CRIPTOGRAFIA

Agenda

- Criando usuários e grupos
- Gerenciando permissões e privilégios

USUÁRIOS E GRUPOS

- Usuário: possui uma identificação no sistema, um nome e um número.
- Composição de um usuário

  Login, password, UID (User IDentification), GID (Group Identification), /home, comentário, shell.
- Grupo: conjunto de usuários.
- Composição de um grupo

  Nome do grupo, Password, GID (Group IDentification), Lista de usuários que compõe o grupo.

GERENCIANDO USUÁRIOS E GRUPOS

Arquivos e diretório de configuração

Arquivo /etc/passwd

- Sintaxe do arquivo:
  - ✓ <usuário>: <senha criptografada>: <UID>: <GID>: <comentário>: <home>: <shell>:
  - ✓ hugo:x:1001:100:Hugo:/home/hugo:/bin/bash

Arquivo /etc/group

- Sintaxe do arquivo:
  - ✓ <grupo>: <senha criptografada>: <GID>: <comentário>: <lista de usuários>:
  - ✓ geral:x:502:lista:juan,bob,alice

COMANDO DE GERENCIAMENTO DE USUÁRIOS E GRUPOS

useradd ou adduser

- adduser unix
- useradd linux

passwd

- passwd linus

userdel

- userdel –r linus

groupadd

- groupadd laboratorio

groupdel

- groupdel laboratorio

su

- su claudio

sudo

- sudo joao

GERENCIMANETO DE PRIVILÉGIOS

Permissões e privilégios

- O Linux fornece facilidades de proteção de arquivos e diretórios.
- Essas proteções são dividas em 3 classes de privilégios: dono, grupo e outros.
- Cada classe é composta de 3 níveis de permissões: leitura, escrita e execução.

VISUALIZANDO LS -LA

- O comando (ls –la) permite visualizar estes parâmetros quando digitado no terminal Linux.

```
-rw-r--r--   1 maziero  users        4068 mar 26 21:09 02.html
drwx------   5 maziero  users        1024 set  5  1998 Desktop/
drwx------   4 maziero  users        1024 jan 26  1998 administ/
drwxr-xr-x   2 maziero  users        1024 set 13  1998 axhome/
drwx------   2 maziero  users        1024 set  7  1998 bin/
-rw-r-----   1 maziero  users        4956 mar 26 20:34 descricao.html
drwx------  11 maziero  users        1024 jan 14 10:52 diversos/
drwx------   2 maziero  users        1024 jan 26  1998 ensino/
drwx------   2 maziero  users        1024 jan 26  1998 extensao/
drwx------   3 maziero  users        1024 mar  8  1998 formacao/
drwx------   4 maziero  users       13312 fev 23 20:49 icons/
drwx------   2 maziero  users        1024 ago  5  1998 mail/
drwx------   2 maziero  users        1024 jul  3  1998 nsmail/
drwx------   2 maziero  users        1024 out 13 19:22 pesquisa/
drwx------   8 maziero  users        1024 nov 24  1997 public_html/
drwx------  10 maziero  users        1024 mar 25 21:28 raytrace/
drwx------   3 maziero  users        1024 set 28 23:03 sistema/
drwxr-xr-x   3 maziero  users        1024 mar 26 21:07 testes/
drwx------   5 maziero  users        1024 out 17  1997 tex/
-rw-------   1 maziero  users        9718 ago  2  1998 wood.gif
```

VISUALIZANDO LS -LA

Tipos de arquivos:

- - : arquivo normal
- d : diretório
- c : dispositivo (mapeado em /dev/) orientado a caracteres (como modems e portas seriais)
- s : socket mapeado em arquivo (para comunicação entre processos)
- p : FIFO ou *Named Pipe* (outro meio de comunicação entre processos)

Chaves de permissão:

- r : permissão de leitura (*read*).
- w : permissão de escrita (*write*).
- x : permissão de execução (*eXecute*).

Consultando permissões

- -rw-r----- 1 marcos users 4956 mar 26 20:34 descricao.html

CRIANDO UM GRUPO

- O motivo mais comum para criar um grupo é fornecer uma maneira para os usuários compartilhar arquivos. Depois de criar ou modificar um grupo, você pode verificar as mudanças visualizando o arquivo **/etc/group** ou executando o comando **getent**.

