

**PREMISSAS TÉCNICAS BÁSICAS DE SEGURANÇA APLICADAS AO LINUX**  
**Tiago Gomes Pereira**

Material desenvolvido baseado em traduções de materiais específicos e de normas práticas de segurança voltadas ao GNU/Linux

algodas@gmail.com  
[http:// www.tiagogomes.eti.br](http://www.tiagogomes.eti.br)  
OUT/2008

## SUMÁRIO

Visão geral .....	3
1. Informações básicas .....	4
2. Segurança BIOS .....	4
3. Senha .....	4
4. O arquivo <code>/etc/exports</code> .....	5
5. Desativação ao acesso de determinados programas através do console .....	6
6. Desabilitar acesso a todos os consoles .....	6
7. O arquivo <code>/etc/inetd.conf</code> .....	7
8. TCP_WRAPPERS .....	9
9. O arquivo <code>/etc/aliases</code> .....	10
10. Bloqueio a requisições de Ping .....	11
11. Bloqueie informações repassadas pelo telnet .....	11
12. O arquivo <code>/etc/host.conf</code> .....	12
13. O arquivo <code>/etc/securetty</code> .....	12
14. Contas especiais .....	12
15. Bloqueando o <code>su</code> para qualquer usuário .....	14
16. Definir limite de recursos .....	15
17. Mais controle na montagem de sistemas de arquivos .....	15
18. Previna-se ao rodar o comando <code>rm -rf *</code> em diretórios .....	15
19. Shell logging .....	16
20. O <code>/etc/lilo.conf</code> .....	16
21. Desabilitar o desligamento do sistema através do <code>Ctrl+Alt+Delete</code> .....	17
22. Corrija as permissões para os scripts em <code>/etc/rc.d/init.d</code> .....	17
23. O arquivo <code>/etc/rc.d/rc.local</code> .....	17
24. Bit SUID e SGID .....	18
25. Permissão World-wiretable .....	21
26. Arquivos sem dono .....	21
27. Arquivo <code>.rhosts</code> .....	21
28. Considerações finais .....	22

## Visão geral

O conceito de Segurança da informação é muito mais complexo que atributos técnicos abordados neste artigo. Tratar de segurança da Informação é tratar a Tecnologia da informação como processos de negócios aplicados a sustentabilidade de uma corporação. Por isso este artigo aborda algumas recomendações básicas para aplicações técnicas a servidores. Não fique limitado a estes comandos ou configurações, leia as Normas ISO/IEC 27001 e a BS17799 , onde são abordados aspectos de gestão e normas práticas aplicadas aos processos de negócio.

## Linux Security

Um sistema UNIX é seguro de acordo a maneira como o administrador o faz. A medida que se introduz mais serviços, mais falhas o sistema tende a apresentar. Sistemas operacionais como o SCO devem realmente ser mais propícios a falhas de segurança devido ao excessivo número de serviços, sendo em sua maioria não utilizados pelo usuário (afim de tornar-se mais "amigável") . O Linux em si é muito estável e seguro mas distribuídos sobre vários "sabores de versões". Em uma das comparações entre o RedHat e o Slackware por exemplo, pessoas têm argumentado sobre qual das distros é mais seguro, uma dúvida peculiar, visto que ao instalar o Linux, deve-se customizar com o mínimo de pacotes e serviços possível, adicionando apenas o que for necessário para as necessidades dos usuários em questão ou natureza de sua utilização, isso sim torna uma distribuição mais eficaz e segura.

Partindo deste princípio nota-se que a consistência da avaliação de segurança parte da implementação da distro pelo administrador do que fornecida pela Distribuição em questão. O Linux é o mais seguro se devidamente implementado, caso uma vulnerabilidade seja descoberta no sistema, há milhares de voluntários prontos a corrigir de forma imediata se possível antes de ser explorada. Em grandes corporações os produtos comerciais abordados tem número limitado de integrantes na equipe responsável pelo setor de ajustes e correções, além de que , algumas divulgações a respeito de algumas vulnerabilidades podem ir de encontro a interesses da empresa retentora dos direitos sobre o software assim como inferir sobre processos de negócios da empresa que o produz e sobre seus clientes.

Alguns problemas possuem Patches para correção mas a displicência de alguns administradores que acabam usando apenas as ferramentas que acompanham o sistema operacional de forma nativa, assim como demais pacotes, aproveitando a comodidade e a “user friendly” ocasionado por estes pacotes pré-configurados.

