

**Centro Universitário UNIBENNETT**  
**Curso de Ciência da Computação**

**Monografia**  
*Trabalho de Conclusão de Curso*

**Anexos**

Rio de Janeiro  
2007.2

FELIPE MARTINS RÔLLA

ORIENTADOR: WILLIAM AUGUSTO R. DE SOUZA

DESENVOLVIMENTO, OTIMIZAÇÃO E  
IMPLEMENTAÇÃO DE SEGURANÇA EM  
SISTEMAS OPERACIONAIS LINUX PARA  
SERVIDORES DE E-MAIL CORPORATIVOS  
BASEADOS EM QMAIL

Monografia apresentada ao Centro  
Universitário Bennett do Instituto  
Metodista Bennett, como parte dos  
requisitos para obtenção do título de  
Bacharel em Ciência da Computação.

Centro Universitário Metodista Bennett

Rio de Janeiro 12/2007

## ÍNDICE DE ANEXOS

Anexo 1 - Patches do Sistema qmail (MCMILK.DE, 2007).....	8
Anexo 2 - Mensagens de Status (MCMILK.DE, 2007) .....	64
Anexo 3 - Arquivos de configuração para Logs .....	64
Anexo 4 - Scripts de Instalação .....	8
Anexo 5 - Particionamento Manual e Automático .....	64
Anexo 6 - Scripts de Hardening .....	64

# Anexo 1

- ESMTP STARTTLS (rfc2595)
  - via tls patch de Scott Gifford

<http://www.suspectclass.com/~sgifford/>
- ESMTP AUTH (rfc2554)
  - Com 6 metodos SASL (plain,login,cram-md5,cram-sha1,cram-ripemd,digest-md5)
  - Configurados por arquivos de controle no diretório control/auth/\*
- ESMTP SIZE command (rfc1870)
  - Configurado pelos arquivos control/databytes e control/databytes+
- ESMTP ENHANCEDSTATUSCODES (rfc3463, rfc2034, rfc1893)
- qmailqueue patch de Bruce Guenter <bguenter-djb-qmail@qcc.sk.ca>
- tarpitting
  - Configurado pelo arquivo control/tarpitcount
    - O valor da variável \$TARPITCOUNT subscreve o arquivo de controle
  - Configurado pelo arquivo control/tarpitdelay
    - O valor da variável \$TARPITDELAY subscreve o arquivo de controle
  - Se a variável \$NO\_TARPITTING é setada, então tarpitting é desabilitado
- ipme patch
  - ip 0.0.0.0 é considerado um endereço especial que sempre refere-se ao próprio host (rfc1122)
  - > <http://www.suspectclass.com/~sgifford/qmail/>
- 2 patches de Paul Jarc
  - realrcptto (Checa pela existência de contas reais)
  - qmail-branch (mais controle aos arquivos .qmail)
- outgoing ip patch
  - De Sergio Gelato e Andy Reptonis
- bmcheck() -> badmailfrom + badmailto + badhelo checks
  - logging variável dessas checagens
  - Pode ser utilizada uma variável de ambiente para cada bmcheck, para que seja setado ao tcpserver
  - Os arquivos de controle bad\* aceitam expressões regulares
- bigdns patch
  - Analisa respostas for a do tamanho comum
- big concurrency patch by Johannes Erdfelt
  - Aumenta o número de mensagens concorrentes suportadas
  - see <http://qmail.org/big-concurrency.patch>
- the big-todo patch
  - De Dave Smith, Russell Nelson e Bruce Guenter
- ccontrol/mfcheck
  - mail de dns check
  - if 1: Apenas dns será consultado
  - if 2: Verificação de SMTP callback/sender é feita