COMANDO GROUPADD

O comando **groupadd** cria um novo grupo.
A opção -g pode ser usada para especificar um ID de grupo:

- groupadd -g 506 research

Se a opção **-g** não for fornecida, o comando **groupadd** fornecerá automaticamente um **GID** para o novo grupo.

CONSIDERAÇÕES DA CONTA

Antes de criar uma conta de usuário, considere quais valores você deseja definir:

- Nome do usuário
- UID
- Grupo primário
- Grupo suplementar
- Diretório home
- Estrutura dos Diretórios
- Shell
- Comentários

CONSIDERAÇÕES DA CONTA

O comando **useradd** permitirá que você crie novos usuários. Exemplo:

- useradd -u 1000 -c 'Jane Doe' jane

Modifica os seguintes arquivos:

- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow

Cria o spool de correio (/var/spool/mail/jane) e o diretório inicial do usuário (/home/jane).

CONSIDERAÇÕES DA CONTA

- Para visualizar as propriedades de um arquivo regular, você pode usar o comando **ls -l**:

```
[sysadmin@localhost ~]$ ls -l /etc/named.conf
-rw-r-----. 1 root named 1163 May 13 10:27 /etc/named.conf
```

Usuário dono Dono do grupo

- Para visualizar as propriedades de um arquivo de diretório, você pode usar o comando **ls -ld**:

```
[sysadmin@localhost ~]$ ls -ld /etc/named
drwxr-x---. 2 root named 4096 Mar 28  2013 /etc/named
```

Usuário dono Dono do grupo

DONO DO ARQUIVO

- Todos os arquivos são de propriedade de um usuário e um grupo.
- Se um usuário criar um arquivo, ele será o proprietário desse arquivo.
- O comando **chown** pode alterar a propriedade do usuário de um arquivo, mas ele só pode ser usado pelo usuário **root**.
- Embora a maioria dos comandos mostre o nome da conta do usuário como o proprietário, o sistema operacional está realmente associando o UID desse usuário como proprietário do arquivo.

COMANDO CHOWN

O comando **chown** pode ser usado pelo usuário root para alterar o proprietário do usuário, o proprietário do grupo ou ambos.

Exemplos:

- chown user:group <arquivo|diretório>
- chown user < arquivo|diretório >
- chown :group < arquivo|diretório >

COMANDO CHOWN

chown

- O comando *chown* executado pelo root permite alterar o proprietário ou grupo do arquivo ou diretório, alterando o dono do arquivo ou grupo.

```
ppgia:~> ls -l
drw-------  2 maziero    prof    0    Mar 27    08:51 dir1

ppgia:~> chown joao dir1
ppgia:~> ls -l
drw-------  2 joao       prof    0    Mar 27    08:51 dir1
```

PERMISSÕES

Quando você executa o comando **ls -l**, os dez primeiros caracteres de cada linha estão relacionados ao tipo de arquivo e às permissões:

- O primeiro caractere indica o tipo de arquivo.
- Os caracteres 2-4 são permissões para o proprietário do usuário.
- Os caracteres 5-7 são permissões para o proprietário do grupo.
- Os caracteres 8-10 são permissões para "outros" ou o que às vezes é referido como as permissões do mundo. Este seria todos os usuários que não são o proprietário do arquivo ou um membro do grupo do arquivo.

VISUALIZANDO PERMISSÕES

- [root@localhost ~]# ls -l /etc/passwd

-rw-r--r--. 1 root root 4135 May 27 21:08 /etc/passwd

- Com base na saída de comando acima, os primeiros dez caracteres podem ser descritos na tabela a seguir:

Arquivo	Usuário dono			Dono do grupo			Outros		
Tipo	Read	Write	Execute	Read	Write	Execute	Read	Write	Execute
-	r	w	-	r	w	-	r	-	-

TIPOS DE ARQUIVOS

Caractere	Tipo de arquivo
-	Um arquivo regular que pode estar vazio, contém texto ou dados binários.
d	Um diretório que contém os nomes de outros arquivos e links para eles.
l	Um link simbólico é um nome de arquivo que aponta para outro arquivo.
b	Um arquivo de bloco é aquele que se relaciona com um dispositivo de hardware de bloco em que os dados são lidos em blocos de dados.
c	Um arquivo de caractere é aquele que se relaciona com um hardware em que os dados são lidos um byte de cada vez.
p	Um arquivo de pipe funciona de forma semelhante ao símbolo da tubulação, permitindo que a saída de um processo se comunique com outro processo através do arquivo de tubulação, onde a saída do processo é usada como entrada para o outro processo.
s	Um arquivo socket permite que dois processos se comuniquem, onde ambos os processos podem enviar ou receber dados.