Os erros podem ocorrer em qualquer nível da programação, mas quando você tem milhares pessoas com o código fonte disponível para eles, esses erros são muitas vezes descobertos de forma mais rápida em um ambiente de código fonte aberto. Claro, com de milhares de pessoas com permissão para desenvolvimento em cerca de 7 milhões de cópias do Linux a fora tem uma probabilidade maior de um desenvolvimento com erros e com abrangência ainda maior na proliferação deste código. Versões estáveis homologadas pelos responsáveis pelo pacote devem ter preferências assim como o patches disponibilizados pelo mesmo.

## **1. Informações básicas**

Não disponibilize ou disponibilize o mínimo de informações a entidades externas sobre seu sistema, seja entidades computacionais ou pessoas (o que é ainda pior). Um simples toque disparado contra um sistema-vítima pode revelar muito sobre seu sistema, além de uma vasta pesquisa utilizando técnicas como Engenharia social afim de descobrir informações muitas vezes vitais ao sistema em questão ou informações sobre para autenticação. Um simples e poderoso finger daemon e / ou tcpd pode se conectar a seu sistema e colher informações importantes sobre seu sistema. Os logs são a única maneira de saber o que está acontecendo no seu sistema Linux, naturalmente isto pressupõe que um atacante não tenha forjado ou corrompido estes arquivos de log. A própria exploração de brechas pode revelar informações sobre o atacante de acordo a suas tentativas de explorar as vulnerabilidades. Tentar compreender logs é um passo importante a acompanhar as rotinas de monitoramento de sistemas GNU/Linux.

Limitar o número de programas possuem o bit SUID setado é fator de extrema importância para sistemas computacionais que rodam Linux. Bit SUID é o bit que altera a permissão do usuário que executa determinado programa que possui o bit setado, adquirindo permissão de dono do arquivo/programa na execução. Setar esse bit torna-se necessário em algumas vezes mas em outras não. Exploits podem

explorar brechas em programas que possuem este bit setado e “ownar” o sistema corrente.

## 2. Segurança BIOS

Definir uma senha para boot previne contra utilização não autorizada do sistema por pessoas que tem acesso as áreas destinadas aos servidores. Faz-se necessário também bloquear a inicialização através de disquetes ou demais mídias. Verifique o seu manual da BIOS analise estes fatores antes de carregá-lo na próxima vez.

## 3. Senha

O ponto de partida da nossa tour em segurança Linux é a senha. Muitas pessoas mantêm a sua vida inteira um computador em que a única coisa que impede demais pessoas de conectarem a ele é uma palavra de em média 8 caracteres, a SENHA. Não se trata de algo com extrema confiabilidade, visto que não existência de senhas “unhackeable”. Dado o tempo apropriado e recursos computacionais adequados, todas as senhas podem ser adivinhados através de força bruta ou ater mesmo a aplicação de técnicas de natureza pessoal e social como a Engenharia Social. Definir rotinas semanais para trocas de senha e utilizar de recursos que não validem senhas fracas pode ser um bom início para estabelecer processos de autenticação mais seguros.

## 4. O arquivo `/etc/exports`

Se você está exportando arquivos usando NFS, certifique-se de configurar `/etc/exports` com o máximo de restrições de acesso possíveis. Isto significa não permitir o acesso do root para escrita além de montar somente para leitura, sempre que possível.

Um exemplo de um arquivo de configuração do NFS com algumas premissas de segurança:

`(vi / etc / exports)` :

```
/foo/bar/export host1.mydomain.com (ro, root_squash)
```

```
/foo/bar/export host2.mydomain.com (ro, root_squash)
```

Onde:

*/foo/bar/export* : é o diretório que você deseja exportar,

*host.mydomain.com* : É o host autorizado a logar neste diretório,

*ro* : Apenas leitura para montagem

*root\_squash* : Não dá permissão de escrita para root no diretório

Para que tenha efeito as modificações é necessário executar o seguinte comando:

```
/usr/sbin/exportfs-a
```

## 5. Desativação ao acesso de determinados programas através do console

Uma maneira simples e comum de personalização é desativar completamente o acesso através do console equivalente a determinados programas como shutdown e halt . Para fazer isso, execute:

```
[root @ profundo] # rm-f /etc/security /console.apps/servicename
```

Onde:

*servicename* : é o nome do programa ao qual deseja desativar para o console equivalente. Caso você utilize o xdm, ter cuidado para não remover o arquivo xserver , neste caso apenas o root será capaz de iniciar o servidor X. (Se você sempre usa o xdm para iniciar o servidor X, o root é o único usuário que o inicia, neste caso, talvez você seja realmente necessário remover o arquivo xserver).

