Hardening Unix Servers

Jairo Willian Pereira, *Hewlett Packard - Brasil*

***Abstract*— Hardening is a security process executed to protect systems against attackers. Usually include removal of unnecessary services, logins control, applying patches, kernel tuning, control over ports and monitoring about system use. The document, try provide to reader, any items cover by hardening process.**

***Index Terms*— Unix, Windows, Hardening, Security, perimeter, kernel, TCP/IP, bastion-hosts, endurecimento.**

I. INTRODUÇÃO

Tornar a vida do atacante mais difícil. Este, o principal conceito que esta por trás do "*Hardening* de Sistemas Operacionais", ação composta por um conjunto de atividades que visam máxima segurança, proteção e controle do equipamento alvo do "endurecimento".

Entre as atividades mais comuns do processo, mas não limitando-se a estas, podemos enumerar:

- Proteções e configurações que visam dificultar ataques físicos;
- Validações e *tunning* em sistemas operacionais pós-instalação;
- Controle e ajustes finos em serviços realmente necessários e/ou oferecidos;
- Controle de nível de atualização de *hardware/software (updates & upgrades);*
- Instalação, configuração, controle e manutenção de ferramentas de segurança;
- Implementação de uma política adequada e coerente de segurança.

Todas essas atividades referenciadas, devem ser planejadas e implementadas de acordo com o perfil do servidor. Um "*set* padrão de *hardening*", pode não ser interessante e eficaz para servidores com perfis diferentes, ou seja, uma política decente para um servidor de *Internet*, pode ser catastrófica se aplicada sem as devidas considerações a um servidor de arquivos.

Partindo desse modelo, o documento tenta oferecer um *baseline* referência para que o administrador possa utilizá-lo como um *checklist* de boas-práticas a ser observado durante o processo de proteção.

II. ESCOPO DE ATUAÇÃO

Embora os exemplos utilizem o ambiente *HP-UX* como referência dos testes e base de implementação, o autor preocupou-se em construir um *checklist* básico, que pudesse ser implementado em igual teor para outros sistemas operacionais de mesma linhagem. Assim, os controles apresentados podem ser portados para o ambiente *Linux, AIX, Mac OS* ou similares, apenas considerando as diferenças de ferramentas, exceções e particularidades de cada plataforma.

A planilha apresentada, foi utilizada para nortear as atividades e controlar a qualidade da implementação. Outros controles podem e devem ser adicionados, mas como anteriormente informado, esse *baseline* inicial presa pela garantia de uma política mínima, mas igualmente implementável em quaisquer plataformas.

Além da coluna com controles desejados, a planilha contém colunas para armazer informações de identificação do equipamento, atual condições e *status* do ativo, campos para adição de comentários pertinentes ao processo, além lembretes ou pendências a serem futuramente tratadas ou consideradas. Idealmente, para cada equipamento devemos preencher uma planilha, facilitando assim, o controle individualizado de cada ativo, suas condições, possíveis exceções, recomendações ou particularidades de cada ambiente. Em ambientes certificados e passíveis de auditoria, vale lembrar que a atualização deste documento, do *server datasheet*, e demais documentações pertinentes devem ser constantemente atualizadas, padronizadas e armazenadas em local adequado.

:: <cliente>			Ambiente HP-UX, <projeto>	
Referência	**Info**	**Status**	**CheckList**	**[?]**
IP	15.175.165.10	**OKAY!**	1. Instalação de Ferramentas	*
Hostname	Z1T1BRUXVAS01	**Partial!**	2. Patches de Segurança	*
Okay iSEC?	**pending...**	**OKAY!**	3. Controle de Login	*
Mudanca root passwd ?	NOK!	**OKAY!**	4. Encerramento de Sessões	*
Instalação AV?	N/A!	**OKAY!**	5. Variáveis de PATH	*
Classificacao (iSEC ID)	Stringent	**OKAY!**	6. Desabilitar permissões-padrão (umask)	*
Vulnerabilidades Status	N/A!	**OKAY!**	7. Ocultando logins e senhas	*
Issues & Riscos	N/A!	**OKAY!**	8. Qualidade de Senhas	*
		NOT!	9. Login Administrativo	*
		OKAY!	10. TCB – Trusted Computing Base	*
		OKAY!	11. Banner de Logon	*
		OKAY!	12. Banners de Serviços	*
		OKAY!	13. Logins e Grupos Desnecessários	*
		Partial!	14. Serviços Desnecessários	*
		OKAY!	15. Relações de Confiança	*
		OKAY!	16. Transmissão de Dados Criptografada	*
		OKAY!	17. UID-0	*
		OKAY!	18. Sincronização Horas - NTP	*
		OKAY!	19. Padrão nomenclatura servidor	*
		OKAY!	20. Habilitação auditoria,objetos,eventos & logs	*
		OKAY!	21. GSLU - Propagação Usuários	*
		OKAY!	22. Instalação ESM ou Medusa ou Bastille	*
		OKAY!	23. Segregação History	*
		OKAY!	24. Segregação Privilégios (sudo)	*

III. IMPLEMENTANDO SEGURANÇA

Agora que temos claramente o escopo definido, iniciaremos o processo de implementação das políticas e controles. Embora os controles apresentados já tenham um padrão desejado, é saudável mencionar que os valores e controles devem estar de acordo com o negócio ou política de segurança em vigência. Assim, os valores devem considerar as necessidades de cada ambiente.

1. Instalação de Ferramentas

Para cada ambiente uma necessidade específica. No caso *do HP-UX*, versões mais antigas não contemplam por padrão o substituto desejado ao *telnet*, *OpenSSH*. Mesmo nas versões mais recentes, a ferramenta *sudo* não vem inicialmente instalada. Para nosso cenário e objeto de estudo, vamos precisar instalar a última versão das seguintes ferramentas:

- OpenSSL/OpenSSH
  Necessário para prover ambiente de comunicação segura entre servidores e processo de administração. Futuramente, necessitaremos do uso de chaves pública e privada para facilitar algumas atividades.
- SUDO
  Ferramenta para minimizar o uso massivo da conta de *root*. Provê privilégios similares de modo controlado e com maior rastreabilidade.
- Tripwire
  Como mencionado, pode variar de ambiente para ambiente. Em nosso caso, não será utilizado, pois o controle sobre modificação de arquivos críticos do sistema será realizado de outra maneira.