SIGNIFICADO DAS PERMISSÕES

Permissão	Significado no arquivo	Significado no diretório
r	O processo pode ler o conteúdo do arquivo, o que significa que o conteúdo pode ser visto e copiado.	Os nomes dos arquivos no diretório podem ser listados.
w	O arquivo pode ser escrito pelo processo, portanto as mudanças em um arquivo podem ser salvas.	O arquivo pode ser escrito ao processo, portanto, devem ser salvas as mudanças do arquivo.
x	O arquivo pode ser executado ou rodar como um processo.	O usuário pode usar o comando cd para "entrar" no diretório e usar o diretório em um caminho para acessar arquivos e, potencialmente, subdiretórios desse diretório.

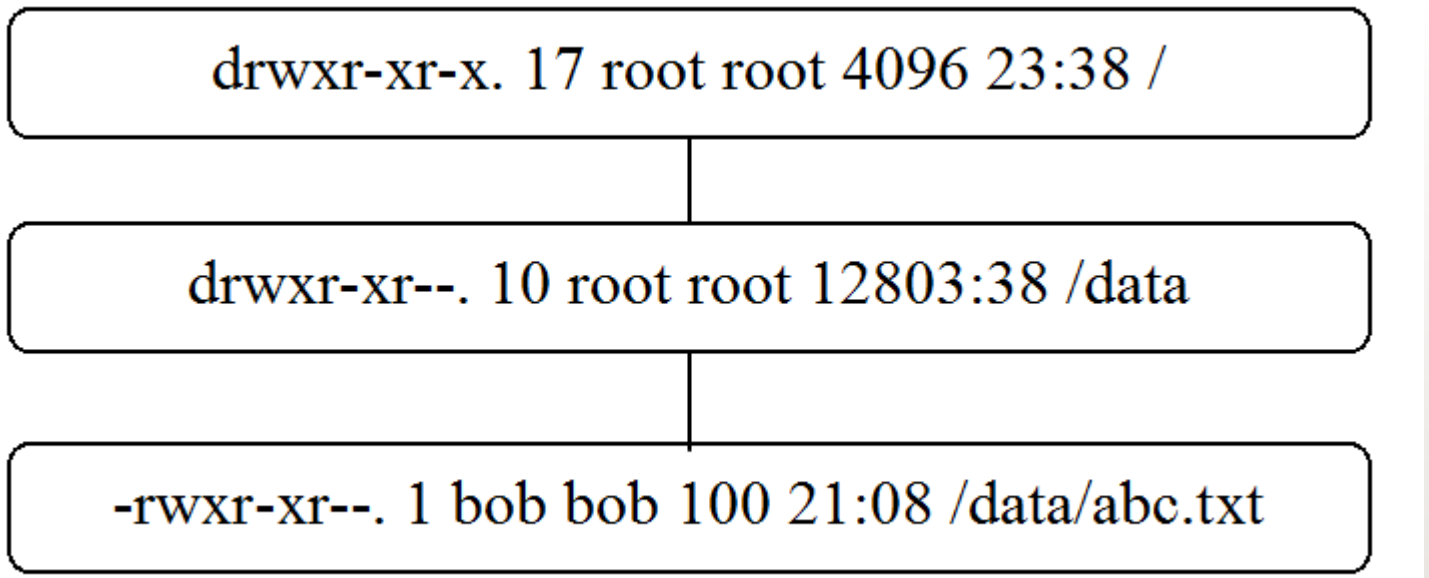
ENTENDENDO AS PERMISSÕES

Apenas um dos três conjuntos de permissões será aplicado quando um usuário tentar algum tipo de acesso em um arquivo:

- Se você é o usuário que possui o arquivo, somente as permissões do proprietário do usuário se aplicam.
- Se você não é o proprietário do usuário, mas é um membro do grupo que possui o arquivo, as permissões do proprietário do grupo se aplicam.
- Se você não é o proprietário do usuário e você não é um membro do grupo que possui o arquivo, as permissões para os "outros" serão aplicadas.