Por exemplo:

```
[root @ profundo] # rm-f /etc/security/console.apps/halt
```

```
[root @ profundo] # rm-f /etc/security/console.apps/poweroff
```

```
[root @ profundo] # rm-f /etc/security/console.apps/reboot
```

```
[root @ profundo] # rm -f /etc/security/console.apps /shutdown
```

```
[root @ profundo] # rm -f /etc/security/console.apps /xserver
```

(se for removido, o root será o único usuário capaz de iniciar X).

## 6. Desabilitar acesso a todos os consoles

A fim de desativar todos os consoles de acesso, incluindo programas e arquivos de acesso, no /etc/pam.d/diretório, comente todas as linhas que remetem para pam\_console.so . Abaixo um script que automatiza isto a você:

```
[root @ profundo] # vi disabling.sh
```

E adicione:

```
#!/bin/bash
```

```
cd / etc / pam.d
```

```
for i in *; do
```

```
    sed '/[^\#].* pam_console.so / s /^\#/' <$ i> foo && mv foo $ i
```

```
done
```

Dê as permissões de execução e logo após o execute:

```
[root @ profundo] # chmod 700 disabling.sh
```

```
[root @ profundo] # ./ disabling.sh
```

## 7. O arquivo /etc/inetd.conf

O Inetd, também chamado de "super servidor", só irá carregar o serviço em questão quando solicitado . O arquivo inetd.conf informa ao inetd quais portas irão ficar escutando quando um serviço for solicitado. É necessário averiguar quais serviços de fato serão imprescindíveis. Os Serviços que não serão necessários devem ser desinstalados e não apenas desativados, menos serviços menos vulnerabilidades expostas.

Observe o /etc/inetd.conf e observe quais serviços estão sendo oferecidos pelo inetd, desative qualquer serviço não utilizado comentando a linha referente

(# no início da linha) e então enviar um sinal ao processo um SIGHUP, além de garantir que as permissões sobre este arquivo estão definidos para 600 .

```
[root @ profundo]# chmod 600 /etc/inetd.conf
```

Assegurar que o dono é root

```
[root @ profundo]# stat /etc/inetd.conf
```

```
File: "/etc/inetd.conf"
Size: 2869    Filetype: Regular File
Mode: (0600/-rw-----)  Uid: ( 0/ root) Gid: ( 0/ root)
Device: 8,6 Inode: 18219 Links: 1
Access: Wed Sep 22 16:24:16 1999(00000.00:10:44)
Modify: Mon Sep 20 10:22:44 1999(00002.06:12:16)
Change: Mon Sep 20 10:22:44 1999(00002.06:12:16)
```

Edite o arquivo inetd.conf (vi /etc/inetd.conf) e desabilite serviços como: ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth, etc.

```
#
#These are standard services.
#
#ftp      stream  tcp    nowait  root    /usr/sbin/tcpd  in.ftpd -l -a
#telnet   stream  tcp    nowait  root    /usr/sbin/tcpd  in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell    stream  tcp    nowait  root    /usr/sbin/tcpd  in.rshd
#login    stream  tcp    nowait  root    /usr/sbin/tcpd  in.rlogind
#exec     stream  tcp    nowait  root    /usr/sbin/tcpd  in.rexecd
#comsat   dgram   udp    wait    root    /usr/sbin/tcpd  in.comsat
#talk     dgram   udp    wait    root    /usr/sbin/tcpd  in.talkd
#ntalk    dgram   udp    wait    root    /usr/sbin/tcpd  in.ntalkd
#dtalk    stream  tcp    wait    nobody   /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2    stream  tcp    nowait  root    /usr/sbin/tcpd  lpop2d
#pop-3    stream  tcp    nowait  root    /usr/sbin/tcpd  lpop3d
#imap     stream  tcp    nowait  root    /usr/sbin/tcpd  imapd
#
#The Internet UUCP service.
#
#uucp     stream  tcp    nowait  uucp    /usr/sbin/tcpd /usr/lib/uucp/uucico -l
#
#Tftp service is provided primarily for booting. Most sites
#run this only on machines acting as "boot servers." Do not uncomment
#this unless you "need" it.
#
#tftp     dgram   udp    wait    root    /usr/sbin/tcpd  in.tftpd
#bootps   dgram   udp    wait    root    /usr/sbin/tcpd  bootpd
#
#Finger, systat and netstat give out user information which may be
#valuable to potential "system crackers." Many sites choose to disable
#some or all of these services to improve security.
```

Não esqueça de mandar um *SIGHUP* para o processo do *inetd* (`killall -HUP inetd`) após qualquer alteração realizada.

```
[root@profundo /root]# killall -HUP inetd
```

Mais uma medida de segurança pode ser tomada em relação ao *inetd*, definindo seu arquivo de configuração como imutável utilizando o *chattr*, da seguinte forma:

```
[root@profundo]# chattr +i /etc/inetd.conf
```