No exemplo, a verificação da instalação dos pacotes solicitados a partir da sintaxe:

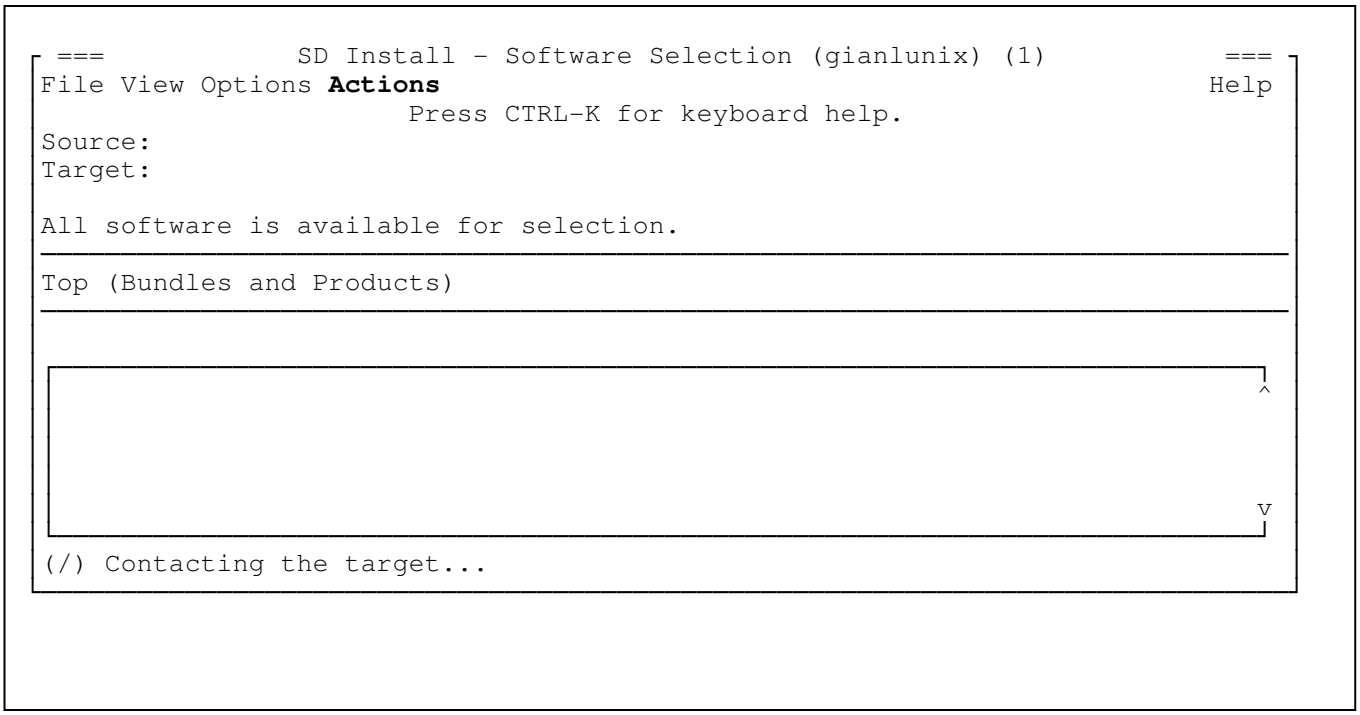
```
gianlunix:/root:# swlist OpenSSL
# Initializing...
# Contacting target "gianlunix"...
#
# Target:  gianlunix:/
# OpenSSL                  A.00.09.07e.012
Secure Network Communications Protocol
  OpenSSL.openssl          A.00.09.07e.012
Secure Network Communications Protocol
```

Caso os pacotes desejados não estejam instalados, podemos providenciar a instalação imediata a partir da seguinte instrução:

```
gianlunix:/root:# swlist -s /software/openssh-4.6p1-ia64-11.23.depot
```

Outra opção, seria a instalação interativa a partir do menu *Action*, *Install* do `swlist` apresentado a seguir.

```
gianlunix:/root:# swinstall
```



Para este controle, precisamosque as duas ferramentas informadas estarão instaladas e disponíveis para uso futuro neste documento. Se necessário, um estudo da *manpage* do *swinstall* poderá servir de referência para opções avançadas.

2. *Patches de Segurança*

É extremamente recomendado que o último "*Quality Pack*" esteja instalado em seu equipamento, além de todos os *patches* de segurança delta (liberados após o lançamento do último *Quality Pack (UX)* ou *Maintenance Level (AIX))*, além de possíveis *patches* de emergência.

Filtrando a saída fornecida pelo *swlist*, foi separado alguns *patches* que são extremamente importantes e que deveriam existir em sua instalação (considerando as versões específicas de cada sistema operacional). Além dos *patches* desejados, as últimas linhas retornaram informações das ferramentas anteriormente instaladas.

```
gianlunix:/root:# swlist
...
BUNDLE11i B.11.23.0409.3  Required Patch Bundle for HP-UX 11i v2 (B.11.23),
HWEnable11i B.11.23.0706.064 Hardware Enablement Patches for HP-UX 11i v2, June 2007
QPKAPPS B.11.23.0706.064  Applications Quality Pack Bundle for HP-UX 11i v2, June 2007
QPKBASE B.11.23.0706.064  Base Quality Pack Bundle for HP-UX 11i v2, June 2007
Sec00Tools B.01.02.00     Install-Time security infrastructure.
SecPatchCk B.02.02        HP-UX Security Patch Check Tool
OnlineDiag B.11.23.09.05  HPUX 11.23 Support Tools Bundle, June 2007
…
#
# Product(s) not contained in a Bundle:
#
DATA-PROTECTOR A.05.50     HP OpenView Storage Data Protector
OSIT-GII-ESAR-UX A.02.92     European System & Application Reporting Standard Components.
  R3-PERF  A.09.02     HP OpenView VantagePoint SMART Plug-In for SAP R/3: Performance Subagent
  gcc              4.1.1      gcc
  sudo             1.6.8p12   sudo
  openssh  4.6p1     openssh
```

Após a instalação, é aconselhável verificar as principais funções do sistema para garantir que *patches* não comprometeram nenhuma de suas características e funcionalidades.

Uma validação mais rápida e automatizada para ambientes *UX*, pode ser feita através do endereço http://www1.itrc.hp.com/, acesssando *Patch Database*. A partir deste site, um *script* pode ser baixado (*swainv*) e executado localmente no equipamento

desejado. Um arquivo *XML* é gerado localmente, o qual deve ser feito *upload* ao *site* do fornecedor. Feito a descarga, é gerado um empacotamente específico para a versão do seu sistema com todas as atualizações, manual de uso e *script* para aplicação das mudanças. Acelera em muito o processo e é bem individualizado.

Em sistemas *AIX*, validar através do link http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp quais são os últimos níveis de *ML (Maintenance Level Packages), TL (Technology Level)* e *SP (Service Packs)*. Nos servidores, aplicar o comando "oslevel –s" para checar *TL's* e *SP's*, e o comando "oslevel –r" para checar os ML's.

Independente da plataforma, tenha certeza que *patches* estejam atualizados, usando as dicas oferecidas ou seu método pessoal.

