Sistemas Operacionais

Teoria e prática

Usuários no Linux

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Sistema Multiusuários

- Sistemas multiusuários permitem o acesso de múltiplos usuários inclusive concorrentes;
- São sistemas preparados para prover segregação e segurança de recursos;
- Unix e seus sucessores são multiusuários;
- Acessa-se por terminal ou remotamente por Telnet ou SSH;

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuários

- Todo usuário no Linux possui um identificador único chamado UID;
- Além do UID sua representação textual ”nome” é único no sistema;
- O UID está entre 0 e INT_MAX;

ATENÇÃO: UID é único mas pode-se fazer sobreposição.

ATENÇÃO: Leiam sobre a vulnerabilidade: CVE-2018-19788

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuários

- Todos os processos e arquivos pertencem a uma conta de usuário;
- Tudo requer permissão de acesso;
- O controle de permissão de acesso do usuário bem como a organização do sistema de arquivos trazem a segurança e estabilidade do sistema.

Usuários

- Existem 3 tipos de usuários no sistema:
  - Usuário comum: onde ficamos a maior parte do tempo;
  - Usuário de administração: conta de usuário que permite a manutenção do sistema;
  - Usuário de sistema: contas que não permite log-on por interface;

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuário de Administração

- Também chamado de superusuário ou root;
- É um usuário fictício;
- O UID do usuário root é 0 (zero);
- Não se mexe em características desta conta, mesmo sendo posssível;
- Um usuário com UID 0 (root) pode executar qualquer operação e até manipular qualquer arquivo;

Usuário de Administração

- Operações Kernel podem ser executadas por este:
  - Modificar diretório raiz chroot;
  - Criar arquivos de E/S;
  - Configurar o relógio do sistema;
  - Aumentar recurso e prioridades de processos;
  - Configurar interfaces e periféricos;
  - Abrir portas na camada de transporte do modelo OSI;
  - Desligar/Reiniciar sistema;

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuário de Administração

```
File  Edit  View  Search  Terminal  Help
  GNU nano 4.8                          /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

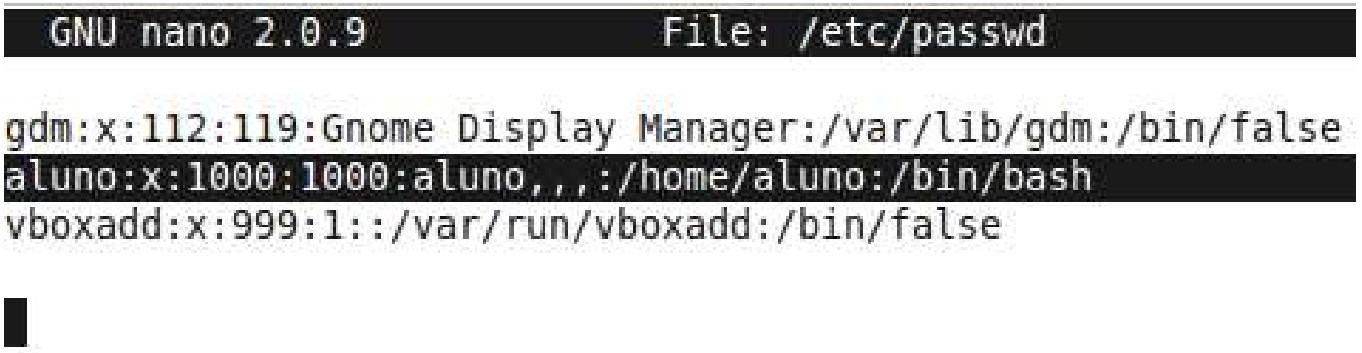
```
  GNU nano 2.0.9                File: /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuário Comum

- Um usuário criado no processo de instalação (UID 1000) ou após a instalação por meio de comandos;
- Possui permissão para entrar no sistema seja por Telnet, SSH ou por interface gráfica;
- É a conta de qualquer expert Unix;



Usuário Sistema

- Todo processo ou arquivo precisa de um Usuário para existir, mesmo que tenha sido criado por outro;
- Usuários de sistema não entram por Telnet, SSH e muito menos por interface;
- Garantimos a segurança dos sistemas que provem serviços de rede assim;

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Usuário Sistema

- www-data é o usuário que os servidores da web no Ubuntu (Apache, nginx, por exemplo) utilizam para executar tais serviços;
- Possuem um diretório padrão, no caso abaixo /var/www

```
  GNU nano 2.0.9                File: /etc/passwd

news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Comando su

- O comando su do Unix é usado para acessar a conta de outro usuário no shell sem encerrar a sessão do usuário atual;
- É uma forma abreviada de se referir a substitute user (substituir usuário);
- Em geral é usado para assumir o usuário root quando privilégios administrativos são necessários e deixá-los tão brevemente quando não forem mais.

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Arquivo /etc/passwd

- O arquivo /etc/passwd é um arquivo de texto com um registro por linha;
- Cada linha descrevendo uma conta de usuário;

```
  GNU nano 2.0.9                File: /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Arquivo /etc/passwd

1. Login do usuário, isto é, a palavra que um usuário digita quando está logando no sistema operacional;
2. informação utilizada para validar a senha de um usuário; Colocar neste campo um asterisco "*" é a maneira típica de desabilitar uma conta para evitar que seja utilizada.