IMPORTÂNCIA DO ACESSO AO DIRETÓRIO

- Pergunta: Qual nível de acesso **bob** tem para **/data/abc.txt**?



- Nenhum, porque sem permissão de execução no **/data**, não há nenhuma maneira para o acesso ao arquivo **/data/abc.txt**.

CHMOD

O comando **chmod** (change mode) é usado para definir ou modificar permissões.
Para alterar as permissões em um arquivo, você deve ser o proprietário ou **root**.
Existem duas técnicas distintas para alterar permissões com **chmod**:

- Simbólico
- numérico

USANDO CHMOD SIMBOLICAMENTE

- Com essa técnica, você especifica quem, um operador, e que:

quem: especifica de quem será alterado:

u para usuário

g para grupo

o para outros

a para todo mundo

operador: especifica se adiciona, remove ou atribui:

+ para adicionar

- para remover

= exatamente

O que: especifica a permissão para ajustar o arquivo:

r para leitura

w para escrita

x para execução

- para nada

EXEMPLOS SIMBÓLICOS COM CHMOD

- **chmod u+x abc.txt** alterará a permissão de execução para o proprietário do usuário.
- **chmod go-rx abc.txt** alterará/removerá a leitura e execução para o proprietário do grupo e outro proprietário.
- **chmod u+wx,g=rx,o-r abc.txt** irá alterar as permissões de gravação e execução para o proprietário do usuário (sem alteração para ler), irá definir **r-x** para o proprietário do grupo e altera/remove a permissão de leitura para "outros".

USANDO O CHMOD NUMERICAMENTE

Ao usar a técnica numérica com **chmod**, um número de três dígitos é usado para representar as permissões do usuário, grupo e outros.
Também é chamado de método octal após os valores octal que são usados para calcular as permissões:

- 4 = ler
- 2 = escrever
- 1 = executar

USANDO O CHMOD NUMERICAMENTE

- Ao combinar as permissões, os valores variam de 0 a 7:
  - 7 = rwx
  - 6 = rw-
  - 5 = r-x
  - 4 = r--
  - 3 = -wx
  - 2 = -w-
  - 1 = --x
  - 0 = ---
- Todas as nove permissões devem ser especificadas ao usar o método octal:
- 777 = rwxrwxrwx
- 775 = rwxrwxr-x
- 755 = rwxr-xr-x
- 700 = rwx------
- 664 = rw-rw-r--
- 640 = rw-r-----

USANDO O CHMOD NUMERICAMENTE

chmod

- As expressões de permissão são substituídas por valores octais representando as permissões desejadas. Assim, para as permissões rwxr-x--- a um arquivo teste.txt, deve-se considerar que rwxr-x--- → 111 101 000 (binário) → 7 5 0 (octal) → 750. Desta forma, o comando a executar é:
  - chmod 750 teste.txt

Permissão	Binário	Decimal
---	000	0
--x	001	1
-w-	010	2
-wx	011	3
r--	100	4
r-x	101	5
rw-	110	6
rwx	111	7