3. *Controle de Login*

Embora importantes, normalmente algumas opções para controle de *login* ficam comentadas ou em algumas versões, o arquivo inicial simplesmente não existe.

```
gianlunix:/etc/default:# ls -la
total 96
dr-xr-xr-x      2  bin                bin
96 Nov 10  2006 .
dr-xr-xr-x     32  bin                bin
8192 Dec 10 00:20 ..
-r--r--r--      1  bin                bin
11 Nov  9  2006 fs
-r--r--r--      1  root              root
626 May  6  2005 nlspath
-r--r--r--      1  root              root
818 Jul  1  2005 syslogd
-r--r--r--      1  bin                bin
84 Oct 28  2004 useradd
```

Caso o arquivo exista, basta editá-lo e ajustar os parâmetros de interesse. Em nosso caso, iremos criar o arquivo e habilitar as opções relevantes:

```
gianlunix:/etc:#echo
"PASSWORD_MAXDAYS=90"                    >>
/etc/default/security
gianlunix:/etc:#                        echo
"PASSWORD_MINDAYS=3"                      >>
/etc/default/security
gianlunix:/etc:#echo
"PASSWORD_WARNDAYS=7"                    >>
/etc/default/security
gianlunix:/etc:#echo
"PASSWORD_HISTORY_DEPTH=10"              >>
/etc/default/security
gianlunix:/etc:#echo
"MIN_PASSWORD_LENGTH=8"                  >>
/etc/default/security
```

- *PASSWORD_MAXDAYS* – Duração máxima de uma senha em dias.
- *PASSWORD_MINDAYS* – Duração miníma da senha em dias. Bloqueia trocas freqüentes.
- *PASSWORD_WARNDAYS* – Mensagem de alerta em número de dias antes da expiração.
- *MIN_PASSWORD_LENGTH* – Tamanho minímo aceito em quantidade de caracteres.

Outras opções interessantes a serem consideradas são:

- *Login Interval* - Intervalo de tempo, em segundos, que, caso ocorram X tentativas de *logon* com senhas incorretas, a conta será bloqueada.
- *Login Re-enable* - Intervalo de tempo, em minutos, que o sistema aguarda até reabilitar uma conta bloqueada por tentativas de acesso com senhas incorretas (condição acima).
- *Login Delay* - tempo, em segundos, que o terminal espera até permitir que outro *login* seja realizado após um *login* bem-sucedido – forma de combater ataques *DoS* (*Denial of Service*) ou de Força Bruta.

A quantidade de opções é bem extensa, porém apenas implementando parte do *set* informado, já temos um ambiente em acordo com uma política de senha forte. Veremos quando tratarmos do controle *TCB (Trusted Computing Base)*, que parte dos parâmetros são manipulados com ferramentas específicas quando o ambiente está em *trusted-mode* (que ainda não é nosso caso).

```
gianlunix:/etc/default:#
/usr/lbin/getprdef -r
System is not trusted.
```

Uma das vantagens do *TCB*, é que os *hashes* criptográficos das senhas, não ficam mais armazenados em /etc/passwd quando passamos para esse modo. Observe as condições atuais:

```
gianlunix:/etc/default:# grep pere /etc/passwd

japere:S8gruuIDTOE7Q:398:20:Jack   Smith,HPS-SC,
LAC iSEC,8043,:/home/japere:/usr/bin/ksh
papere:A2cyVRJYDHdn.:399:20:Paul     Satriani,IT
Services,4017,:/home/papere:/usr/bin/ksh
repere:flAM.JdYrkcts:455:20:George Gaton,HPSSC -
2nd NIX,6967,:/home/repere:/usr/bin/ksh
```

Esse tipo de armazenamento, devido a herança de permissões do *Unix* e fragilidades do *hash*, é extremamente perigoso e fácil de se comprometer. Veremos em *TCB*, como melhorar esse cenário.

4. *Encerramento de Sessões*

. O ajuste, permite que consoles esquecidas em utilização possam ser desconectadas minimizando acessos indevidos. Habilitar para sessões remotas e locais (consoles seriais), variável de ***TIMEOUT*** automático para derrubar sessões e terminais inativos após um certo período é algo desejado.

```
gianlunix:/etc/default:# echo $TMOUT
0
```

O valor padrão para a maioria dos sistemas *Unix* é infinito (0). Injetaremos código em /etc/profile para garantir que um valor mais seguro possa ser propagado para todo o ambiente.

```
echo  "#  Security  Session  Timeout"  >>
/etc/profile
echo "TMOUT = 300" >> /etc/profile
echo "export TMOUT" >> /etc/profile
```

As entradas, definem em 5 minutos (300 segundos) o tempo para a sessão e permite exportar a variável globalmente. Após próximo *logon* ao servidor, o novo valor já estará em operação, sendo:

```
gianlunix:/etc/default:# ssh localhost 'echo $TMOUT'
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 92:02:7b:32:39:dc:14:b5:e6:12:3e:32:9c:ed:31:94.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
300
```

Pensando em um cenário de multiplas aplicações, seria prudente que o administrador tratasse cada conta de aplicação separadamente, usando um modelo global e tratando as exceções quando necessário. Os arquivos específicos de *shells* (e.g. .bash_profile) podem ser uma forma de personalização, além do .profile de cada conta existente. Contas futuras, podem ser contempladas alterando /etc/skel/.bash_profile.

5. Variáveis de PATH

Rever *paths* configurados no perfil global, além do diretório de root pode ajudar em reter a execução descontrolada de binários em quaisquer localizações. Entradas na variável *PATH* que apontem para o diretório raiz (.) permitem a execução de qualquer binário seja pesquisada em todo *file-system*.

```
gianlunix:/etc/default:# echo $PATH

/usr/sbin:/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/contrib/bin:/opt/hparray/bin:/opt/nettladm/bin:/opt/upgrade/bin:/opt/fcms/bin:/opt/resmon/bin:/usr/bin/X11:/usr/contrib/bin/X11:/opt/pd/bin:/opt/gnome/bin:/opt/perf/bin:/usr/sbin/diag/contrib:/opt/mozilla:/opt/wbem/bin:/opt/wbem/sbin:/opt/graphics/common/bin:/opt/hpsmh/bin:/opt/prm/bin:/opt/ssh/bin:/opt/wlm/bin:/opt/gwlm/bin:/opt/ignite/bin:/opt/perl/bin:/usr/local/bin:/usr/local/sbin:/opt/OV/bin:/opt/pwp+/bin:/bin/expect:/sbin:/home/root
```

Felizmente o diretório raiz (.) não está especificado, porém a quantidade de entradas ainda é grande. Temos também a referência direta as linguagens *Perl* e *Expect* que devem ser validadas se realmente são necessárias ao ambiente em análise.

Caso mudanças sejam necessárias, os informações encontram-se em /etc/PATH.

6. Desabilitar permissões-padrão desnecessárias

Arquivos recém-criados nos sistema devem, por padrão, permitir permissões de escrita, leitura e execução adequadas ao dono do arquivo e ao mesmo tempo negar escrita aos membros do mesmo grupo ou a outros. Definir o parâmetro de ***UMASK*** como **022**, permite que arquivos sejam criados com permissão 755, o que garante as premissas solicitadas.

```
gianlunix:/etc/default:# umask
022
```

Ajustes podem ser feitos adicionando o conteúdo abaixo em /etc/profile.

```
# Added for Security
umask 22
```

Outra opção seria procurar e adicionar ou habilitar a entrada em /etc/default/security

```
# Default umask value upon login. Note: This parameter controls
# umask(2) of all sessions initiated via pam_unix(5) and/or pam_hpsec(5).
UMASK=022
```

O valor é suficiente, mas algumas implementações preferem máscara 027. Estude e decida pelo melhor e mais adequado modelo para seu ambiente.

