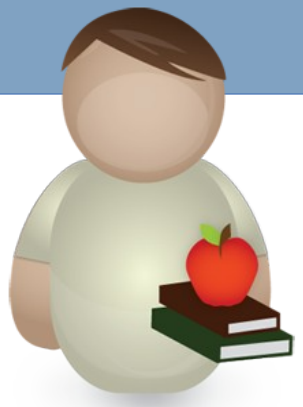

Disciplina:
Segurança de Redes

Professor:
Roitier Campos

Senha de Segurança do Grub

O Boot Loader é o primeiro programa a ser executando quando o computador é ligado. Ele é o responsável por carregar e passar o controle da máquina para o kernel do Sistema Operacional a ser executado.

O Grub (GRand Unified Bootloader) é um boot loader utilizado no linux para gerenciar a carga de um, ou mais, SO's em um mesmo computador.

Proteger a edição do Grub é importante para previnir que intrusos utilizem-o para manipular os sistemas carregados por ele.

Vulnerabilidade do Grub

- Passo 1 – Digite *“e”* quando a tela do GRUB aparecer;
- Passo 2 – Edite a linha que indica como o linux deve ser inicializado, fazendo com o mesmo seja inicializado direto no BASH.
  Encontre a linha: /boot/vmlinux- e digite init=/bin/bash no final desta linha.
- Passo 3 – Retorne a inicialização (sem reinicializar o sistema):
  Tecle Crtl+x
- Passo 4 – Monte a raiz do sistema de forma “genérica”: *mount -o remount /*
- Passo 5 – Altere a senha do usuário que desejar, inclusive o “root”:
- *#passwd “usuário”*
- Passo 6 – Reinicie o servidor: *crtl+alt+del*
- Passo 7 *- Efetue o login com o usuário que foi alterado*

Gerando senha criptografada para o Grub

1. **Gere a senha;**

   # grub-mkpassword-pbkdf2
   your PBKDF2 is grub.pbkdf2.....

2. **Edite o arquivo /etc/grub/00_header colocando a string a seguir no fim do arquivo:**

   cat << EOF

   set superusers=**root (crie um usuário. Não é necessário estar cadastrado no SO)**

   password_pbkdf2 **root** "**grub.pbkdf2.....**"

   EOF

3. **Atualize o grub**

   # update-grub

Restringindo o uso do console

Os tty's são terminais virtuais que podem ser acessados pelos usuários do sistema, através dos quais os usuários podem disparar comandos no sistema.

Definir a forma como o ***root*** vai acessar esses terminais pode ser determinante para o controle e segurança do sistema.

Uma maneira importante de determinar essa restrição é fazer com que o root só consiga logar no sistema à partir do login de um usuário comun.

Restringindo o uso do console

Restringir o usuário root a acessar o terminal apenas quando o usuário já tiver logado como usuário comum evita que um invasor, de posse da senha “root” possa fazer o login na máquina. Isso permite também identificar de qual usuário partiu o login como root.

- Edite o arquivo **/etc/securetty** removendo todas a linhas que contenham as palavras “vc“ e “tty“.

OBS: Isso impede que scripts seja executados como root sem que haja interação de um usuário comum.

Nota: Mesmo estando logado como usuário comum, será requisitada a senha do usuário root.

Desativando a reinicialização do sistema

Um problema comum em maquinas Debian é a possibilidade de reiniciar o sistema utilizando as teclas CTRL+ALT+DEL.

Eliminar essa função minimiza a possibilidade de uma intruso, com acesso fisico à máquina, reiniciar o sistema, mesmo sem ter a senha do root.

Edite o arquivo /etc/inittab, comentando a linha a seguir:

 # ca:12345:crtlaltdel:/sbin/shutdown -t1 -a -r now

Agendamento de tarefas

O crontab, é um programa do Unix que edita o arquivo onde são especificados os comandos a serem executados e a hora e dia de execução pelo cron, um programa que executa comandos agendados nos sistemas operacionais do tipo Unix (como o Linux ou o MINIX, por exemplo).

O cron se encarregará de verificar a hora e determinar se existe ou não algum programa a ser rodado. Caso exista ele o rodará na hora e data solicitada

Crontab

Para a maioria das tarefas pouco importa a hora que vai ocorrer mas sim a frequência em que ela vai ser executada, como diariamente ou semanalmente. Para isso já existe 4 diretórios especiais, que basta o administrador botar o script lá dentro, eles já serão executados na periodicidade desejada.

- /etc/cron.daily ---- agendamentos diários
- /etc/cron.hourly ----agendamentos a cada hora
- /etc/cron.monthly ---- agendamentos mensais
- /etc/cron.weekly ---- agendamentos semanais

Agendamento específico

Mas caso você mesmo queira fazer um periodo especifico, com hora e tudo mais, basta editar o arquivo /etc/crontab:

```
# m h dom mon dow user command
17* * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

/etc/contrab

A cada espaço, se avança um campo e os campos seguem o padrão a seguir:

minuto hora diadomês mês diadasemana usuário comando

m h dom mon dow user command

17 * * * * root cd / && run-parts --report /etc/cron.hourly

Observações

Cada campo pode receber valores segundo a tabela a seguir:

Caractere	Exemplo	Siginificado
Hífen	2-4	intervalo de 2 a 4
Virgula	2,4,6,8	os numeros 2, 4, 6 e 8
Barra	*/10	de dez em dez
asterisco	*	todas as opções possíveis

Obs: O campo Mês recebe valores de 1 a 12 e o campo Semana recebe valores de 0 a 7, onde zero é domingo, 1 é segunda-feira, 2 terça-feira e assim por diante.

Atividade Complementar

Simule agendamentos de tarefas semanais, mensais, diárias, etc:

1) backup semana;

2) Cópia do arquivo /var/log a cada 10 minutos;

3) Use sua imaginação e exercite

sugestão: crie scripts e coloque nos agendamentos.