- control/goodmailfrom
  - Aceita emails do envelope MAIL FROM pré configurado
  - Pode ser usado o endereço de e-mail que não passar pelo mfcheck.
- Esta configuração sobscrive os valores do mfcheck
  - > e.g. root@some.stupidhost.local -> adminmails@host.de
- control/maxrcpt
  - Numero máximo de destinatários autorizados por uma sessão
  - Caso ultrapasse o cliente sofre as regras de tarpit
- control/maxhops
  - O valor agora pode ser mudado sem restart do serviço
- control/maxcmdlen
  - Tamanho máximo de um commando smtp
  - Se ultrapassar o valor máximo, clients sofrem as regras de tarpit
- control/maxaddrlen
  - Tamanho maximo de caracteres para definir um endereço de e-maildado ao RCPT TO ou MAIL FROM
  - Se ultrapassar o valor máximo, clients sofrem as regras de tarpit
- control/smtpgreeting can Pode ter múltiplas linhas
- control/rcptcheck
  - Checar veracidade de destinatários
- control/datechecks
  - checagem de data no formato YYYYMMDD sob o RCPT TO
- Se a variável de ambiente \$BLACKLISTED for setada, fornecemos dados oara atualizarmos o spamassassin.
  - "RCPT TO" é ignorado, o e-mail é enviado para \$BLACKLISTED
  - Foi utilizado o patch rblsmtpd
    - <http://www.mcmilk.de/qmail/dl/djb-ware/ucspi-tcp-0.88-rbl.diff.bz2>
- \$RCPTTOFIXED pode ser utilizada para entregar todo e-mail para um endereço especial
- HELO/EHLO requerem explicitamente um hostname, caso contrário o cliente recebe um erro.
  - "501 5.5.4 syntax error, I need your hostname"

## Anexo 2

### Enhanced Mail System Status Codes

=====

2.X.X	Success
4.X.X	Persistent Transient Failure
5.X.X	Permanent Failure
X.0.X	Other or Undefined Status
X.0.0	Other undefined Status
X.1.X	Addressing Status
X.1.0	Other address status
X.1.1	Bad destination mailbox address
X.1.2	Bad destination system address
X.1.3	Bad destination mailbox address syntax
X.1.4	Destination mailbox address ambiguous
X.1.5	Destination mailbox address valid
X.1.6	Mailbox has moved
X.1.7	Bad sender's mailbox address syntax
X.1.8	Bad sender's system address
X.2.X	Mailbox Status
X.2.0	Other or undefined mailbox status
X.2.1	Mailbox disabled, not accepting messages
X.2.2	Mailbox full
X.2.3	Message length exceeds administrative limit.
X.2.4	Mailing list expansion problem
X.3.X	Mail System Status
X.3.0	Other or undefined mail system status
X.3.1	Mail system full
X.3.2	System not accepting network messages
X.3.3	System not capable of selected features
X.3.4	Message too big for system
X.4.X	Network and Routing Status
X.4.0	Other or undefined network or routing status
X.4.1	No answer from host
X.4.2	Bad connection
X.4.3	Routing server failure
X.4.4	Unable to route
X.4.5	Network congestion
X.4.6	Routing loop detected
X.4.7	Delivery time expired
X.5.X	Mail Delivery Protocol Status
X.5.0	Other or undefined protocol status
X.5.1	Invalid command
X.5.2	Syntax error
X.5.3	Too many recipients
X.5.4	Invalid command arguments
X.5.5	Wrong protocol version
X.6.X	Message Content or Media Status
X.6.0	Other or undefined media error

X.6.1	Media not supported
X.6.2	Conversion required and prohibited
X.6.3	Conversion required but not supported
X.6.4	Conversion with loss performed
X.6.5	Conversion failed
X.7.X	Security or Policy Status
X.7.0	Other or undefined security status
X.7.1	Delivery not authorized, message refused
X.7.2	Mailing list expansion prohibited
X.7.3	Security conversion required but not possible
X.7.4	Security features not supported
X.7.5	Cryptographic failure
X.7.6	Cryptographic algorithm not supported
X.7.7	Message integrity failure