- E isto irá prevenir quaisquer alterações (acidental ou não) no *inetd.conf*. Um arquivo com este atributo não pode ser modificado: não pode ser apagado ou renomeado, nenhum link pode ser criado para ele, e dados não poderão ser escritos neste arquivo. Somente o root pode definir ou retirar este atributo. Se você deseja modificar o arquivo *inetd.conf* você precisará retirar o atributo com o seguinte comando:

```
[root@profundo]# chattr -i /etc/inetd.conf
```

## 8.TCP\_WRAPPERS

Por padrão, o Red Hat Linux, por exemplo, permite que todas requisições de serviços sejam respondidas de acordo a disponibilidade do mesmo. O TCP\_WRAPPERS torna a segurança dos servidores mais pertinente contra intrusão exterior além de ser muito simples sua configuração. Uma boa medida seria NEGAR (Deny) todos os hosts, adicionando "*ALL: ALL @ ALL, PARANOID*" no arquivo */etc/hosts.deny* e inserir uma lista de hosts confiáveis que estão autorizadas a acessar os serviços definidos através do arquivo */etc/hosts.allow*.

O TCP\_WRAPPERS é controlado a partir destes dois arquivos. A procura encerra-se no primeiro caso o host que solicite o serviços não se enquadre nas premissas de acesso já definidas.

*/etc/hosts.allow*

*/etc/hosts.deny*

- O acesso será concedido quando um (daemon ou cliente) coincide com uma entrada no arquivo `/etc/hosts.allow` .
- Caso contrário, o acesso será negado quando um (daemon ou cliente) coincide com uma entrada no arquivo `/etc/hosts.deny`.
- Caso contrário o acesso será garantido .

Edite o arquivo `hosts.deny` (`vi /etc/hosts.deny`) e adicione a seguinte linha:

```
# Negando acesso a todos
```

```
# Acesso negado por Padrão
```

```
ALL:ALL@ALL, PARANOID # Corresponde qualquer máquina cujo nome não coincide com o seu endereço, veja abaixo.
```

- Que significa que todos os serviços, de qualquer local , de modo que o serviço não seja explicitamente permitido no outro `host.allow`, por padrão será bloqueado.

Com o parâmetro `PARANOID` torna-se necessário caso você deseja executar o telnet ou ftp no servidor em questão não esqueça de adicionar a máquina cliente junto ao seu IP e Host no arquivo `/etc/hosts` ou você terá de esperar o delay de publicação e atualização do DNS antes do login.

Edite o `hosts.allow` (`vi / etc / hosts.allow`) e adicione a seguinte linha:

```
sshd: 192.168.1.10/255.255.255.0 gate.linuss.com
```

Onde a máquina cliente: 192.168.1.10 (Ip) e o nome de host `gate.linuss.com` ou um de seus clientes poderão usar o serviço de `sshd`.

Após concluída a configuração é conveniente rodar o **`tcpdchk`** para verificação de parâmetros em busca de possíveis erros de configuração que ocasionarão falhas no propósito de “barrar” o que nunca será bem-vindo.

```
[root@profundo]# tcpdchk
```

## 9. O arquivo /etc/aliases

O arquivo aliases pode facilmente ser utilizado para obter um privilégios de administrador do sistema se indevidamente configurado. A entradas neste arquivo favoreciam a troca de arquivos binários através do **mail** entre usuários , fazendo com que o arquivo binário fosse enviado e o /usr/bin/uucode o recebesse como usuário e efetuasse a conversão de ASCII para binário onde previamente já havia ocorrido a conversão do mesmo, tornando mais rápido a transferência.

Comente as linhas do arquivo relacionadas ao **decode** ou a qualquer outra referência a programas que não são utilizados .

```
# Basic system aliases -- these MUST be present.
MAILER-DAEMON: postmaster
postmaster:    root

# General redirections for pseudo accounts.
bin:           root
daemon:       root
#games:       root ← remover oucomentar
#ingres:      root ← remover oucomentar
nobody:       root
#system:      root ← remover oucomentar
#toor:        root ← remover oucomentar
#uucp:        root ← remover oucomentar

# Well-known aliases.
#manager:     root ← remover oucomentar
#dumper:      root ← remover oucomentar
#operator:    root ← remover oucomentar

# trap decode to catch security attacks
#decode:      root

# Person who should get root's mail
#root:        marc
```

Após remover as entradas não esquecer de carregar a base de aliases com o comando

```
[root@profundo]# /usr/bin/newaliases
```

## 10. Bloqueio a requisições de Ping

Impedir que requisições de ping sejam respondidas evita que informações sejam reveladas a respeito de topologias, serviços e muitas outras no que diz respeito ao sistema em questão.

```
echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Pode adicionar esta entrada no arquivo `/etc/rc.d/rc.local` para que esta configuração não se perca no próximo boot .

## 11. Bloqueie informações repassadas pelo telnet

Se você não quiser que seu sistema envie informação sobre serviços na tentativa de conexões remotas por telnet é necessário apenas alterar o arquivo `/etc/inetd.conf` com a seguinte linha referente ao telnet::

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd-h
```

Adicionando a opção `-h` ao final fará com que o daemon não exiba quaisquer informações na tentativa de se logar. Remotamente.