Arquivo /etc/passwd

3. identificador de usuário, o número que o sistema operacional utiliza para propósitos internos;
4. identificador do grupo. Este número identifica o grupo primário do usuário; todos os arquivos que forem criados por este usuário pertencerão inicialmente a este

Arquivo /etc/passwd

5. chamado campo Gecos, é um comentário que descreve a pessoa ou a conta. Tipicamente, é um conjunto de valores separados por vírgulas
6. diretório home do usuário.
7. o programa de shell que será iniciado toda vez que o usuário logar no sistema.

/bin/sync e /bin/false

- /bin/false e /bin/sync são apenas binários que saem imediatamente, retornando false, quando é chamado;

```
aluno@aluno-desktop:~$ file /bin/sync
/bin/sync: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically
 linked (uses shared libs), for GNU/Linux 2.6.15, stripped
aluno@aluno-desktop:~$
```

```
aluno@aluno-desktop:~$ file /bin/false
/bin/false: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamicall
y linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

```
aluno@aluno-desktop:~$ /bin/false
aluno@aluno-desktop:~$
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

/sbin/nologin

- Quando /sbin/nologin é definido como o shell, se o usuário com esse shell efetuar login, eles receberão uma mensagem educada dizendo que o usuário não pode efetuar log-in.

```
kimjong@kimjong:~$ file /usr/sbin/nologin
/usr/sbin/nologin: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynam
ically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=c1bf7b828e
58663d9e714d8e1038c64c3e6746a5, for GNU/Linux 3.2.0, stripped
```

```
kimjong@kimjong:~$ /usr/sbin/nologin
This account is currently not available.
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

/etc/shadow

- Segundo arquivo que devemos conhecer que possui dados de conta de usuário;
- Dados desmembrados para dar liberdade para visualização do arquivo /etc/passwd

```
-rw-r----- 1 root shadow 1007 2012-09-19 16:30 /etc/shadow
aluno@aluno-desktop:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 1612 2012-09-19 16:30 /etc/passwd
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

/etc/shadow

```
aluno@aluno-desktop:~$ sudo cat /etc/shadow
[sudo] password for aluno:
root:!:15602:0:99999:7:::
daemon:*:14545:0:99999:7:::
bin:*:14545:0:99999:7:::
sys:*:14545:0:99999:7:::
sync:*:14545:0:99999:7:::
games:*:14545:0:99999:7:::
kernoops:*:14545:0:99999:7:::
saned:*:14545:0:99999:7:::
pulse:*:14545:0:99999:7:::
gdm:*:14545:0:99999:7:::
aluno:$6$K7tSMF9g$1W2rnwrb8RLTEcEf.qebO5Hj5OMPqwmIq9F4tZBkQ0e
xXwJFSHbSur85uOS/Gj7u.v/:15602:0:99999:7:::
vboxadd:!:15602::::::
```

/etc/shadow

1. O login do usuário;
2. Senha, pode ter
    1. uma senha criptografada,
    2. * para não possui senha e nunca teve e não pode logar
    3. ! para não possui senha;
3. Ultima mudança de senha (dias após 1/1/1970);

/etc/shadow

4. Dias para que a senha possa ser alterada;
5. Dias antes de me obrigar a trocar a senha (-1 ou 9999 está desabilitado);
6. Número de dias do aviso antes de ser obrigado a trocar a senha;
7. Dias entre expiração e desativação;
8. Data de expiração, data em que a conta será desabilitada (em numero de dias);

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Comando sudo

- O usuário root é singular, permitir que outras pessoas entrem por su pode ser permissivo de mais;
- O comando sudo é um escopo limitado para se executar operações de root;
- Sudo utiliza os argumentos de linha de comando para executar operações como se fosse o próprio root;

```
aluno@aluno-desktop:~$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Comando sudo

- Sudo consulta um arquivo /etc/sudoers que lista as pessoas que estão autorizadas a utilizar e qual o grau de permissão para isso;
- É possível utilizar para rodar um determinado comando como se fosse outra pessoa que não seja o root

```
aluno@aluno-desktop:~$ sudo -u professor cat /etc/passwd
```

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Comando sudo

- Podemos listar as permissões do usuário atual utilizando o parâmetro -l conforme exemplo

```
aluno@aluno-desktop:~$ sudo -l
Matching Defaults entries for aluno on this host:
    env_reset

User aluno may run the following commands on this host:
    (ALL) ALL
aluno@aluno-desktop:~$
```

Instalação do sudo

- Antes da instalação execute: apt update;
- Instale usando o comando: apt install sudo;
- Configure as permissões dos usuários em sudoers, utilize visudo.

Prof. Wellington Pinto de Oliveira
http://lattes.cnpq.br/1473011256195357

Comando visudo

```
  GNU nano 2.0.9                File: /etc/sudoers.tmp

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# 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

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

Regra em sudoers

- root ALL = (ALL: ALL) ALL - Isso se aplica ao usuário root
- root ALL = (ALL: ALL) ALL - Esta regra se aplica a todos os usuários root conectados a partir de todos os hosts
- root ALL = (ALL : ALL) ALL - o usuário root pode executar comandos como todos os usuários
- root ALL = (ALL: ALL) ALL - o usuário root pode executar comandos como todos os grupos
- root ALL = (ALL: ALL) ALL - Essas regras se aplicam a todos os comandos

Referência

- Manual Completo do Linux / Evi Nemeth; Garth Snyder; Trent R. Hein; com Adam Boggs, Matt Crosby e Ned McClain; São Paulo : Pearson Prentice Hall, 2007;