## Anexo 3

- /var/qmail/control/log/bmchecks  
-> Habilita/Desabilita logging de um padrão que combine nos arquivos de controle bad\*
- /var/qmail/control/log/datechecks  
-> Habilita/Desabilita logging de checagens para padrões de data definidos por regexp como : foo-bar-YYYYMMDD@domain.com
- /var/qmail/control/log/orchecks  
-> Habilita/Desabilita logging de testes open relay
- /var/qmail/control/log/tarpitting  
-> Habilita/Desabilita the logging algumas informações sobre os clients que sofrem tarpit
- /var/qmail/control/log/pop3\_in  
- 1 = Liga / 0 = Desliga  
- Faz logging de todos os comandos POP3 vindos de clients
- /var/qmail/control/log/pop3\_out  
- 1 = Liga / 0 = Desliga  
- Faz logging de todas as respostas de saída do servidor do daemon qmail-pop3d + qmail-popup
- /var/qmail/control/log/pop3\_fd  
- logging do descritor de arquivo(filedescriptor)  
- Usado para o logging dos daemons qmail-popup e qmail-pop3d (in/out)
- /var/qmail/control/log/smtp\_in  
- 1 = Liga / 0 = Desliga  
- Faz logging de todos os comandos de clientes
- /var/qmail/control/log/smtp\_out  
- 1 = Liga / 0 = Desliga  
- Faz logging de todas as repostas de saída do daemon qmail-smtpd
- /var/qmail/control/log/smtp\_fd

- logging do descritor de arquivo (filedescriptor)
- Usado para o logging do daemon qmail-smtpd (in/out)
- /var/qmail/control/log/remote\_fd
  - logging do descritor de arquivo (filedescriptor) / 0 significa Desligado
  - Sempre loga a sessão completa

## Anexo 4

```
#!/bin/sh
#
# Copyright 2007 Felipe Martins, Rio de Janeiro, Rio de Janeiro, Brazil
# Copyright 2001, 2003, 2004 Slackware Linux, Inc., Concord, CA
# All rights reserved.
#
# Modified by Felipe Martins, Rio de Janeiro, Brazil, for Qubit Linux.
#
# Redistribution and use of this script, with or without modification, is
# permitted provided that the following conditions are met:
#
# 1. Redistributions of this script must retain the above copyright
# notice, this list of conditions and the following disclaimer.
# THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY
EXPRESS OR IMPLIED
# WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF
# MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO
# EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
# SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO,
# PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS;
# OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY,
# WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR
# OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF
# ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
#
# As always, bug reports, suggestions, etc: volkerdi@slackware.com
#
TMP=/var/log/setup/tmp
if [ ! -d $TMP ]; then
  mkdir -p $TMP
fi
```

```

rm -f $TMP/SeT*

echo "$SLACK_KERNEL" > $TMP/SeTkernel

export T_PX="/mnt"
echo "$T_PX" > $TMP/SeTT_PX

echo "on" > $TMP/SeTcolor # turn on color menus
PATH="$PATH:/usr/lib/setup"
export PATH;
export COLOR=on

if mount | fgrep /var/log/mount 1> /dev/null 2> /dev/null ; then # clear source
    umount /var/log/mount # location
fi

# Anything mounted on /var/log/mount now is a fatal error:
if mount | fgrep /var/log/mount 1> /dev/null 2> /dev/null ; then
    echo "Can't umount /var/log/mount. Reboot machine and run setup again."
    exit
fi

# If the mount table is corrupt, the above might not do it, so we will
# try to detect Linux and FAT32 partitions that have slipped by:
if [ -d /var/log/mount/lost+found -o -d /var/log/mount/recycled \
    -o -r /var/log/mount/io.sys ]; then
    echo "Mount table corrupt. Reboot machine and run setup again."
    exit
fi

rm -f /var/log/mount 2> /dev/null
rmdir /var/log/mount 2> /dev/null
mkdir /var/log/mount 2> /dev/null

while [ 0 ]; do

    dialog --title "Qubit Linux Setup" \
    --menu \
    "Welcome to Qubit Linux Setup developed by Felipe Martins.\n\
    Select an option below using the UP/DOWN keys and SPACE or ENTER.\n\
    Alternate keys may also be used: '+', '-', and TAB." 20 72 12 \
    "KEYMAP" "Select a keyboard map" \
    "PARTITION" "Partition your hard drive if needed" \
    "ADDSWAP" "Set up your swap partition(s)" \
    "TARGET" "Set up your target partitions" \
    "SOURCE" "Select source media" \
    "INSTALL" "Install Linux O.S. packages" \
    "CONFIGURE" "Reconfigure your Linux system" \
    "INSTALLQUBIT" "Install Qubit Qmail packages" \
    "CONFIGUREQUBIT" "Reconfigure your Qubit Qmail System" \
    "HELP" "Help File" \
    "EXIT" "Exit Setup" 2> $TMP/hdset