7. Ocultando logins e senhas

O arquivo **.netrc** possuem *logins* e senhas para alguns serviços "r", usado também como processo de *login* automático em sessões de *FTP*. Execute uma busca geral no sistema pelo arquivo .netrc e verifique seu conteúdo.

```
gianlunix:/etc/default:# find / -local -name .netrc
/home/interfaz/.netrc

gianlunix:/etc/default:# more /home/interfaz/.netrc

machine inter_peru login ftpinterprete password cisco21
machine inter_mexico login interprete password fas@200
```

Devem ser localizados e removidos do ambiente, optando por outra solução que não armazene essas informações em "texto-puro" em arquivos espalhados pelo sistema. Aconselha-se minusciosa análise de *logs* no sistema para identificar sistemas e aplicações que possam estar utilizando o método. Caso realmente não posso ser executada a remoção instantânea do arquivo, o mesmo deve ter permissão 600.

8. Qualidade de Senhas

Outros artifícios podem ser habilitados para garantir um controle de qualidade mais efetivo no quesito "senha forte". A maioria dos *Unices* permitem que uma série de atributos sejam controlados, e somente se, estes forem cumpridos, o sistema permite as mudanças desejadas. Dentre alguns itens interessantes, podemos utilizar:

- Checar que senhas não incluam determinadas *strings* ou palavras (uso de dicionário);
- Número máximo de caracteres que podem ser repetidos em uma senha;
- Número máximo de semanas após expiração em que a senha pode ser substituída;
- Número mínimo de caracteres alfabéticos que a senha deve conter;

- Número mínimo de caracteres não-alfabéticos que a senha deve conter;
- Número mínimo de numerais que a senha deve conter;
- Tempo máximo e mínimo para troca das senhas;
- Número de dias anteriores à expiração da senha em que o usuário recebe alerta de expiração;
- Histórico de senhas utilizadas, impedindo reutilizações;
- Tamanho mínmo de senha e impedir uso de senhas em branco (**null passwords**);

Para nosso experimento, via arquivo /etc/default/security garantimos os seguintes complicadores:

```
# Minimum length of NEW passwords.
MIN_PASSWORD_LENGTH=8

# Trusted mode only: password history
depth
PASSWORD_HISTORY_DEPTH=10

# Optional restrictions for new passwords
PASSWORD_MIN_UPPER_CASE_CHARS=1
PASSWORD_MIN_LOWER_CASE_CHARS=1
PASSWORD_MIN_DIGIT_CHARS=1
PASSWORD_MIN_SPECIAL_CHARS=1

# Standard and Shadow modes only: number
# of days that passwords are valid
PASSWORD_MAXDAYS=90
PASSWORD_MINDAYS=3

# Shadow mode only: number of days prior
to
# password expiration to give a warning
PASSWORD_WARNDAYS=14
```

Apenas para efeito comparativo, em ambientes *AIX* em **/etc/security/user** temos:

```
dictionlist = /usr/share/dict/words
maxrepeats = 2
maxexpired = 2 weeks
minalpha = 2
minother = 2
maxage = 90
minage = 7
pwdwarntime = 14 days
histsize/histexpire = 10
minlen = 8
```

No *Linux*, os controles *default* são mais modestos. Outras extensões podem ser habilitadas utilizando módulo *PAM*, adicionando muito mais recursos e controles. Veja *manpages PAM* para mais detalhes.

9. *Login Administrativo*

O acesso direto via *root* deve ser desabilitado para *logins* remotos e habilitado somente para *logins* via console serial. Usuários autorizados a terem acesso administrativo devem utilizar suas contas individuais e somente após conexão no equipamento, fazer uso controlado da conta de *root* (se realmente necessário) utilizando o "**su – root**". Idealmente, "su – root" deve ser desencorajado, preferindo execução de comandos previamente permitidos via **sudo**.

Valide se o valor "*console*" está descomentando dentro do /etc/securetty.

```
gianlunix:/home/japereir:$ more
/etc/securetty
console
```

Em ambientes *AIX*, muda um pouco a semântica e localização.

```
# more /etc/securety/login.cfg
/dev/console
```

10. *TCB – Trusted Computing Base*

Habilitar o modo *Trusted (TCB – Trusted Computing Base)* durante a instalação do Sistema Operacional (*BOS – Base Operating System*), além de aumentar o nível de segurança e controles sobre alguns arquivos base, permite extender a quantidade de opções oferecidas para cobrir questões relacionadas a segurança.

O processo é bem simples, e está amarrado a execução de dois comandos, sendo:

```
/usr/lbin/tsconvert     # conversao para Trusted
Mode
/usr/lbin/modprpw  -V  #  refresh  tempo  vida
password para data corrente
```

O primeiro comando, faz a extrusão dos *hashes* de senha do arquivo /etc/passwd, cria a estrutura de propagação de controles do *TCB* (/tcb), além aplicar alguns valores padrão. Observe a execução no equipamento atual:

```
gianlunix:/:# /usr/lbin/tsconvert
Creating secure password database...
Directories created.
Making default files.
System default file created...
Terminal default file created...
Device assignment file created...
Moving passwords...
secure password database installed.
Converting at and crontab jobs...
At and crontab files converted.
```

O processo invalida as contas atuais expirando-as, forçando o usuário a efetuarem mudanças de acordo com os novos valores já no próximo *login*. Uma maneira de evitar esse problema (que pode parar aplicações em execução e ser danoso a outras contas), seria fazendo um *refresh* do tempo de expiração das senhas. Assim, as mudanças, seriam solicitadas somente quando a conta expirasse.

```
gianlunix:/:# /usr/lbin/modprpw -V
gianlunix:/:#
```

Observe as mudanças em função do cenário anterior e o atual respectivamente:

```
gianlunix:/etc/default:#
/usr/lbin/getprdef -r
System is not trusted.

gianlunix:/etc/default:#
/usr/lbin/getprdef -r
NO, 0, 8, 0, 0, -1, 0, YES, YES, NO, NO,
NO, YES, 3, 10, 2, 0
```

tsconvert nao checa inconsistências de base *NIS*, estruturas de arquivos e outros problemas antes de executar a conversão – simplesmente a faz. Os seguintes comandos devem ser executados quando o ambiente possuir *NIS* para validação do arquivo de password e grupos.

```
/usr/sbin/pwck -s && /usr/sbin/grpck

gianlunix:/home/japereir:$ /usr/sbin/pwck
-s

webadmin:*:40:1::/usr/obam/server/nologin
dir:/usr/bin/false
        Login directory not found

iwww:*:102:1::/home/iwww:/sbin/sh
        Login directory not found

Checking protected database password
files...
Not Superuser.
```

Neste caso, os problemas são simples. Podem ser corrigidos ou a conversão efetuada sem maiores problemas. Efetuada a conversão uma nova estrutura a partir do diretório raiz é criada (/tcb).