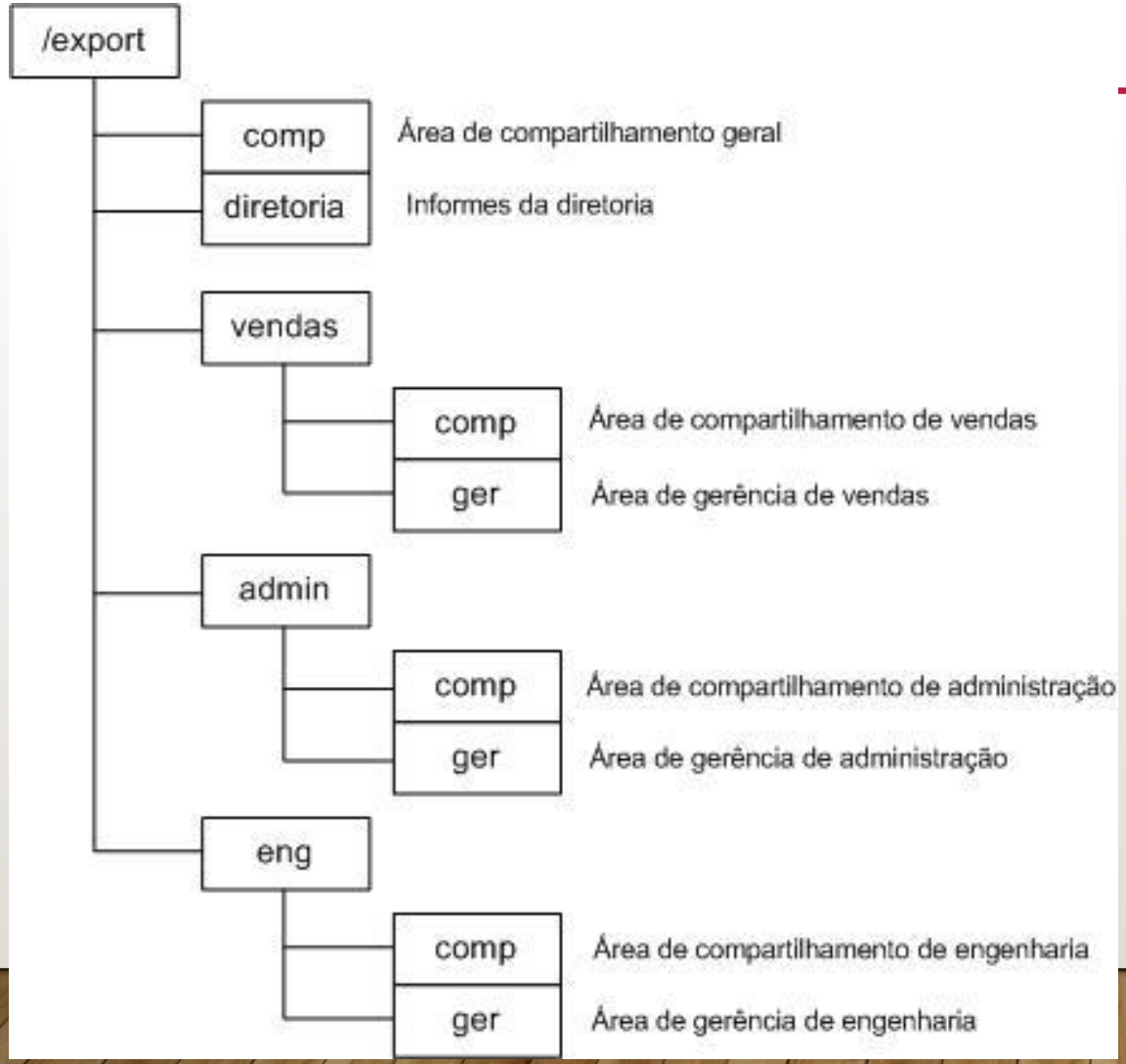
User (owner)			Group			Other		
r	w	x	r	w	x	r	w	x
4	2	1	4	2	1	4	2	1

0 : --- (nenhuma permissão)
1 : --x (somente execução)
2 : -w- (somente escrita)
3 : -wx (escrita e execução)
4 : r-- (somente leitura)
5 : r-x (leitura e execução)
6 : rw- (leitura e escrita)
7 : rwx (leitura, escrita e execução)

USANDO O CHMOD NUMERICAMENTE

- chmod 755 abc.sh - para rwxr-xr-x
- chmod 660 abc.txt - para rw-rw----
- chmod 771 somedir - para rwxrwx--x
- chmod 400 my.txt - para r--------
- chmod 700 userdir - para rwx------

CENÁRIO DE COMPARTILHAMENTO



CENÁRIO DE COMPARTILHAMENTO

Nesse cenário tem-se um único servidor de arquivos sendo compartilhado em 3 departamentos distintos e segmentados.

Para cada funcionário existem 2 pastas de compartilhamento para que todos possam trocar informações entre si:

- Uma pasta de compartilhamento corporativa geral para toda a empresa.
- Uma pasta de compartilhamento para o seu departamento específico.