## 12. O arquivo `/etc/host.conf`

Edite o arquivo: `host.conf` (`vi /etc/host.conf`) e adicione as seguintes entradas :

```
# Lookup names via DNS first then fall back to /etc/hosts.  
order bind,hosts  
# Não possuímos múltiplas máquinas que utilizam vários endereços ips na mesma  
interface  
(like virtual server, IP Aliasing).  
multi off  
# Checagem por endereço de ip SPOOFING.  
nospoof on
```

.IP Spoofing : é uma técnica onde uma máquina passa assumir o papel de outra máquina que mantém uma relação confiável com o servidor em questão .

### 13. O arquivo `/etc/securetty`

O `/etc/securetty` é o arquivo onde se define em qual dispositivo TTY será permitido que o usuário root venha a se logar. Desabilite todos que não são necessários (vi `/etc/securetty`) :

```
tty1
#tty2
#tty3
#tty4
#tty5
#tty6
#tty7
#tty8
```

### 14. Contas especiais

O Linux fornece algumas contas padrões para que posterior a instalação do sistema operacional sejam usadas por algum daemon, é interessante excluir todas as contas que não vem sendo utilizada pelo sistema operacional ou por nenhum serviço em atividade.

Para excluir um usuário de seu sistema utilize o comando:

```
[root@profundo]# userdel username
```

Para excluir um grupo de usuário no Linux, execute:

```
[root@profundo]# groupdel username
```

Execute os comandos abaixo para apagar os usuários e grupos listados :

```
[root@profundo]# userdel adm
```

```
[root@profundo]# userdel lp
```

```
[root@profundo]# userdel sync
```

```
[root@profundo]# userdel shutdown
```

```
[root@profundo]# userdel halt
```

```
[root@profundo]# userdel mail (Apague caso você nao possua instalado o sendmail, procmail ou mailx).
```

```
[root@profundo]# userdel news
```

```
[root@profundo]# userdel uucp
```

```
[root@profundo]# userdel operator
```

```
[root@profundo]# userdel games (apague caso nao utilize o X Window Server).
```

```
[root@profundo]# userdel gopher
```

```
[root@profundo]# userdel ftp (delete caso não utilize o ftp anonymous).
```

Grupos:

```
[root@profundo]# groupdel adm
```

```
[root@profundo]# groupdel lp
```

```
[root@profundo]# groupdel mail (apague este grupo apenas se voce não tem o sendmail server, procmail e mailx instalados e com o serviço ativo).
```

```
[root@profundo]# groupdel news
```

```
[root@profundo]# groupdel uucp
```

```
[root@profundo]# groupdel games (apague apenas caso não utilize o X Window Server).
```

```
[root@profundo]# groupdel dip
```

```
[root@profundo]# groupdel pppusers
```

```
[root@profundo]# groupdel popusers (apague apenas não use o pop como servidor de email).
```

```
[root@profundo]# groupdel slipusers
```

Adicione os usuários necessários com o comando:

```
[root@profundo]# useradd username
```

Para adicionar a senha do usuário criado use o comando :

```
[root@profundo]# passwd username
```

Por exemplo:

```
[root@profundo]# useradd admin
```

```
[root@profundo]# passwd admin
```

Torná-lo imutável é imprescindível para evitar a sobreposição ou exclusão acidentalmente um arquivo. Ele também impede alguém de criar um link simbólico para este arquivo , que por sinal vem sendo apagado com freqüência em ataques do

tipo OWNED .

Os seguintes comandos devem ser usados:

```
[root@profundo]# chattr +i /etc/passwd
[root@profundo]# chattr +i /etc/shadow
[root@profundo]# chattr +i /etc/group
[root@profundo]# chattr +i /etc/gshadow
```

## 15. Bloqueando o su para qualquer usuário

Caso não deseje que o su seja executado para o root ou que haja restrição para qualquer usuário edite o arquivo referente ao su (`vi /etc/pam.d/su`) e adicione no início do arquivo as seguintes linhas:

```
auth sufficient /lib/security/pam_rootok.so debug
auth required /lib/security/pam_wheel.so group=wheel
```

Onde apenas usuários do grupo wheel podem dar um su para o root.