Todas as informações individiduais de cada conta, modelos de segurança, *hashes*, informação do usuário e exceções estarão armazenadas a partir deste momento nesta estrutura. Os diretórios correspondem as inicias (a-Z) de cada conta do sistema, e na estrutura *system*, os padrões globais.

```
gianlunix:/tcb/files/auth:# ls

A       G       M       S       Y       e
k       q       v
B       H       N       T       Z       f
l       r       w
C       I       O       U       a       g
m       s       x
D       J       P       V       b       h
n       system  y
E       K       Q       W       c       i
o       t       z
F       L       R       X       d       j
p       u


gianlunix:/tcb/files/auth/r:# ls

radiaz      resilva    rispolon   robednar
root        royoda
raporto     riacuna    ritonett   rolopes
roteixei     rusouza
rasilva     rimattos   rizanett   ronaito
rotrevel
```

E o conteúdo de cada conta e arquivo, diz respeito as informações individuais de cada perfil.

```
gianlunix:/tcb/files/auth/r:# more root
root:u_name=root:u_id#0:\
     :u_pwd=SOezDpxGB1ONY:\
     :d_boot_authenticate@:\
     :u_auditflag#1:\

:u_minchg#0:u_succhg#1196340939:u_unsucchg#11913
45971:u_pw_expire_warning#0:\
:u_pswduser=root:u_suclog#1197383907:u_suctty=pt
s/2:u_unsuclog#1197383844:\
     :u_maxtries#0:u_lock@:chkent:
```

Existem outros campos não padrão que podem ser inseridos ou modificados. Observe uma pequena descrição de alguns campos e conteúdos: Um @ antes da entrada, significa que está desativada.

```
Entry        Description
u_minchg       min time (in secs) before pwd can
be changed, again
u_exp          accout expires (sec since account
creation)
u_life         pwd lifetime (sec until this pwd
can be re-used)
u_genpwd       generate pronounceable passwords
u_genchars     generate a string of characters
u_genletters   generate a string of letters
u_pickpw       user can pick password
```

Opções *default* da estrutura *system*, conforme mencionado, são propagadas com os padrões:

```
gianlunix:/tcb/files/auth/system:# more default

default:\
        :d_name=default:\
        :d_boot_authenticate@:\
        :u_pwd=*:\
        :u_owner=root:u_auditflag#-1:\

:u_minchg#0:u_maxlen#8:u_exp#15724800:u_life#169
34400:\

:u_pw_expire_warning#604800:u_pswduser=root:u_pi
ckpw:u_genpwd@:\

:u_restrict@:u_nullpw@:u_genchars@:u_genletters@
:\

:u_suclog#0:u_unsuclog#0:u_maxtries#3:u_lock:\
        :\

:t_logdelay#2:t_maxtries#10:t_login_timeout#0:\
        :chkent:
```

A página de manual de *modprdef, modprpw, getprdef* poderá ajudar entender quais as melhores opções dos parâmetros e qual melhor se adequa as necessidades do ambiente. Inicialmente, os valores padrões são bem consideráveis. As respectivas *manpages*, têm detalhadamente a função e descrição de cada opção demonstrada. Esses valores, devem estar de acordo com as necessidades do cliente, de seu negócio ou aplicação.

11. Banner de Logon

Por padrão, alguns sistemas definem o banner de logon para apresentar o nome do host, versão do sistema operacional, *kernel* e outras informações particulares. Essas informações são extremamente valiosas quando um "invasor" está a procura de brechas ou problemas de segurança.

Por questões de segurança (por obscuridade), e por questões legais, este banner deve ser removido e trocado por um alerta contra uso não-autorizado, e informando sobre questões legais.

```
=========================================
============================
= This is a private system operated by
Dvox Company & Telecom for   =
=  <cust._name>  business.  Authorization
from DCT or <cust._name>     =
=  management  is  required  to  use  this
system. Use by unauthorized    =
=       persons       is       prohibited.
=
=  WARNING  -  This  computer  system  is
accessed by authorized users    =
=             outside of <customer_name>.
All security and control    =
=             procedures must be strictly
followed.                   =
=========================================
============================
```

Os arquivos relacionados com este tipo de controle são:

```
/etc/issue
/etc/issue.net
/etc/motd
/etc/copyright
```

Adeque-os aos interesses do seu negócio, e preocupe-se também com aspectos legais.

12. Banners de Serviços

Da mesma forma, *banners* de serviços como *FTP*, *Telnet* e *SMTP* também revelam informações sobre a versão dos serviços e níveis de *patches* aplicados. Os serviços devem ser reconfigurados tendo em vista a desativação destes recursos e, quando possível, a substituição dos *banners* por versões simples e seguras. Efetue conexões nas portas de alguns serviços do ambiente e observe se são reveladas informações críticas sobre os serviços (nome, versão, patch level, etc.).

Observe as condições atual no servidor analisado, e veja se podem ser comprometedoras as informações disponíves:

```
gianlunix:/home/japereir:$ telnet localhost 21
Connected to localhost.
Escape character is '^]'.
220 gianlunix FTP server (Revision 1.1 Version
wuftpd-2.6.1(PHNE_34698) Fri Nov 10 10:21:03 GMT
2006) ready.

gianlunix:/home/japereir:$ telnet localhost 25
Connected to localhost.
Escape character is '^]'.
220    gianlunix    ESMTP    Sendmail    8.11.1
(PHNE_35485)/8.11.1; Tue, 11 Dec 2007 11:59:17 -
0300 (SAT)

gianlunix:/home/japereir:$ telnet localhost
Connected to localhost.
Escape character is '^]'.
Local flow control on
Telnet TERMINAL-SPEED option ON

HP-UX gianlunix B.11.23 U ia64 (ta)

login:
```

Observe que todos os serviços retornaram informações preciosíssimas sobre versões instaladas, o que pode ajudar o atacante a direcionar seu ataque em sistemas conhecidos, além

de facilitar o uso de *exploits*. Vamos fazer algumas modificações simples observar o resultado. Para os serviços de *Telnet* e *FTP*, as mudanças são no arquivo /etc/inetd.conf, sendo:

11.1 Telnet

```
- Original
telnet            stream   tcp6   nowait   root
/usr/lbin/telnetd   telnetd

- Ajustado
telnet            stream   tcp6   nowait   root
/usr/lbin/telnetd   telnetd -b /etc/issue
```

11.2 FTP

```
- Original
ftp       stream tcp6 nowait root /usr/lbin/ftpd
ftpd

- Ajustado
ftp       stream tcp6 nowait root /usr/lbin/ftpd
ftpd -l -a
```

A opção –l habilita *logs* para *syslogd* e –a habilta o serviço de *FTP* para ler e validar um arquivo *ftpaccess*. Execute /usr/bin/ckconfig para validar *PATHs* ativos de *FTP* e localização de arquivos de configuração. Após essa ativação, o arquivo *ftpaccess* deve conter pelo menos:

```
# Security Baseline for FTP
banner /etc/issue
greeting terse
#suppresshostname yes
#suppressversion yes
```

Supress version/hostname em algumas versões estão descontinuada e não funcionam. Procure pelo substituto de acordo com a versão de seu serviço.

Para o serviço de *email*, o arquivo a ser modificado é sendmail.cf. Como pode variar sua localização em função de versão e sistema operacional, procure suaa exata localização.

11.3 SMTP

```
- Original
# SMTP initial login message (old $e macro)
O SmtpGreetingMessage=$j Sendmail $v/$Z; $b
O PrivacyOptions=authwarnings, restrictqrun


- Ajustado
# SMTP initial login message (old $e macro)
O SmtpGreetingMessage=
O PrivacyOptions=
```

OBS: não esqueça de reinicializar os serviços para que as mudanças tenham efeito!

