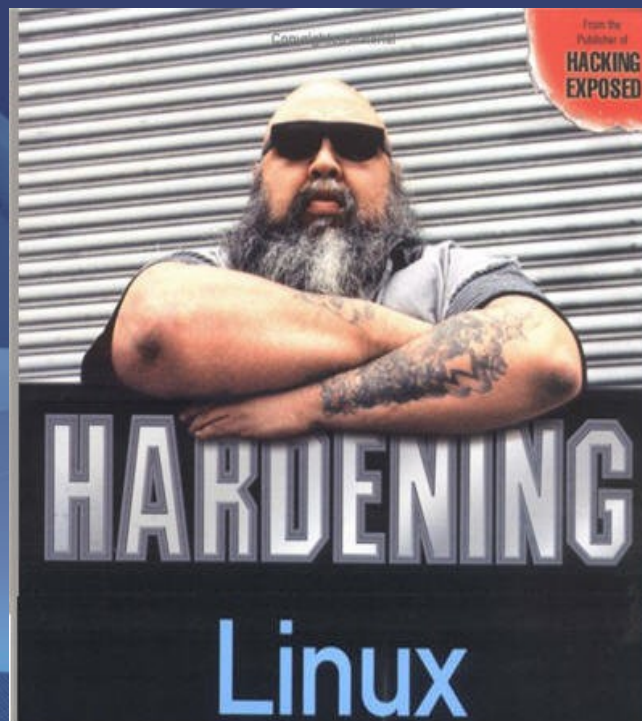


Hardening Linux

Alexandro Silva



Apresentação

- Atua no mercado OpenSource a mais de 10 anos
- Professor da Graduação e Pós-Graduação da Unijorge
- Sysadmin do Projeto Gnome
- Consultor em Segurança da Informação e Tecnologias OpenSource
- Membro oficial do Ubuntu Internacional nas áreas de segurança e documentação

Hardening Linux

- É o processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas - com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

Hardening Linux

- Limitar o software instalado aquele que se destina à função desejada do sistema;
- Aplicar e manter os patches atualizados, tanto de sistema operacional quanto de aplicações;
- Revisar e modificar as permissões dos sistemas de arquivos, em especial no que diz respeito a escrita e execução;
- Reforçar a segurança do login, impondo uma política de senhas fortes.

Hardening Linux

Procedimentos básicos

- Pré-instalação:
 - Planejamento de daemons/serviços;
 - Esquemas de particionamento.
- Pós-Instalação:
 - Proteger o GRUB com senha;
 - Atualizações e Patches;
 - Remover serviços desnecessários;
 - Remover SUID/SGID;
 - Uso do sudo;
 - Bloquear o usuário root.

Hardening Linux

Na prática

- Atualização do sistema:
 - aptitude update && aptitude upgrade

- Protegendo o GRUB

- grub-md5-crypt

Password: **INFORME SENHA <ENTER>**

Retype password: **REPITA SENHA <ENTER>**

- Copie o hash informado

- vim /boot/grub/menu.lst

Hardening Linux

Na prática

- vim /boot/grub/menu.lst

title Debian GNU/Linux, kernel 2.6.26-2-686

root (hd0,1)

kernel /boot/vmlinuz-2.6.26-2-686 root=/dev/hda2 ro quiet

initrd /boot/initrd.img-2.6.26-2-686

password --md5 \$1\$!MM1/\$cB0VonMnHi9fyOxuGp7JB1

Hardening Linux

Na prática

- Habilitar sudo:
 - aptitude install sudo
 - addgroup admin
 - adduser aluno admin
 - vim /etc/sudoers

Hardening Linux

Na prática

- vim /etc/sudoers

Uncomment to allow members of group
sudo to not need a password

(Note that later entries override this, so you
might need to move it further down)

%sudo ALL=NOPASSWD: ALL

%admin ALL=(ALL) ALL

Hardening Linux

Na prática

- Desabilitar o SUID/SGID
 - `find / -perm -4000 > suidfiles.txt`
 - `find / -perm -2000 > sgidfiles.txt`

Hardening Linux

Na prática

- Bloqueando o usuário root:
 - `usermod -L root`
- Para desbloquear:
 - `usermod -U root`

Hardening Linux

Bastille

- O Bastille protege o sistema operacional, configurando o sistema de maneira proativa para aumentar sua segurança e reduzir as chances de comprometimento.

Hardening Linux

Hardening Apache

HANDS ON!!!!

Dúvidas?!?!

Contatos

penguim@ubuntu.com

penguim.wordpress.com