MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico de Cibersegurança		
UFCD:	Instalar e configurar ferramentas de análise e recolha de logs e evidências	CÓDIGO UFCD:	UC01485
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Instalação e configuração de Sistemas operativos para os trabalhos práticos de cibersegurança

Alguns comandos básicos

A tabela seguinte procura ilustrar o significado (função) atribuído a alguns dos comandos mais utilizados numa Shell de um sistema operativo Linux. Note que no âmbito deste sistema operativo o uso de letras maiúsculas e minúsculas é distinto ("case sensitive").

Designação	Função
`cat`	Concatenar e listar para a consola (`stdout`) o conteúdo de ficheiro(s) de texto (`cat textoX.txt textoY.txt`)
`cd`	altera o diretório atual para o especificado (`cd /home, cd .., cd /`)
`clear`	limpa a consola
`cp`	copiar ficheiros (`cp /home/deapc/source_file /home/deapc/temp/dest_file`)
`date`	imprimir a data e a hora do sistema
`df`	imprimir a ocupação do espaço em disco dos diversos sistemas de ficheiros
`gcc`	compilador da Linguagem C (`gcc -o <nome do ficheiro executável> <nome do ficheiro C>` ou `gcc <nome do ficheiro C>`)
`grep`	imprimir as ocorrências de uma sequência de caracteres ("string") no conjunto de ficheiros apontado (`grep "Linux is cool" *.txt`)
`gzip/gunzip`	comprimir/descomprimir ficheiros
`ls`	listar o conteúdo de um diretório (`ls -la` lista a totalidade, opção `a`, incluindo ficheiros "escondidos", do conteúdo do diretório atual usando o formato longo, opção `l`)

man	obter as páginas de manual sobre um determinado comando/programa
mkdir	criar um novo diretório (`mkdir mydir`)
more	listar para consola (`stdout`), um ecrã de cada vez, o conteúdo de um ficheiro de texto (`more texto.txt`)
mv	alterar o nome e/ou a localização de um ficheiro (`mv /home/deapc/source_file /home/deapc/temp/dest_file`)
passwd	alterar a senha ("password") de um utilizador (faz parte das suas credenciais para validar o utilizador)
pwd	imprimir na consola o diretório atual
rm	eliminar, eventualmente sem pedir confirmação (depende da configuração da consola), um ficheiro (`rm texto.txt`)
rmdir	eliminar um diretório vazio (`rmdir mydir`)
tail	listar para a consola (`stdout`) a última parte (10 linhas) do ficheiro de texto (`tail texto.txt`)
tar	criar, adicionar e extrair ficheiros para/de um arquivo
touch	alterar a data/hora de última modificação do ficheiro, se o ficheiro não existir então é criado (`touch newfile.txt`)
whereis	localizar um programa (`whereis gpg`)
wc	conta o número de caracteres, linhas, palavras, etc. de um ficheiro
who	lista os utilizadores ativos

Exemplos:

1. Abra um terminal no Ubuntu e digite o comando **whoami**

```
silva@silva-QEMU-Virtual-Machine:~$ whoami
silva
```

2. Para saber onde esta digite o comando **pwd.**

```
silva@silva-QEMU-Virtual-Machine:~$ pwd
/home/silva
```

3. Para listar as pastas e ficheiros do diretório atual, digite o comando **ls**:

```
silva@silva-QEMU-Virtual-Machine:~$ ls
Desktop     invent.gnmap  Modelos     Público          Vídeos
Documentos  invent.nmap   msfinstall  snap
Imagens     invent.xml    Música      Transferências
```