Agora, vamos rever as atuais condições no servidor analisado, e ver se melhorou o cenário:

```
gianlunix:/home/japereir:$ telnet localhost 21
Trying...
Connected to localhost.
Escape character is '^]'.
```

```
220-
================================================
====================
220-=
=
220-= This is a private system operated by Dvox
Company & Telecom for   =
220-= <cust._name> business. Authorization from
DCT or <cust._name>     =
220-= management is required to use this system.
Use by unauthorized    =
220-=       persons       is       prohibited.
=
220-=
=
220-= WARNING - This computer system is accessed
by authorized users    =
220-=           outside of <customer_name>. All
security and control    =
220-=              procedures must be strictly
followed.                  =
220-=
=
220-
================================================
====================
220 FTP server ready.
```

```
gianlunix:/home/japereir:$ telnet localhost 25
Trying...
Connected to localhost.
Escape character is '^]'.
220  ESMTP
```

```
gianlunix:/home/japereir:$ telnet localhost
Trying...
Connected to localhost.
Escape character is '^]'.
Local flow control on
Telnet TERMINAL-SPEED option ON

login:
```

13. Logins e grupos desnecessários

Desativar contas de serviços padrão/desnecessários, não utilizadas no dia-a-dia do ambiente é uma prática extremamente recomendada. Além de contribuir para que contas não sirvam de mecanismo de entrada/exploração, facilita a administração e controle sobre acesso.

```
gianlunix:/home/japereir:$ more /etc/passwd
root:*:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp
/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/u
ucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
smbnull:*:101:101:DO NOT USE OR DELETE - needed
by Samba:/home/smbnull:/sbin/sh
sshd:*:102:102:sshd
privsep:/var/empty:/bin/false
hpsmh:*:105:103:System                Management
Homepage:/home/hpsmh:/sbin/sh
sfmdb:*:106:20::/home/sfmdb:/sbin/sh
opc_op:*:777:77:VPO                        default
operator:/home/opc_op:/usr/bin/ksh
```



```
gslu:*:1100:20:Ger.     Seg.     Logica     de
Usuarios:/home/gslu:/sbin/sh
...
```

São exemplos de contas que podem ser desabilitadas: ***guest***, ***imnadm***, ***ldp***, ***uucp*** e ***nuucp***.
Os respectivos grupos relacionados as contas desnecessárias/removidas, devem ser também eliminados. Para o cenário proposto as contas referenciadas serão removidas. Identifique suas necessidades e elimine o que for necessário.

14. Serviços Desnecessários

Muitos serviços são configurados automaticamente durante a instalação e o *startup* da máquina, porém muitos deles não são necessários para o escopo/perfil do servidor em questão. O seguinte comando pode lhe ajudar com a tarefa:

```
gianlunix:/home/japereir:$ grep -v "^#"
/etc/inetd.conf | sort -u

...
chargen      dgram  udp6 nowait root internal
chargen      stream tcp6 nowait root internal
daytime      dgram  udp6 nowait root internal
daytime      stream tcp6 nowait root internal
discard      dgram  udp6 nowait root internal
discard      stream tcp6 nowait root internal
echo         dgram  udp6 nowait root internal
echo         stream tcp6 nowait root internal
exec                  stream  tcp6  nowait  root
/usr/lbin/rexecd   rexecd
ftp                   stream  tcp6  nowait  root
/usr/lbin/ftpd     ftpd -l -u002
rpc     dgram           udp      wait      root
/usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd
telnet                stream  tcp6  nowait  root
/usr/lbin/telnetd  telnetd
tftp                  dgram    udp    wait     root
/usr/lbin/tftpd    tftpd\
time         stream tcp6 nowait root internal
...
```

Muitos destes serviços possuem vulnerabilidades, sendo que uma boa parte desnecessários devendo ser desativados. **telnet, ftp, remshd, rlogind, finger, echo, discard, daytime, chargen, time, bootps, walld, rexd, uucp, ntalkd, xntpd, rbootd, mrouted e rwhod**, são exemplos de possíves candidatos a desativação. Após essa inspeção para validar as necessidades do perfil do servidor, certifique-se que os arquivos **/etc/inetd.conf**, **/var/adm/inetd.sec** e **/etc/inittab** possuem *root* como dono e estejam com permissão **600**.

15. Relações de Confiança

As relações de confiança entre os *hosts* devem ser montadas em cima da estrutura **OpenSSH** com autenticação via chaves públicas e chaves de *hosts*. Serviços como **remshd** e **rlogind** devem ser desabilitados, e todos os arquivos **.rhosts** e **hosts.equiv** devem ser removidos do sistema.

```
gianlunix:/:# find / -name *rhost*
/home/fapadm/.rhosts

gianlunix:/:# more /home/fapadm/.rhosts
fasacire        root
fasa1re         root
```

```
fasaclre        root
```

Idealmente, isto deve ser feito antes da instalação e configuração das principais aplicações, para que as mesmas utilizem configuração baseada em ssh como padrão desde início de implantação. Caso sejam descobertos a posteriori, trabalho adicional vai ser necessário para identificar as necessidades desta relação promíscua. Em ambientes grandes, a quantidade de relacionamentos é fator complicador (regra *full-mesh*).

16. Transmissão de Dados Criptografada

Serviços e comandos cuja transmissão de dados é feita em texto puro (*clear-text*) devem ser desativados. A desativação pode ser feita através do inetd.conf ou usando o comando **securetcpip**. Os principais vilões são: **telnet, ftp, tftp, rcp, rsh, rshd, rlogin** e **remsh**. Em seu lugar, deve ser utilizado o *OpenSSH* e suas respectivas ferramentas (**ssh**, **scp**, **sftp**, etc.), que permitem transmissão de dados com criptografia e uso de chaves públicas/privadas.

Assim, recomenda-se fortemente o uso de *ssh*, e desativação dos serviços mencionados o mais rápido possível.

17. UID-0

Sistema bem comportados deve considerar a existência de somente um usuário com UID 0 no sistema - usuário ***root***.

```
gianlunix:/:# grep :0: /etc/passwd
root:*:0:3::/:/sbin/sh
```

Verifique a existência de outros super-usuários e providencie a eliminação de seus priviégios. Felizmente, estamos imune ao problema.

18. Sincronização de horas - NTP

Sua rede deve possuir um servidor de *NTP* para garantir que os servidores possuam uma referência de data e hora comum, e facilite quando necessário a localização e manipulação de *logs*.

Em ambientes onde o servidor *NTP* está disponível, apenas a inserção na *crontab* do seguinte comando é suficiente.

```
0   11,23   *   *   *   /usr/sbin/ntpdate
IP_NTP_SERVER
```

O comando permite que 2 vezes ao dia seja iniciado um processo de verificação da hora, e realiazado os ajustes necessários. Em ambiente que existam controladores de domínio, o próprio DC serve de servidor NTP. Caso não seja o seu caso, procure informações para subir um servidor NTP para o ambiente, ou veja a possibilidade de usar um serviço externo de alguma autoridade confiável. No Brasil, o Observatório Nacional oferece o serviço, disponível para acesso público no endereço 200.20.186.75, porta 123 UDP.

