivity
@ Sound and Video
@ Graphics
@ Authoring and Publishing
@ Development Tools
@ KDE Desktop Environment
```

```
@ OpenAFS Client
@ Packages added to Scientific Linux
#------------ extra packages ----------
lynx
gv
compat-libstdc++
rhpl
XFree86-devel
yum
pine
############################################################
%post
#/bin/touch /mnt/sysimage/etc/mail/*.db

#
# Setup Network
#
cat <<EOF> /etc/resolv.conf
search bo.infn.it
nameserver 131.154.10.4
nameserver 131.154.11.102
EOF
#echo 'pctest.bo.infn.it' > /etc/HOSTNAME

#####################################################
# The following is executed during the first boot
#####################################################
cat <<EOF> /etc/init.d/postinstall
#!/bin/bash
# Avoid users to halt the machine...?
######chmod 750 /usr/bin/consolehelper
#
# Set KDE as default
#
#echo DESKTOP="KDE" > /etc/sysconfig/desktop
mkdir /linux
mount 131.154.10.107:/linux /linux
#cp /linux/config/yum-scientific.conf /etc/yum.conf

# aggiungo pacchetti extra con yum
yum -y install xmms

# tolgo l'applet dell'rhn (quello rosso in basso a destra):
    yum -y remove rhn-applet

# questo altrimenti non funziona acroread:
perl -pi -e 's|en_US\.UTF-8|en_US|g' /etc/sysconfig/i18n

# questo per impostare il server di posta per sendmail:
perl -pi -e 's/^DS/DSlnxm.bo.infn.it/g' /etc/mail/sendmail.cf

# setta il server INFN di ntp
perl -pi -e 's/^server.*/server  server11.infn.it/g' /etc/ntp.conf
#
# Update et al.
#
/linux/scripts/update
/linux/scripts/cups-conf.pl
/linux/scripts/makePeriodic.pl
#
#unalias cp
cp -fr /linux/skel /etc/
cp -f /linux/profile.d/* /etc/profile.d/.

#PROBLEMA: cosi' l'installazione avviene in ordine alfabetico e si perdono le
#dipendenze (per es, si cerca di installare prima openafs-client e poi
#openafs-kernel invece del contrario). Ma se si fa 'rpm -Uvh *' e se c'e' gia'
#un pacchetto installato non ne installa di non installati.

rpm -ivh /linux/contrib/all/*.rpm
for i in /linux/contrib/scientific/305/*.rpm ;do
  k=\`basename \$i| awk -F- '{printf("%s",\$1); for (j=2;j<=NF-2;j++) printf("-%s",
\$j)}'\`
  a=\`rpm -qi \$k\`
  if [ "\$a" = "package \$k is not installed" ]; then
    rpm -Uvh \$i
  fi
```

```
done


### Se e' dual boot installo il modulo ntfs
#if [ "No" != "No" ]; then
#  arch=\`uname -m\`
#  rpm -Uvh /linux/fedora/updates/305/\$arch/kernels/kernel-ntfs*.rpm
#fi
#
# stop and start some services
#
#/sbin/chkconfig sendmail off
/sbin/chkconfig isdn     off
/sbin/chkconfig iptables off
/sbin/chkconfig ntpd     on
#
# Installation of non RPM packages
#
#ver=\`rpm -q --queryformat "%{VERSION}" mozilla\`
#cp /linux/contrib-norpm/*flashplayer* /usr/lib/mozilla-\$ver/plugins/.
#cp /linux/contrib-norpm/ShockwaveFlash.class /usr/lib/mozilla-\$ver/plugins/
# questo richiede j2re:
ln -s /usr/java/jre1.5.0/plugin/i386/ns7/libjavaplugin_oji.so libjavaplugin_oji.so
/usr/lib/mozilla/plugins/libjavaplugin_oji.so
#
cp /linux/contrib-norpm/*flashplayer* /usr/lib/mozilla/plugins/.


if [ ! -d /opt/bin ]; then
  mkdir /opt/bin
fi
mkdir -p /root/.kde/share/config
cp /linux/contrib-norpm/gifmerge /opt/bin/.
cp /linux/contrib-norpm/pdf2ps /opt/bin/.
cp /linux/contrib-norpm/psmerge /opt/bin/.
cp /linux/contrib-norpm/psA4toA3 /opt/bin/.
cp /linux/contrib-norpm/ps2gif /opt/bin/.
chown -R root.root /opt
# configuarazione kppp (modem)
cp -f /linux/config/kppprc  /root/.kde/share/config/.