```

```

if [ ! $? = 0 ]; then
    rm -f $TMP/hdset $TMP/SeT*
    exit
fi
MAINSELECT=""`cat $TMP/hdset`"
rm $TMP/hdset

# Start checking what to do. Some modules may reset MAINSELECT to run the
# next item in line.

if [ "$MAINSELECT" = "KEYMAP" ]; then
    SeTkeymap
    MAINSELECT=""
fi

if [ "$MAINSELECT" = "PARTITION" ]; then

    MAINSELECT=$(dialog --stdout --title "Partition Setup" \
        --menu \
        "Please choose the desired partition method.\n\
        Alternate keys may also be used: '+', '-', and TAB.\n" 11 70 3 \
        "AUTOMATIC" "Automatic Partitioning" \
        "MANUAL" "Manual Partitioning")

    if [ "$MAINSELECT" = "MANUAL" ]; then
        SeTdisk
        MAINSELECT="ADDSWAP"
    fi
    if [ "$MAINSELECT" = "AUTOMATIC" ]; then
        SeTdiskauto
        MAINSELECT="ADDSWAP"
    fi
fi

if [ "$MAINSELECT" = "ADDSWAP" ]; then
    SeTswap 2>/dev/null
    if [ -r $TMP/SeTswap ]; then
        MAINSELECT="TARGET"
    elif [ -r $TMP/SeTswapskip ]; then
        # Go ahead to TARGET without swap space:
        MAINSELECT="TARGET"
    fi
fi

if [ "$MAINSELECT" = "TARGET" ]; then
    if probe -l | fgrep "Linux\$" 1> /dev/null 2> /dev/null ; then
        probe -l | fgrep "Linux\$" | sort 1> $TMP/SeTplist 2> /dev/null
        SeTpartitions
        SeTDOS
        if [ -r $TMP/SeTnative ]; then

```

```

    MAINSELECT="SOURCE"
fi
else
    dialog --title "NO LINUX PARTITIONS DETECTED" \
--msgbox "There don't seem to be any Linux partitions on this machine \
You'll need to make at least one of these to install Linux." 10 60

    MAINSELECT=""
fi
fi

if [ "$MAINSELECT" = "SOURCE" ]; then
    SeTmedia
    if [ -r $TMP/SeTsource ]; then
        MAINSELECT="INSTALL"
    fi
fi

if [ "$MAINSELECT" = "INSTALL" ]; then
    if [ ! -r $TMP/SeTsource -o ! -r $TMP/SeTnative ]; then
        dialog --title "CANNOT INSTALL SOFTWARE YET" --msgbox "\
\n\
Before you can install software, you must select your source media \
and set up your target Linux partition. You may also optionally remap \
your keyboard and set up your swap partition(s). \n\
\n\
Press ENTER to return to the main menu." 16 68
        continue
    fi

    # unpack and install packages to the root install
    SeTpackages

    # copy current kernel to the root install
    SeTkernel

    MAINSELECT="CONFIGURE"
fi

if [ "$MAINSELECT" = "CONFIGURE" ]; then

    if [ -r $TMP/SeTnative ]; then
        cat /dev/null > $T_PX/etc/fstab
        if [ -r $TMP/SeTswap ]; then
            cat $TMP/SeTswap > $T_PX/etc/fstab
        fi
        cat $TMP/SeTnative >> $T_PX/etc/fstab
        if [ -r $TMP/SeTDOS ]; then
            cat $TMP/SeTDOS >> $T_PX/etc/fstab
        fi
    fi