19. Padrão de nomenclatura do servidor

Parece não ser considerável, mas servidores com nomes dedutíveis não são recomendados. Validar se equipamento está em conformidade com política de nomenclatura do ambiente, sendo desejado (não obrigatório) que esta nomenclatura não caracterize o "perfil" do servidor. Acrônimos e mneumônicos são preferencialmente desejados ao invés de:


```
- wwwserv      - prnserver     - bruxdns001
- ftpserv      - isaproxy      - brw2kisa02
```

Prefira algo mais abstrato e que faça sentido somente para quem conhece a codificação. Exemplo:

```
- z1t2brpavlf01   - z1t2brpaptp01
```

Não faz muito sentido, a não ser que alguem conheça o mecanismo. **Z1** (*Zone* 1), **T1** (*Tier* 2), **BR** (*Brazil*), **PA** (Porto Alegre), **V**/P (*Virtual* ou *Phisical*), **L**/T (*Live* ou *Test*), **F**/P (*File Server* ou *Proxy*) e **0x** como elemento de sequenciamento das máquinas. Interessante não?

20. Habilitação auditoria, objetos, eventos & *logs*

Logs de auditoria são essenciais quando precisamos levantar informações sobre operações em obejtos diversos (diretórios, arquivos...), levantamento de eventos (remoção de pastas, aumento de privilégios, acessos indevidos...) ou vasculhamento dos próprios *logs* e seu contéudo. Se não houver uma maneira de interligar esses eventos, ficará muito difícil prover rastreabilidade de algum evento crítico. Sempre que possível, *logs* devem ser armazenados externamente ao servidor ao qual esta sendo coletado.

Contabilidade de eventos de sistema, (*CPU, I/O* de disco e memória) podem ser ativados através de:

```
/etc/rc.config.d/acct
START_ACCT=1
```

Rastreabilidade de commandos, *system-calls* e outros controles em nível de *kernel* podem ser manipuladas via comando *audisp*, e habilitadas através de:

```
/etc/rc.config.d/auditing
AUDITING=1
PRI_SWITCH=10000
SEC_SWITCH=10000
```

Quando habilitar tais recursos, considerem também como parte da política:

- Ajustar tamanho *log Security* para tamanho desejado e legal;
- Definir/checar demais valores de acordo com política do ambiente;
- Definir rotatividade/armazenamento de acordo com política corrente;
- Ajustar eventos e objetos a serem auditados.

21. GSLU – Propagação de usuários

A propagação de usuários no ambiente, deve seguir um padrão conhecido, e possuir mecanismos de alocar cada usuário em seus respectivos grupos, estes, com privilégios controlados e mensurados.

Neste cenário, para o servidor contemplado, criamos um usuário administrativo com poderes consideráveis, e fizemos uma relação de confiança por chave pública/privada a partir de um outro servidor confiável. Isso permite administração fácil e centralizada, a partir de um usuário base com poderes de reverter possíveis problemas com o super-usuário. Veja os passos executados, contemplando criação do usuário, chaves e propagação entre servidores de "administração".

```
1. Criar usuario GSLU & set passwd
# useradd -g users -d /home/gslu -c "Grupo
Seguranca Logica Usuarios" -m gslu
# su - gslu && passwd

2. Gerar PKI
# su - gslu && ssh-keygen -t rsa -b 2048

3. Criar relacao confianca gslu de Master Server
-> Admin Server

################################################
########
# Created By :  JWP                    #
#  Date           :    05/10/2007.  Last  update:
01/11/2007   #
# Function   :  Transfer Public-Key Current User
#
################################################
########
{
if [ -z "$1" ]
then
   echo  "\n  =====  You  need  provide  user@host
info! ====\n"
fi
cd $HOME
if [ -e "./.ssh/id_rsa.pub" ]
then
   cat  ./.ssh/id_rsa.pub  |ssh  $1  'mkdir  -p  -m
0700 .ssh && cat >> .ssh/authorized_keys'
else
   ssh-keygen -t rsa
   cat  ./.ssh/id_rsa.pub  |ssh  $1  'mkdir  -p  -m
0700 .ssh && cat >> .ssh/authorized_keys'
fi
}
```

A partir deste ponto, o "usuário administrativo" está propagado para o servidor a ser gerenciado.

22. Instalação ESM, Medusa ou Bastille

Uma ferramenta de controle e análise de vulnerabilidades deve ser considerada como parte da instalação. No caso de ambiente *UX*, as opções foram:

- *Symantec ESM* (comercial, excelente e cara);
- *MEDUSA* (distribuição controlada e atualmente descontinuada)
- *Bastille* (gratuíto e possui excelentes controles e atualização)

Escolha uma que melhor adeque as necessidades/orçamento do projeto e conheça ao máximo seus recursos, limitações, pontos forte e fraco. Extraia relatórios e inicie o processo de transformação do ambiente (obtenha um "*base report*", defina políticas de ajuste, prioridades e inicie o trabalho). Essa é a melhor e mais emocionante parte.

23. Segregação history

Este recurso, permite que ações indesejadas sejam sobrepostas por limitações do *history* corrente, e separe acessos de *root* basedo em IDs de sessão. Facilita em muito o processo de identificação de "operações não desejadas" e mais importante, o autor delas.

```
# Cria diretorio para armazenamento
mkdir -m 700 ~root/.histories

# Cria arquivo de inicialização da shell
(sh e sh-posix)
echo          'HISTFILE=~/.histories/hist-
`/usr/bin/date       +%Y%m%d`-$$'       >>
~root/.shrc
echo 'export HISTFILE' >> ~root/.shrc
chmod 600 ~root/.shrc

#Configura arquivo de inicialização da
shell
echo 'ENV=~root/.shrc' >> ~root/.profile
echo 'export ENV' >> ~root/.profile
```