Para adicionar usuários ao grupo capaz de executar o su para o usuário root, no nosso caso o usuário admin, execute o comando como abaixo:

```
[root@profundo]# usermod -G10 admin
```

Onde a opção `-G` indica que estamos adicionando um grupo secundário no usuário admin, o número que o segue (10) indica o id do grupo em questão .

## 16. Definir limite de recursos

Definir limite de recursos para usuários previne contra possíveis ataques DoS providos pelos mesmos. Estes limites agregam processos, memória , etc . Para atingir todos os usuários deve ser configurado o arquivo `limits.conf` (`vi /etc/security/limits.conf`) , adicionando as seguintes linhas :

```
* hard core 0
* hard rss 5000
```

```
* hard nproc 20
```

A primeira linha proíbe a criação de “core files” ou seja o estado da memória em determinado momento , geralmente criado dentro do /proc.

A segunda linha restringe o uso da memória a 5M.

A terceira limita o número de processos a serem criados para 20.

Você deve editar também o arquivo /etc/pam.d/login , adicionar ou verificar a existência da seguinte linha:

```
session required /lib/security/pam_limits.so
```

Alterações estas aplicadas a todos os usuários do sistema.

## 17. Mais controle na montagem de sistemas de arquivos.

Há possibilidade de tornar algumas opções de segurança pertinentes logo na montagem de um sistema de arquivos. Estas configurações são feitas no arquivo fstab (vi /etc/fstab) . Opções como noexec, nodev, nosuid tornam as partições referentes aos respectivos pontos de montagem /home e /tmp mais customizáveis. Veja a seguir:

```
/dev/sda11 /tmp ext2 nosuid,nodev,noexec 1 2
```

```
/dev/sda6 /home ext2 nosuid,nodev 1 2
```

Onde *nodev* bloqueia a interpretação de caracteres ou blocos especiais no sistemas de arquivos, *nosuid* não permite que seja setado o id do dono de arquivo para demais usuários assim como o do grupo do dono , *suid* e *guid* . Por último o *noexec* que não permite a execução de nenhum binário no sistema de arquivos em questão .

## 18. Previna-se ao rodar o comando *rm -rf \** em diretórios

Aos diretórios considerados de extrema importância é de grande valia rodar o comando *touch -- -i* , fazendo com que não seja executado o comando em questão

```
(rm -rf *) .
```

Por exemplo:

```
[root@profundo]# cd /usr/  
[root@profundo]# touch -- -i
```

## 19. Shell logging

É extremamente recomendável setar os valores das variáveis HISTFILESIZE e HISTSIZE para um valor tão baixo quanto 20, estas variáveis são setadas através do arquivo `/etc/profile` e definem até quantos comandos antigos poderão ser guardados no `bash_history`. Também é necessário definir como imutável os arquivos `.bash_history` e demais arquivos do bash, utilizando o `chattr` definindo que neste arquivo só poderão ser acrescentados registros(linhas), não será possível apagar ou alterá-las.

Edite o profile (`vi /etc/profile`) e altere os respectivos valores para as variáveis:

```
HISTFILESIZE=20  
HISTSIZE=20
```

```
cd ~/ (ir para o home)
```

```
[root@profundo]# chmod 640 .bash_history  
[root@profundo]# chattr +A .bash_history  
[root@profundo]# chattr +A .bash_logout  
[root@profundo]# chattr +A .bash_profile  
[root@profundo]# chattr +A .bashrc
```

## 20. O `/etc/lilo.conf`

- a) Adicionar: `restricted`

É requerido senha para antes de passar quaisquer parâmetros para o LOADER, como o Single Mode.

b) Adicionar: `password = alguma_alguma`

Em conjunto com o modo restrito é definido a senha para passagem de acesso , onde desta forma estará tornando o sistema precavido contra leitura indevidas do lilo.conf por meio do Single-mode, por exemplo.

exemplo do arquivo lilo.conf (`vi /etc/lilo.conf`):

```
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
prompt
timeout=00 ← altere para 00
Default=linux
restricted ← add this line.
password=some_password ← adicione este linha.
image=/boot/vmlinuz-2.2.12-20
label=linux
initrd=/boot/initrd-2.2.12-10.img
root=/dev/sda6
read-only
```

`[root@profundo]# chmod 600 /etc/lilo.conf` (Irá retirar a permissão de leitura do arquivo).

`[root@profundo]# /sbin/lilo -v` (atualizar o lilo.conf).