DIRETÓRIOS

Diretório	Máscara	Grupo
/export/diretoria	750	labredes
/export/comp	770	labredes
/export/vendas	750	vendas
/export/vendas/comp	770	vendas
/export/vendas/ger	750	vendas
/export/admin	750	admin
/export/admin/comp	770	admin
/export/admin/ger	750	admin
/export/eng	750	eng
/export/eng/comp	770	eng
/export/eng/ger	750	eng
/export	750	labredes

CRIANDO DIRETÓRIOS

- mkdir /export
- mkdir /export/diretoria
- mkdir /export/comp
- mkdir /export/vendas
- mkdir /export/vendas/comp
- mkdir /export/vendas/ger
- mkdir /export/admin
- mkdir /export/admin/comp
- mkdir /export/admin/ger
- mkdir /export/eng
- mkdir /export/eng/comp
- mkdir /export/eng/ger

VERIFICANDO A ESTRUTURA CRIADA

- apt-get install tree
- cd /export
- tree

CRIANDO GRUPOS DE USUÁRIOS

- groupadd vendas
- groupadd admin
- groupadd eng
- groupadd labredes
- getent group

USUÁRIOS/GRUPOS

User/grupo	labredes	vendas	admin	eng
user1	X	X – owner		
user11	X	X		
user12	X	X		
user13	X	X		
user2	X		X - owner	
user21	X		X	
user22	X		X	
user23	X		X	
user3	X			X - owner
user31	X			X
user32	X			X
user33	X			X

CRIANDO USUÁRIO E DIRETÓRIO PESSOAL

- mkdir /home/labredes
- useradd –m user1 –g labredes –G vendas –c “Gerente Vendas” –d /home/labredes/user1
- useradd –m user11 –g labredes –G vendas –c “Usuario Vendas” –d /home/labredes/user11
- useradd –m user2 –g labredes –G admin –c “Gerente Administrativo” –d /home/labredes/user2
- useradd –m user21 –g labredes –G admin –c “Usuario Administrativo” –d /home/labredes/user21
- useradd –m user3 –g labredes –G eng –c “Gerente Engenharia” –d /home/labredes/user3
- useradd –m user31 –g labredes –G eng –c “Usuario Engenharia” –d /home/labredes/user31

VISUALIZAR USUÁRIOS E GRUPOS

- getent group
- cat /etc/group
- cat /etc/passwd
- cat /etc/shadow

ATRIBUIR SENHAS AOS USUÁRIOS

- passwd user1 (digitar a senha duas vezes)
- passwd user11
- passwd user2
- passwd user21
- passwd user3
- passwd user31
- cat /etc/shadow

ATRIBUIR DONOS E GRUPOS AOS DIRETÓRIOS

- chown root.labredes /export
- chown root.labredes /export/diretoria
- chown root.labredes /export/comp
- chown root.vendas /export/vendas
- chown root.vendas /export/vendas/comp
- chown user1.vendas /export/vendas/ger
- chown root.admin /export/admin
- chown root.admin /export/admin/comp
- chown user2.admin /export/admin/ger
- chown root.eng /export/eng
- chown root.eng /export/eng/comp
- chown user3.eng /export/eng/ger

ATRIBUIR MÁSCARA AOS DIRETÓRIOS

- chmod 750 /export
- chmod 750 /export/diretoria
- chmod 770 /export/comp
- chmod 750 /export/vendas
- chmod 770 /export/vendas/comp
- chmod 750 /export/vendas/ger
- chmod 750 /export/admin
- chmod 770 /export/admin/comp
- chmod 750 /export/admin/ger
- chmod 750 /export/eng
- chmod 770 /export/eng/comp
- chmod 750 /export/eng/ger

TESTANDO O CENÁRIO DE COMPARTILHAMENTO

Logar com usuário:

- Usar um outro terminal (**CTRL + Alt + F1**): digitar o usuário e senha;/
- Digitar **su –l user1** (no exemplo, é o user1)
  - **cd /export/vendas/comp** (entrar no diretório com a permissão para ler e escrever), tentar entrar em outros diretórios em que não possui permissão de acesso)
  - **touch arquivo1.txt**

BIBLIOGRAFIA

- FILHO, João Eriberto Mota. Descobrindo o Linux: entenda o sistema operacional GNU/Linux. 3. ed. rev. e ampl. São Paulo: Novatec, 2013. 924 p. ISBN 9788575222782.
- USERADD. <https://www.cheatography.com/tag/useradd>. Acesso em 29.09.2024.
- USER MANAGEMENT. <https://www.patchesoft.com/linux-command-cheatsheet-user-management>. Acesso em 29.09.2024.
- Notas de aula.