24. Segregação privilégios (`sudo`)

Permite utilizar os recursos do *sudo* para segregar grupos de uso, comandos, e invocação de alguns comandos antes restritos a figura do *root*, a partir de um usuário comum habiltado. O arquivo em anexo, define alguns grupos e respectivos comandos que possuem permissão de execução, servindo como ótimo método de controle por áreas de serviço/atuação.

```
# sudoers file - HP-UX                          (c) 2006
- JWP
# This file MUST be edited with the 'visudo' command
as root.
# See the man page for the details on how to write a
sudoers file.

## Override builtin defaults
Defaults syslog=auth
Defaults logfile=/var/adm/syslog/sudo.log
Defaults !authenticate

## Host alias specification

## User alias specification

## Cmnd alias specification
Cmnd_Alias
DISK=/usr/sbin/ioscan,/usr/sbin/diskinfo,/opt/fcms/bin
/fcmsutil,/sbin/spmgr,/usr/sbin/insf,/usr/sbin/rmsf,/u
sr/sbin/mc,/usr/bin/mt,/usr/bin/du,/usr/bin/lifcp,/usr
/s
bin/mkboot
Cmnd_Alias
STORAGE_VA=/opt/sanmgr/commandview/client/sbin/*,/opt/
sanmgr/commandview/server/sbin/*,/sbin/autopath
Cmnd_Alias
Cmnd_Alias
LVM_PLUS=/usr/sbin/lvreduce,/usr/sbin/lvremove,/usr/sb
in/lvrmboot,/usr/sbin/pvremove,/usr/sbin/pvcreate   -f
*,/usr/sbin/vgcfgrestore,/usr/sbin/vgchgid,/usr/sbin/v
gex
port,/usr/sbin/vgreduce,/usr/sbin/vgremove,/usr/sbin/v
gscan,/usr/sbin/pvchange,/usr/sbin/mknod
Cmnd_Alias
FILESYSTEM=/usr/sbin/fsck,/usr/sbin/extendfs,/usr/sbin
/fsadm,/usr/sbin/bfs,/usr/sbin/cachefsstat,/usr/sbin/d
umpfs,/usr/bin/nfsstat,/usr/sbin/mount,/usr/sbin/umoun
t,
```

```
/usr/sbin/pfs_exportfs,/usr/sbin/pfs_mount,/usr/sbin/p
fs_mountd,/usr/sbin/pfs_umount,/usr/sbin/pfsd
Cmnd_Alias
FILESYSTEM_PLUS=/usr/sbin/newfs,/usr/sbin/mkfs,/usr/sb
in/fuser
Cmnd_Alias
NETWORK=/usr/sbin/ifconfig,/usr/sbin/arp,/usr/sbin/rou
te,/usr/bin/rad,/usr/bin/netstat,/usr/sbin/ping
Cmnd_Alias    FILEVIEW=/usr/bin/cat,/usr/bin/crontab -
l,/usr/bin/strings
Cmnd_Alias
SHUTDOWN=/sbin/init,/usr/sbin/reboot,/usr/sbin/shutdow
n
Cmnd_Alias    SWAP=/usr/sbin/swapon,/usr/sbin/swapinfo
Cmnd_Alias
PROCESS=/usr/bin/kill,/sbin/init.d/*,/usr/sbin/kmtune,
/sbin/set_parms,/usr/bin/adb,/usr/sbin/dmesg
Cmnd_Alias    NFS=/usr/sbin/exportfs
...
# User privilege specification
root        ALL=ALL
%temproot ALL=/usr/bin/su - root
%l2sec
ALL=DISK,LVM,LVM_PLUS,FILESYSTEM,FILESYSTEM_PLUS,NETWO
RK,SW,USERS,FILEVIEW,SHUTDOWN,SWAP,PROCESS,NFS,OPENVIE
W,/usr/bin/setacl,/usr/bin/su - root
%l2ux
ALL=STORAGE_VA,DISK,LVM,LVM_PLUS,FILESYSTEM,FILESYSTEM
_PLUS,NETWORK,SW,USERS,FILEVIEW,SHUTDOWN,SWAP,PROCESS,
NFS,OPENVIEW,MCSG
%l2sap
ALL=DISK,LVM,!LVM_PLUS,!FILESYSTEM,!FILESYSTEM_PLUS,!N
ETWORK,SW,!USERS,FILEVIEW,SHUTDOWN,!SWAP,PROCESS,NFS,!
OPENVIEW,ORA1,SAP1
%l2db
ALL=DISK,LVM,!LVM_PLUS,!FILESYSTEM,!FILESYSTEM_PLUS,!N
ETWORK,SW,!USERS,FILEVIEW,SHUTDOWN,!SWAP,PROCESS,NFS,!
OPENVIEW,ORA1,SAP1
ALL=DISK,!LVM,!LVM_PLUS,!FILESYSTEM,!FILESYSTEM_PLUS,!
NETWORK,SW,!USERS,FILEVIEW,SHUTDOWN,!SWAP,PROCESS,NFS,
!OPENVIEW,OMNIBACK,MCSG
%l1sapux
ALL=DISK,LVM,!LVM_PLUS,FILESYSTEM,!FILESYSTEM_PLUS,NET
WORK,!SW,USERS,FILEVIEW,SHUTDOWN,!SWAP,PROCESS,NFS,OPE
NVIEW,MCSG,ORA1,SAP1
%l2tools
ALL=DISK,LVM,!LVM_PLUS,FILESYSTEM,!FILESYSTEM_PLUS,NET
WORK,SW,USERS,FILEVIEW,SHUTDOWN,!SWAP,PROCESS,NFS,OPEN
VIEW,/usr/sbin/cmviewcl

# GSLU specific permissions
gslu
ALL=NOPASSWD:/usr/sbin/useradd,NOPASSWD:/usr/sbin/user
del,NOPASSWD:/usr/sbin/usermod,NOPASSWD:/usr/sbin/grou
padd,NOPASSWD:/usr/sbin/groupdel,NOPASSWD:/usr/sbin/gr
oupmod,NOPASSWD:/home/gslu/add_key.sh,NOPASSWD:/usr/bi
n/passwd,NOPASSWD:/usr/bin/cat
```

IV. Status Checklist

O *checklist* inicial apresentado (2 – Escopo de Atuação), serve de referência para que o administrador possa ter uma padrão de controles previamente definidos. Utilize-o ou crie o seu próprio *checklist*, e uso-o como acompanhamento durante a fase de implantação. No final, compare os resultado obtidos, identifique alguns *issues* que possam persister, e retorne ao plano de ação em busca de seus objetivos finais. Mantenha-o sempre atualizado como documentação de seu projeto e possível fonte de evidências caso alguém, um dia, possa requisitá-lo.

V. Conclusão

Manter um ambiente seguro não é atividades das mais triviais. Um projeto baseado em PDCA (*Plan, Do, Check e Act*), deve ser considerado, pois sem este sistema circular de validações, seu ambiente estará coerente por algumas semanas (pra não dizer dias). Considere processos de automatização para facilitar tarefas repetitivas, e prefira ferramental que possa ser integrado.

Uma política de segurança do ambiente deve existir para nortear as atividades e prioridades de sua implementação, além de servir de base para quaisquer questionamentos sobre o assunto. Garantir um nível adequado de CID/CIA em épocas onde o processo de comunicação aumenta exponencialmente, aliado a complexidade e heterogeneidade dos ambientes é algo extremamente difícil. Como profetizava Andy Grove, "*Only the paranoid survive*."

VI. References

HP-UX Reference
http://docs.hp.com/en/B2355-60103/

HP-UX Security Guide
http://www.sabernet.net/papers/hp-ux10.html

Porting and Archive Centre For HP-UX
http://hpux.cs.utah.edu/

Rosetta Stone for Unix
http://bhami.com/rosetta.html

Technical Tips
http://pete.gulotta.name/Technical%20Tips.htm#_Toc159153860

IT Resource Center – Patch Database
http://www1.itrc.hp.com

Jairo Willian Pereira é especialista em Redes de Computadores pela Universidade Estadual de Compinas (Unicamp)e especialista em Segurança pela Veris Educacional (IBTA/Ibmec), onde atualmente leciona disciplina com foco em Seguranca da Informação e Normatização Internacional. Atualmente, trabalha na *Hewlett Packard* como Consultor em *Outsourcing*, divisão de *Audit & Compliance Security* para América Latina e Caribe. Certificado ITIL, CompTIA Security+, e Network+, Módulo MCSO, Linux Professional Institute (Level-1) e *Microsoft* MCSA & MCSE (*Microsoft Certified System Administrator & Engineer*). Possui larga experiência em "*hardening*" em diversas plataformas, aplicações e sistemas operacionais. É também autor de um livro sobre "*Desktop Publishing*" e um dos criadores do projeto fortune-mod-isec.