```

```

# Scanning for CD/DVD/CDRW devices

cd_num=0
dvd_num=0
for procdevice in /proc/ide/hd* ; do
    device="$(basename $procdevice)"
    media="$(cat $procdevice/media)"
    model="$(cat $procdevice/model)"
    if [ "$( echo $media | grep -i "cdrom" )" ] ; then
        if [ "$( echo $model | grep -i "dvd" )" ] ; then
            type="dvd"
            if [ "$dvd_num" = "0" ] ; then
                num=""
            else
                num="$dvd_num"
            fi
            dvd_num=$(( $dvd_num + 1 ))
        else
            type="cdrom"
            if [ "$cd_num" = "0" ] ; then
                num=""
            else
                num="$cd_num"
            fi
            cd_num=$(( $cd_num + 1 ))
        fi
        mkdir -p $T_PX/mnt/$type$num
        printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/$device" "/mnt/$type$num"
        "iso9660" "noauto,user,ro" "0" "0" >> $T_PX/etc/fstab
    fi
done

total_num=$(( $cd_num + $dvd_num ))

if [ "$total_num" == "0" ] ; then
    printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/cdrom" "/mnt/cdrom"
    "iso9660" "noauto,user,ro" "0" "0" >> $T_PX/etc/fstab
fi

    printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/fd0" "/mnt/floppy" "auto"
    "noauto,user" "0" "0" >> $T_PX/etc/fstab
    printf "%-16s %-16s %-11s %-16s %-3s %s\n" "devpts" "/dev/pts" "devpts"
    "gid=5,mode=620" "0" "0" >> $T_PX/etc/fstab
    printf "%-16s %-16s %-11s %-16s %-3s %s\n" "proc" "/proc" "proc" "defaults" "0"
    "0" >> $T_PX/etc/fstab
    # printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/tmpfs" "/dev/shm" "tmpfs"
    "size=10%,mode=0777" "0" "0" >> $T_PX/etc/fstab
    # printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/usbmedia" "/mnt/usb" "auto"
    "noauto,user,rw,exec" "0" "0" >> $T_PX/etc/fstab

```

```

    # printf "%-16s %-16s %-11s %-16s %-3s %s\n" "/dev/usbmedia1" "/mnt/usb1"
"auto" "noauto,user,rw,exec" "0" "0" >> $T_PX/etc/fstab
fi

# Install lilo
ROOT_DEVICE=`cat $TMP/SeTrootdev`
chroot $T_PX /sbin/liloconfig / $ROOT_DEVICE /boot/vmlinuz

# Some more settings and tunning
SeTconfig

# Finished
dialog --title "SYSTEM SETUP COMPLETE" --msgbox "You may now EXIT setup
and then reboot your machine or continue with qmail installation." 7 55

fi

# Beggining of the qmail profiles installation
if [ "$MAINSELECT" = "INSTALLQUBIT" ]; then

MAINSELECT=$(
dialog --stdout --title "Qmail Installation" \
--menu \
"Please choose the desired Qubit Qmail installation profile.\n\
Alternate keys may also be used: '+', '-', and TAB.\n" 13 70 5 \
"FULL1" "Full Install and Software Integration" \
"FULL2" "Full Install and Software Integration (see HELP)" \
"MX-SERVER" "Secondary Mail Exchanger Server" \
"CUSTOM" "Administrators Custom Install" \
"HELP" "Explanation about each profile"
)

if [ "$MAINSELECT" = "FULL1" ]; then
    SeTqmailfull1
fi
if [ "$MAINSELECT" = "FULL2" ]; then
    SeTqmailfull2
fi
if [ "$MAINSELECT" = "MX-SERVER" ]; then
    SeTqmailmx
fi
if [ "$MAINSELECT" = "CUSTOM" ]; then
    SeTqmailcustom
fi
if [ "$MAINSELECT" = "HELP" ]; then
    SeTqmailhelp
    MAINSELECT="INSTALLQUBIT"
fi

fi

fi

