

Laboratório de Redes de Computadores e Sistemas Operacionais

Poderees da Conta Root

Fabricio Breve

Introdução

- Todo processo e arquivo em um sistema Linux pertence a uma conta de usuário em particular
- Os demais usuários não podem acessar essa conta sem permissão do proprietário
- Os arquivos e processos de sistema pertencem a um usuário chamado “root”
- O que pertence a root não pode ser acessado por outros usuários

Introdução

- A conta root também é usada para fazer alterações administrativas
- Propriedades “mágicas” do root:
 - Pode atuar como proprietário de qualquer arquivo ou processo
 - Pode executar operações especiais que usuários comuns não podem
 - Muito poderosa, e muito perigosa em mãos erradas

Propriedade de Arquivos e Processos

- Todo arquivo possui um proprietário e um “proprietário de grupo”
 - Capacidade de modificar as permissões do arquivo
 - O arquivo tem apenas um proprietário, mas pode ter vários “proprietários de grupo”, que são usuários pertencentes a um mesmo grupo Linux (/etc/group)

Verificando propriedade de um arquivo

- ls -l

```
[fbreve@localhost ~]$ ls -l
total 16
drwxr-xr-x  2 fbreve fbreve 4096 Ago  3 03:36 Desktop
-rw-rw-r--  1 fbreve fbreve  15 Ago 16 12:21 fabricio.txt
[fbreve@localhost ~]$ _
```

Propriedade de Arquivos e Processos

- O Linux internamente utiliza números em vez de nomes:
 - UID (User Identification Numbers)
 - GID (Group Identification Numbers)
- Os nomes ficam armazenados em:
 - /etc/passwd
 - /etc/group

Propriedade de Arquivos e Processos

- Os processos tem quatro identidades associadas a eles:
 - UID real e efetivo
 - GID real e efetivo
- Normalmente real e efetivo são os mesmos
- O efetivo é usado em alguns comandos, como passwd

O Superusuário

- O root tem UID igual a 0
- Apesar de possível nunca:
 - Troque o nome do usuário root
 - Crie outros usuários com UID igual a 0
 - Tais práticas podem causar brechas de segurança além de modificar o padrão

Operações restritas do root

- Criar arquivos de dispositivos
- Configurar o relógio do sistema
- Aumentar os limites de uso de recursos e as propriedades de processos
- Definir o nome de host do sistema
- Configurar interfaces de rede
- Abrir portas de rede privilegiadas (números menores que 1024)
- Desligar o sistema

Operações restritas do root

- Modificar seu próprio UID e GID
 - O processo de login é executado como root, e ao validar o usuário modifica o UID e GID para os desse usuário e inicia seu ambiente de trabalho

Selecionando uma senha root

- Utilize no mínimo 8 caracteres
- Estratégia: Invente uma frase absurda e pegue a primeira letra de cada palavra
- Incluir números, sinais de pontuação e letras maiúsculas aumenta a segurança da senha

Trocando a senha root

- passwd
- Troque a senha:
 - Pelo menos a cada 3 meses
 - Cada vez que alguém que conhece a senha saia da empresa
 - Sempre que achar que a segurança possa ter sido comprometida
 - Um dia em que você não esteja planejando se divertir até altas horas da noite e ter esquecido a senha na manhã seguinte

Tornando-se root

- É possível desabilitar a conta root, isso em alguns casos é vantajoso pois:
 - A conta root não tem registro de quem a usou
 - A conta root não registra log do que foi feito
- Nesses casos a conta root pode ser acessada com:
 - su
 - sudo

SU

- Se digitado sem parametros solicita senha de root, e o usuário terá os privilégios de root até encerrar com exit
- Registra log de quem entrou como root
- Pode ser usado para entrar na conta de outro usuário (digitando sua senha)
- O root pode entrar na conta de outros usuários sem digitar senha
- Para aumentar a segurança, utilize o caminho completo `/bin/su`

sudo

- Util para dar a usuários permissão para executar apenas determinadas tarefas de administrador (como fazer um backup por exemplo)
- sudo consulta o arquivo `/etc/sudoers`, que lista as pessoas autorizadas a usar sudo e os comandos que elas podem usar, se encontrar a autorização sudo pede a senha do próprio usuário, que passa a ter privilégio de root para os comandos estabelecidos por um período de tempo pré-configurado

Vantagens do sudo

- Logging dos comandos
- Operadores podem realizar tarefas sem necessidade de privilégios de root ilimitados
- A verdadeira senha pode ser conhecida por apenas uma ou duas pessoas
- É mais rápido usar sudo que su ou logar como root
- Podem ser revogados privilégios sem a necessidade de mudar a senha root
- Há menos chances de um shell root ficar abandonado

Desvantagem do sudo

- Qualquer brecha em uma conta pessoal de um usuário sudoer pode ser equivalente a uma brecha em uma conta root

Referências Bibliográficas

- NEMETH, Evi.; HEIN, Trent R.; SNYDER, Garth. *Manual Completo do Linux: Guia do Administrador*. Makron Books, 2004.