Você pode ainda torná-lo imutável afim de aumentar a segurança a cerca deste arquivo:

`[root@profundo]# chattr +i /etc/lilo.conf` com isso você está prevenido contra eventuais descuidos (acidentais ou não) . Para desfazer basta retirar setar a opção `-i` junto ao comando `chattr` .

c) Adicione `timeout=X`

É interessante definir como 0 (zero) o tempo de espera para carregamento do sistema padrão, a menos que seja um servidor com DUAL BOOT .

## 21. Desabilitar o desligamento do sistema através do Ctrl+Alt+Delete.

É extremamente a utilização mútua dessas teclas caso não haja uma boa segurança física, onde seja extremamente restrito o acesso direto aos servidores. O arquivo em questão a ser configurado é o `/etc/inittab` :

```
[root@profundo]# vi /etc/inittab
```

Localiza a linha:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Comente :

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Agora carregue as alterações com :

```
[root@profundo]# /sbin/init q
```

## 22. Corrija as permissões para os scripts localizados em `/etc/rc.d/init.d`

```
[root@profundo]# chmod -R 700 /etc/rc.d/init.d/*
```

Onde apenas o usuário root poderá ler, escrever e executar os devidos scripts.

## 23. O arquivo `/etc/rc.d/rc.local`

Por padrão as identificações do sistema são mostradas antes do login no sistema, sendo necessário restringir essas informações ao prompt de usuário e senha.

Para não exibir estas informações será necessário apenas editar o `/etc/rc.d/rc.local` , comentando as seguintes linhas abaixo:

```

--
# This will overwrite /etc/issue at every boot. So, make any changes you
# want to make to /etc/issue here or you will lose them when you reboot.
#echo "" > /etc/issue
#echo "$R" >> /etc/issue
#echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue
#
#cp -f /etc/issue /etc/issue.net
#echo >> /etc/issue
--

```

Execute também :

```

[root@profundo]# rm -f /etc/issue
[root@profundo]# rm -f /etc/issue.net
[root@profundo]# touch /etc/issue
[root@profundo]# touch /etc/issue.net

```

## 24. Bit SUID e SGID

É extremamente importante remover o bit 's' dos programas. Quando aplicados faz com que o arquivo rode com as permissões de superusuário. Esta tarefa pode ser realizada com o comando `chmod a-s`.

Alguns programas necessitam a qualquer custo desse atributo de permissão para serem executados, pela maneira como inferem em configurações de arquivos e no próprio sistema de arquivos, por isso é bom ter precauções com os arquivos em questão.

Execute o comando abaixo para localizar os programas com o bit SUID e SGID respectivamente :

```

[root@profundo]# find / -type f \( -perm -04000 -o -perm -02000 \) \! -exec ls -lg {} \;

```

Alguns binários mostrados abaixo associados aos comandos para remoção (sinalizados com o asterisco, \*) estão sendo avaliados acordo a rotina de uso pelo próprio sistema. É essencial a verificação do próprio usuário sobre as rotinas de uso, lembre-se ,” trata-se de recomendações”.