```

```

if [ "$MAINSELECT" = "EXIT" ]; then
    break
fi

done # end of main loop

# Enable the postinstall rc script
chmod 755 $T_PX/etc/rc.d/rc.postinstall

sync
chmod 755 $T_PX
if [ -d $T_PX/tmp ]; then
    chmod 1777 $T_PX/tmp
fi
if mount | fgrep /var/log/mount 1> /dev/null 2> /dev/null ; then
    umount /var/log/mount
fi
# Anything mounted on /var/log/mount now is a fatal error:
if mount | fgrep /var/log/mount 1> /dev/null 2> /dev/null ; then
    exit
fi
# If the mount table is corrupt, the above might not do it, so we will
# try to detect Linux and FAT32 partitions that have slipped by:
if [ -d /var/log/mount/lost+found -o -d /var/log/mount/recycled \
    -o -r /var/log/mount/io.sys ]; then
    exit
fi
rm -f /var/log/mount 2> /dev/null
rmdir /var/log/mount 2> /dev/null
mkdir /var/log/mount 2> /dev/null
chmod 755 /var/log/mount

if [ -f /mnt/etc/fstab ]; then
    # umount CD:
    if [ -r $TMP/SeTCDdev ]; then
        if mount | grep iso9660 > /dev/null 2> /dev/null ; then
            umount `mount | grep iso9660 | cut -f 1 -d ' '`
        fi
        eject `cat $TMP/SeTCDdev`
        echo "Please remove the installation disc and press ctrl-alt-delete to reboot."
    else
        echo "You may now press ctrl-alt-delete to reboot."
    fi
    echo
fi

# final cleanup
rm -f $TMP/tagfile $TMP/SeT* $TMP/tar-error $TMP/PKGTOOL_REMOVED

```

```
rmdir /mnt/tmp/orbit-root 2> /dev/null
# end setup script
```

## Anexo 5

```
#!/bin/sh
```

```
# Copyright Felipe Martins <martins.felipe@gmail.com>. This program is free
software;
# you can redistribute it and/or modify it under the terms of the GNU General Public
License
# as published by the Free Software Foundation; either version 2 of the License,
# or (at your option) any later version. Please take a look at
http://www.gnu.org/copyleft/gpl.htm
```

```
while [ "1" = "1" ] ; do
```

```
    dglst=""
    n=0
    for dev in "$( cat /proc/partitions \
| grep -v '^$' \
| grep -v 'name' \
| grep -v 'loop' \
| sed -e 's/^[ \t]*[0-9]*[ \t]*[0-9]*[ \t]*[0-9]*[ \t]*\([a-z]*\) [0-9]*[^\0-9]*$ \1 disk
\""/" | sort -u )" ; do
```

```
        dglst="$dglst $dev"
        n=$((n+1))
    done
```

```
    disk=$(dialog \
--stdout \
--ok-label "Edit" \
--cancel-label "End" \
--title "PARTITIONS EDITOR" \
--radiolist "Edit partition tables (press SPACE to select a disk) :" \
$((n+9)) 75 $((n+2)) ${dglst} )
```

```
    if [ ! "$disk" ]; then
        exit 0
    fi
    clear
    cfdisk /dev/$disk 2>/dev/null
```

```
done
```