if [ "No" = "No" ]; then
#
# NIS
#
cp -f /linux/config/yp.conf /etc/.
cp -f /linux/config/nsswitch.conf /etc/.
cp -f /linux/config/aautofs_link /etc/rc.d/init.d/.
if [ "" != "" ]; then
  echo "NISDOMAIN=itgoes" >> /etc/sysconfig/network
  echo +@_u:::::: >> /etc/passwd
#    if [ "" != "ccl" ]; then
#       echo +@ccl_u:::::: >> /etc/passwd
#    fi
  echo + >> /etc/group
  chkconfig --level 345 ypbind on
  chkconfig --level 345 aautofs_link on
  echo "/yp      yp:auto.users   --timeout 60" >> /etc/auto.master
  perl -pi -e 's|^/misc|####/misc|g' /etc/auto.master
#  echo /pctest_home @_h >> /etc/exports
  echo /home @_h >> /etc/exports
  if egrep -e '^USENIS=no' /etc/sysconfig/authconfig ;then
    perl -pi -e 's|^USENIS=no|USENIS=yes|g' /etc/sysconfig/authconfig
  else
    echo "USENIS=yes" >> /etc/sysconfig/authconfig
  fi
fi
fi

# for ssh:
a=\`grep '#ClientAliveInterval 0' sshd_config\` > /dev/null 2>&1
    if [ "$a" != "" ]; then
  perl -pi -e 's/#ClientAliveInterval 0/ClientAliveInterval 300/g'  /etc/ssh/sshd_config
else
  echo "ClientAliveInterval 300" >>  /etc/ssh/sshd_config
fi
```

```
# for AFS:
# autenticazione afs con kerberos 5
cp -f /linux/config/krb5.conf /etc/.
# configurazione afs:
echo "infn.it" > /usr/vice/etc/ThisCell
cp -f /linux/config/CellServDB /usr/vice/etc/CellServDB
# corregge un baco dello script di startup di openafs
if [ \`uname -m\` = "i586" ]; then
  /linux/scripts/afs586
fi
# corregge una protezione di tetex che non permette di usare dvips e xdvi
#chmod -R 1777 /var/lib/texmf
#chmod -R 1777 /usr/share/texmf
mkdir -p /var/lib/texmf/pk/cx/public
chmod 1777 /var/lib/texmf/pk/cx/public
mkdir -p /var/lib/texmf/pk/ljfour
chmod 1777 /var/lib/texmf/pk/ljfour
#
# evita che gli utenti leggano le password del NIS:
chmod 550 /usr/bin/ypcat
#
cp -f /linux/config/pine.conf.fixed /etc/
#
# Running some scripts
#
. /linux/scripts/security
#
# viene fatto un link su afs nazionale:
#ln -sf /afs/infn.it/asis/bo/linkdir/i386_redhat71/usr.local /usr/local2
#ln -sf /afs/infn.it/bo/system/locale/linux_62 /usr/locale
ln -sf /afs/infn.it/asis2/bo/i386_redhat73/cern /cern
# viene messo /usr/local/sbin dopo /sbin e /usr/sbin
perl -pi -e 's|PATH=/usr/local/sbin:\\\$PATH|PATH=\\\$PATH:/usr/local/sbin|'
/etc/profile
#
# Accounts.
#
if [ "" = "" ] && [ "" != "" ]; then

    if [ "No" = "No" ]; then
#  /usr/sbin/useradd -m -c "" -d '/pctest_home/' -s '/bin/tcsh' -p 'RMqXNvCDf.1Ao'
  /usr/sbin/useradd -m -c "" -d '/home/' -s '/bin/tcsh' -p 'RMqXNvCDf.1Ao'
    fi

    if [ "No" = "Si" ]; then
  /usr/sbin/useradd -m -c "" -d '/home/' -s '/bin/tcsh' -p 'RMqXNvCDf.1Ao'
    fi
fi
#
# Video
#
#Xconfigurator --kickstart --monitor Generic06 --vsync "50-90" --startxonboot
#
#
# Dual Boot
#
if [ "No" != "No" ]; then
cat <<GRUB>> /etc/grub.conf
title win
        rootnoverify (hd0,0)
        chainloader +1
GRUB
fi
#
rm -f /etc/rc.d/rc3.d/S99AAApostinstall /etc/rc.d/rc5.d/S99AAApostinstall
#rm -f /etc/rc.d/init.d/postinstall
/sbin/shutdown -r now
EOF
chmod +x /etc/rc.d/init.d/postinstall
ln -sf ../init.d/postinstall /etc/rc.d/rc3.d/S99AAApostinstall
ln -sf ../init.d/postinstall /etc/rc.d/rc5.d/S99AAApostinstall
#
# END
#
```