Universidade Tuiuti do Paraná Ciência da Computação



Hardening

Conteúdo programático

- O que é Hardening?
- Dicas iniciais
- Opções de Sistemas de Arquivos
- Usuário root
- Atualizações
- Verificando serviços de rede
- Conhecer o funcionamento do sistema
- Limitando uso do sistema
- Ferramentas de controle de vulnerabilidades

"Hardening" é um processo de mapeamento das ameaças, avaliação dos riscos e execução de atividades corretivas, com foco na infra-estrutura e o objetivo principal é torná-la preparada para enfrentar tentativas de ataque.

É uma espécie de tunning no sistema para encontrar e prevenir vulnerabilidades.

Estou pronto para colocar meu servidor em produção?

Dicas iniciais:

- ✓ Remover/Desabilitar logins de usuários que não estejam em uso;
- ✓ Limitar os pacotes instalados aqueles que se destina à função desejada do sistema (# dpkg -I);
- ✓ Desabilitar serviços desnecessários (# chkconfig --list);
- Desabilitando "ctrl+alt+del";
- ✓ Aplicar e manter os "patches" atualizados, tanto de S.O. quanto de aplicações;
- Revisar e modificar as permissões dos sistemas de arquivos;
- Impôr uma política de senhas fortes, testar com john;
- ✓ Verificar as conexões ativas e portas em estado de LISTEN;

Opções de Sistemas de Arquivos

- ✓ exec, noexec permite ou não a execução de binários no sistema de arquivos;
- ✓ rw monta o sistema em modo leitura e escrita;
- ✓ ro monta o sistema em modo somente leitura;
- ✓ suid, nosuid habilita/desabillita o bit de "set-user-identifier" ou "set-group-identifier"
- ✓ dev, nodev habilita/desabilita a interpretação de dispositivos de blocos especiais em um sistema de arquivos;

Exemplo:

```
/dev/sda3 /home ext3 defaults,noexec,nodev 0 0 /dev/sda7 /tmp ext3 defaults,noexec,nodev 0 0
```

Usuário root

- ✓ Se possível desabilite o login de root, acessando a conta de root somente após o login de usuário autorizado (# su / # sudo su -);
- # vi /pam.d/su
 auth required pam_wheel.so group=admin
- ✓ Utilize senhas fortes para senhas de administrador, com números, caracteres especiais, letras minuúsculas e maiúsculas. Para criação de senhas pode ser usado o programa pwgen (# pwgen -n <tamanho> -y);
- ✔ Habilitar a váriavel de ambiente TMOUT no arquivo /etc/profile, assim o usuário terá sua sessão encerrada por inatividade;
- ✓ Desabilite os teminais em que o root não poderá se logar: # vim /etc/securetty

Atualizações

 O Debian GNU/Linux possui um repositório de atualizações de segurança: http://ftp.br.debian.org/debian-security/

✓ Lista de discussão de notificação de segurança no Debian GNU/Linux: http://lists.debian.org/debian-security-announce/

Verificando serviços de rede

Conhecendo o funcionamento do sistema

```
# uname -r # cat /proc/version
# cat /proc/cpuinfo # free # df -h # Ispci # Isusb
# cat /etc/fstab # cat /proc/mounts # cat /proc/partitions
# Ismod
# Idconfig [-p]
# umask
# find / -perm -4000
```

Limitando o uso do sistema

Ativando as biblioteas tally e time para o pam:

```
# vim /etc/pam.d/login
account requisite pam_time.so
auth required pam_tally.so per_user deny=3 lock_time=3
```

O arquivo de confguração do "pam_limits" é o "/etc/security/limits.conf". Dentro dele, as linhas serão confguradas da seguinte forma:

```
<usuario/grupo> <tipo_de_limite> <recurso> <valor_do_limite>
```

Limitando o uso do sistema

Bloqueando a edição das entradas do GRUB:

```
# vim /etc/grub.d/00_header
.....
cat << EOF
set superusers="user1"
password user1 password1
EOF
# update-grub2</pre>
```

Limitando o uso do sistema

Bloqueando a edição das entradas do GRUB com senha criptografada: # grub-mkpasswd-pbkdf2 # vim /etc/grub.d/00 header cat << EOF set superusers="user1" password pbkdf2 user1 grub.pbkdf2.sha512.10000.long number EOF # update-grub2

Ferramentas de controle de vulnerabilidades

Nessus - é um programa de verificação de falhas/vulnerabilidades de segurança. Ele é composto por um cliente e servidor, sendo que o scan propriamente dito é feito pelo servidor. Site: http://www.nessus.org/products/nessus

Cacti - é uma ferramenta administrativa de rede, que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos Site: http://www.cacti.net/



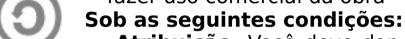
Atribuição-Compartilhamento pela mesma licença 2.5

(http://creativecommons.org/licenses/by-sa/2.5/deed.pt)



Você pode:

- copiar, distribuir, exibir e executar a obra
- criar obras derivadas
- fazer uso comercial da obra



Atribuição. Você deve dar crédito ao autor original, da forma especificada pelo autor ou licenciante.

Compartilhamento pela mesma Licença. Se você alterar, transformar, ou criar outra obra com base nesta, você somente poderá distribuir a obra resultante sob uma licença idêntica a esta.

- Para cada novo uso ou distribuição, você deve deixar claro para outros os termos da licença desta obra.
- Qualquer uma destas condições podem ser renunciadas, desde que Você obtenha permissão do autor.

Qualquer direito de uso legítimo (ou "fair use") concedido por lei, ou qualquer outro direito protegido pela legislação local, não são em hipótese alguma afetados pelo disposto acima.

Este é um sumário para leigos da Licença Jurídica

(na íntegra: http://creativecommons.org/licenses/by-sa/2.5/br/legalcode).

Termo de exoneração de responsabilidade:

http://creativecommons.org/licenses/disclaimer-popup?lang=pt