## Anexo 6

```
#!/bin/bash
#
# Escape : System and Service Hardening
# Author : Felipe Martins (GPL for Qubit Linux)

#####
### SECTION: SYSTEM HARDENING ###
#####

# Securing /etc/fstab, /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow
chown root.root /etc/fstab
chown root.root /etc/passwd /etc/shadow /etc/group /etc/gshadow
chmod 640 /etc/passwd /etc/group
chmod 400 /etc/shadow

# Allowing only root user to use crontab
rm -f cron.deny at.deny
echo root > /etc/cron.allow
echo root > /etc/at.allow
chown root:root /etc/cron.allow /etc/at.allow
chmod 400 /etc/cron.allow /etc/at.allow

# Disallow Ctrl+Alt+Del to all users
sed -i "s/^ca::crtlaltdel:/#ca::crtlaltdel:/g"
init q

# Turn Off SUID bit of important files (MELHORAR ESTE SCRIPT)
chmod a-s /bin/ping /bin/mount /bin/ping6 /bin/umount /usr/bin/at
chmod a-s /usr/bin/cu /usr/bin/rcp /usr/bin/rsh /usr/bin/uux
chmod a-s /usr/bin/chfn /usr/bin/chsh /usr/bin/sudo /usr/bin/uucp
chmod a-s /usr/bin/wall /usr/bin/lppasswd /usr/bin/crontab
chmod a-s /usr/bin/crontab /usr/bin/chage /usr/bin/write
chmod a-s /usr/bin/traceroute6 /usr/bin/traceroute
chmod a-s /usr/bin/fdmount /usr/bin/slocate /usr/bin/expiry
chmod a-s /usr/bin/newgrp /usr/bin/passwd /usr/bin/gpasswd
chmod a-s /usr/bin/rlogin /usr/bin/uuname /usr/bin/uustat
chmod a-s /usr/bin/lockfile /usr/bin/slrnpull /usr/bin/procmail
chmod a-s /usr/lib/utempter/utempter /usr/sbin/uuxqt
chmod a-s /usr/sbin/uucico /usr/libexec/pt_chown

# Configuring Warning Banners
# /etc/issue
```

```
echo
#####
#####";
echo "#                WARNING                #";
echo
#####
#####";
echo "#                #";
echo "# This is a Private computer system and is the property of this Company.
#";
echo "# It is for authorized use only. Users (authorized or unauthorized) have no
#";
echo "# explicit or implicit expectation of privacy.                #";
echo "#                #";
echo "# Any or all uses of this system and all files on this system may be                #";
echo "# intercepted, monitored, recorded, copied, audited, inspected, and disclosed to
#";
echo "# authorized site, Department of Energy, and law enforcement personnel,
#";
echo "# as well as authorized officials of other agencies, both domestic and foreign.
#";
echo "# By using this system, the user consents to such interception, monitoring,
#";
echo "# recording, copying, auditing, inspection, and disclosure at the discretion of
#";
echo "# authorized site or Department of Energy personnel.                #";
echo "#                #";
echo "# Unauthorized or improper use of this system may result in administrative
#";
echo "# this system you indicate your awareness of and consent to these terms and
#";
echo "# conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions #";
echo "# stated in this warning.                #";
echo "#                #";
echo
#####
#####";
```

```
# /etc/issue.net
```

```
echo "#####"
echo "# MESSAGE #
echo "#####"
```

```
# /etc/motd
```

```
echo "#####"
echo "# MESSAGE #
echo "#####"
```

```
#####  
### SECTION: SERVICES HARDENING ###  
#####
```

```
# Securing SSH Server (/etc/ssh/sshd_config)
```

```
SSHCONFIG="/etc/ssh/sshd_config"
```

```
if [ -f $SSHCONFIG ];
```

```
then
```

```
  rm $SSHCONFIG;  
  echo '# SSH Config';  
  echo '# Hardened by Qubit Linux';  
  echo '';  
  echo 'Protocol 2';  
  echo 'Port 22';  
  echo 'PermitRootLogin no';  
  echo 'PermitEmptyPasswords no';  
  echo 'UsePrivilegeSeparation yes';  
  echo 'Banner /etc/issue';  
  echo 'ClientAliveInterval 1200';  
  echo 'ClientAliveCountMax 0';  
  echo 'IgnoreRhosts yes';  
  echo 'RhostsAuthentication no';  
  echo 'RhostsRSAAuthentication no';  
  echo 'HostbasedAuthentication no';  
  echo 'AllowTcpForwarding no';  
  echo 'X11Forwarding no';  
  echo 'StrictModes yes';  
  echo 'SyslogFacility AUTH';  
  echo 'AllowUsers admin';  
  echo 'MaxStartups 10';  
  echo 'MaxAuthTries 5';  
  echo '#EOF';
```

```
#Ciphers blowfish-cbc,aes256-cbc,aes256-ctr
```

```
#IgnoreRhosts yes
```

```
#IgnoreUserKnownHosts yes
```

```
#RSAAuthentication yes
```

```
fi;
```

```
#####  
## Hardening Network files in /proc  
#####
```

```
PROC=/proc/sys/net/ipv4
```

```
# Enable TCP SYN Cookie Protection
```

```
echo "1" > $PROC/tcp_syncookies
```

```
# Enable TCP Spoofing Protection  
echo "1" > $PROC/rp_filter
```

```
# Enable Ignoring Broadcasts Request  
echo "1" > $PROC/icmp_echo_ignore_broadcasts
```

```
# Enable Bad Error Message Protection  
echo "1" > $PROC/icmp_ignore_bogus_error_responses
```

```
# Enable Logging of Spoofed Packets, Source Routed Packets, Redirect Packets  
echo "1" > $PATH/conf_all.log_martians
```