-rwsr-xr-x	1	root	root	33120	Mar 21	1999	/usr/bin/at
*-rwsr-xr-x	1	root	root	30560	Apr 15	20:03	/usr/bin/chage
*-rwsr-xr-x	1	root	root	29492	Apr 15	20:03	/usr/bin/gpasswd
-rwsr-xr-x	1	root	root	3208	Mar 22	1999	/usr/bin/disable-paste
-rwxr-sr-x	1	root	man	32320	Apr 9	1999	/usr/bin/man
-r-s--x--x	1	root	root	10704	Apr 14	17:21	/usr/bin/passwd
-rws--x--x	2	root	root	517916	Apr 6	1999	/usr/bin/suidperl
-rws--x--x	2	root	root	517916	Apr 6	1999	/usr/bin/sperl5.00503
-rwxr-sr-x	1	root	mail	11432	Apr 6	1999	/usr/bin/lockfile
-rwsr-sr-x	1	root	mail	64468	Apr 6	1999	/usr/bin/procmail
-rwsr-xr-x	1	root	root	21848	Aug 27	11:06	/usr/bin/crontab
-rwxr-sr-x	1	root	slocate	15032	Apr 19	14:55	/usr/bin/slocate
*-r-xr-sr-x	1	root	tty	6212	Apr 17	11:29	/usr/bin/wall
*-rws--x--x	1	root	root	14088	Apr 17	12:57	/usr/bin/chfn
*-rws--x--x	1	root	root	13800	Apr 17	12:57	/usr/bin/chsh
*-rws--x--x	1	root	root	5576	Apr 17	12:57	/usr/bin/newgrp
*-rwxr-sr-x	1	root	tty	8392	Apr 17	12:57	/usr/bin/write
-rwsr-x---	1	root	squid	14076	Oct 7	14:48	/usr/lib/squid/pinger
-rwxr-sr-x	1	root	utmp	15587	Jun 9	09:30	/usr/sbin/utempter
*-rwsr-xr-x	1	root	root	5736	Apr 19	15:39	/usr/sbin/usernetctl
*-rwsr-xr-x	1	root	bin	16488	Jul 6	09:35	/usr/sbin/traceroute
-rwsr-sr-x	1	root	root	299364	Apr 19	16:38	/usr/sbin/sendmail
-rwsr-xr-x	1	root	root	34131	Apr 16	18:49	/usr/libexec/pt_chown
-rwsr-xr-x	1	root	root	13208	Apr 13	14:58	/bin/su
*-rwsr-xr-x	1	root	root	52788	Apr 17	15:16	/bin/mount
*-rwsr-xr-x	1	root	root	26508	Apr 17	20:26	/bin/umount
*-rwsr-xr-x	1	root	root	17652	Jul 6	09:33	/bin/ping
-rwsr-xr-x	1	root	root	20164	Apr 17	12:57	/bin/login
*-rwxr-sr-x	1	root	root	3860	Apr 19	15:39	/sbin/netreport
-r-sr-xr-x	1	root	root	46472	Apr 17	16:26	/sbin/pwdb_chkpwd

```
[root@profundo]# chmod a-s /usr/bin/chage
```

```
[root@profundo]# chmod a-s /usr/bin/gpasswd
```

```
[root@profundo]# chmod a-s /usr/bin/wall
```

```
[root@profundo]# chmod a-s /usr/bin/chfn
```

```
[root@profundo]# chmod a-s /usr/bin/chsh
```

```
[root@profundo]# chmod a-s /usr/bin/newgrp
```

```
[root@profundo]# chmod a-s /usr/bin/write
```

```
[root@profundo]# chmod a-s /usr/sbin/usernetctl
```

```
[root@profundo]# chmod a-s /usr/sbin/traceroute
```

```
[root@profundo]# chmod a-s /bin/mount
```

```
[root@profundo]# chmod a-s /bin/umount
```

```
[root@profundo]# chmod a-s /bin/ping
```

```
[root@profundo]# chmod a-s /sbin/netreport
```

## 25. Permissão World-wiretable

Caso um Cracker tenha acesso à máquina em questão, minimizar as possibilidades de impacto devido a alteração em arquivos ou até mesmo em links simbólicos é o mínimo que já se pode esperar para continuidade dos serviços em questão . Em diretórios ou arquivos World-writable qualquer pessoa pode alterar, caso em diretórios qualquer um pode criar ou remover arquivos dentro deste, em arquivo , ainda se pode editar os arquivos em questão . Esta permissão é notada da seguinte forma:

```
[root@profundo]# ls -l
```

```
-rw-rw-rw- 1 bbrazil bbrazil 0 Dec 25 20:08 file
```

^ esta é a indicação de que o arquivo é world-writable

## 26. Arquivos sem dono

Arquivos que apresentam nome do dono do arquivo ou grupo como nouser ou nogroup podem indicar que o sistema foi “ownado”.

```
[root@profundo]# find / -nouser -o -nogroup > unowed-results
```

Atenção: Arquivos reportados no `/dev` não contam .

## 27. Arquivo .rhosts

O arquivo `.rhosts` especifica quais usuários ou sistemas remotos podem acessar uma conta local utilizando rsh ou rcp. Um cracker só precisa de uma conta potencial para ter acesso à sua rede. O ideal é que não seja usado tal arquivo . Para localizar os arquivos use o comando:

```
[root@profundo]# find /home -name .rhosts > rhost-results
```

## 28. Considerações finais

Algumas ferramentas estão disponíveis para verificação de conformidades de acordo os assuntos abordados neste artigo, entre elas podemos destacar o Lynis (<http://www.rootkit.nl/projects/lynis.html>). Retorno as palavras do início do artigo “O

conceito de Segurança da informação é muito mais complexo que atributos técnicos abordados neste artigo. Tratar de segurança da Informação é tratar a Tecnologia da informação como processos de negócios aplicados a sustentabilidade de uma corporação” Por isso não limite-se a implementações técnicas pois a gestão de segurança também aplica à pessoas quando mal-aplicadas podem interferir e arruinar processos vitais ao negócio em questão.

This document was created with Win2PDF available at <http://www.win2pdf.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.  
This page will not be added after purchasing Win2PDF.