4. O comando anterior só mostrou os nomes das pastas (cor azul), ficheiros (cor branca) e atalhos (cor verde). Se desejar ver as informações destas pastas e ficheiros com mais pormenor, use o comando **ls -l** (comando primário + espaço + comando secundário):

```
silva@silva-QEMU-Virtual-Machine:~$ ls -l
total 80
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Desktop
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Documentos
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Imagens
-rw-r--r-- 1 root  root   1548 abr 19 16:44 invent.gnmap
-rw-r--r-- 1 root  root   5393 abr 19 16:44 invent.nmap
-rw-r--r-- 1 root  root  23019 abr 19 16:44 invent.xml
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Modelos
-rwxr-xr-x 1 root  root   6139 abr 24 12:07 msfinstall
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Música
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Público
drwx------ 5 silva silva  4096 abr  2  2024 snap
drwxr-xr-x 3 silva silva  4096 abr  4  2024 Transferências
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Vídeos
```

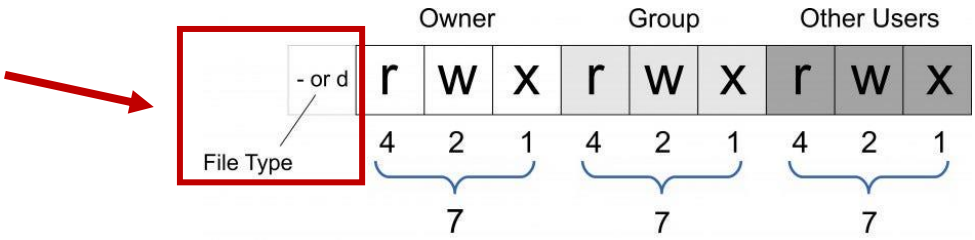
Repare que este comando deu informações mais personalizadas para cada elemento, tais como:

- 1ª Coluna: permissões do conteúdo
- 2ª Coluna: número de links do conteúdo
- 3ª Coluna: proprietário do conteúdo
- 4ª Coluna: proprietário do grupo do conteúdo
- 5ª Coluna: tamanho do conteúdo em bytes
- 6ª Coluna: última data/hora de modificação do conteúdo
- 7ª Coluna: nome do ficheiro ou diretório

Repare na 1ª Coluna das permissões do conteúdo.

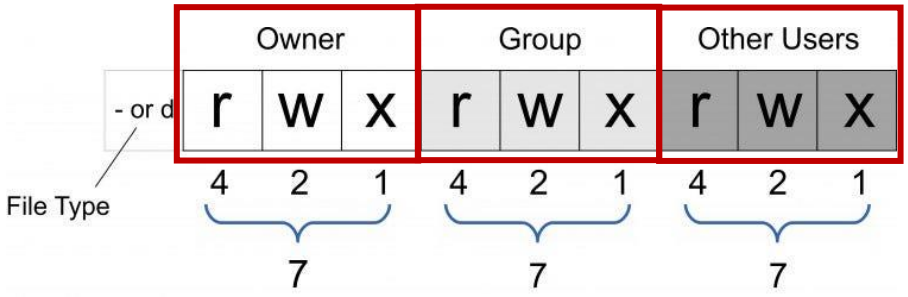
Em primeiro lugar, temos qual o tipo de ficheiro encontrado com o símbolo:

- **-** →corresponde a um ficheiro;
- **d** → corresponde a uma pasta/diretório;



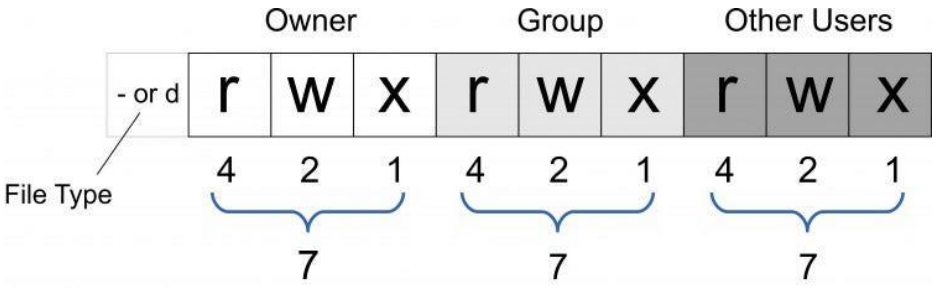
Esta informação mostra quais os 3 grupos da utilização da pasta/ficheiro:

- **Owner**: representa as permissões associadas ao dono do ficheiro;
- **Group**: representa as permissões para utilizadores do grupo do dono desse ficheiro;
- **Other Users**: representa os outros utilizadores da máquina;



A ordem de cada grupo de permissões é a mesma para todos os ficheiros/pastas, e cada conjunto tem sempre 3 posições "rwx" sempre por esta ordem:

- **R** (Read): permissão para ler a informação que corresponde ao número 4;
- **W** (Write): permissão para escrever na pasta/ficheiro que corresponde ao número 2;
- **X** (Executar): permissão para executar que corresponde ao número 1;



Se uma dada permissão está inativa aparece um "-" na posição respetiva e, por isso, essa operação é proibida para a entidade a que se refere.

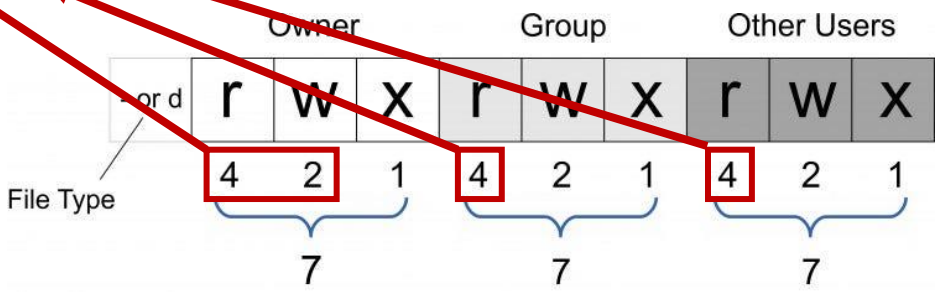
```
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Documentos
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Imagens
-rw-r--r-- 1 root  root   1548 abr 19 16:44 invent.gnmap
-rw-r--r-- 1 root  root   5393 abr 19 16:44 invent.nmap
```

O **comando chmod** permite alterar as permissões do proprietário do ficheiro, o grupo ao qual está associado o proprietário e as permissões de acesso ao ficheiro.

Este comando pode ser utilizado de forma numérica. No final converte-se o número binário resultante para octal. Se se pretender obter as permissões indicadas a seguir deve executar o comando chmod 644 gotas.png.

```
-  rw-  r--  r--  1 userX groupZ 453951 2007-03-03 17:29 gotas.png
   110  100  100

   6    4    4
```



O numero máximo a atribuir em cada grupo vai de 0 até 7 (soma das permissões do r (4), w (2) e x (1).

Esta ação também pode ser efetuada em modo gráfico: executar o explorador de ficheiros; selecionar o ficheiro pretendido; pressionar o botão lado direito do rato; escolher propriedades; alterar as permissões.

5. Se usar o comando **ls -la**, vai ter a exibição do conteúdo ainda mais aprofundado, ou seja, mostra os ficheiros ou diretórios em formato de tabela com informações adicionais ***que incluem os ficheiros ou diretórios ocultos:***

```
silva@silva-QEMU-Virtual-Machine:~$ ls -la
total 136
drwxr-x--- 19 silva silva  4096 abr 24 12:09 .
drwxr-xr-x  5 root  root   4096 abr 15  2024 ..
-rw-------  1 silva silva   908 jul  2 18:06 .bash_history
-rw-r--r--  1 silva silva   220 mar 22  2024 .bash_logout
-rw-r--r--  1 silva silva  3771 mar 22  2024 .bashrc
drwx------ 14 silva silva  4096 abr 15  2024 .cache
drwx------ 13 silva silva  4096 mar 22  2024 .config
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Desktop
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Documentos
drwx------  2 silva silva  4096 out  4 11:15 .gnupg
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Imagens
-rw-r--r--  1 root  root   1548 abr 19 16:44 invent.gnmap
-rw-r--r--  1 root  root   5393 abr 19 16:44 invent.nmap
-rw-r--r--  1 root  root  23019 abr 19 16:44 invent.xml
drwx------  3 silva silva  4096 mar 22  2024 .local
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Modelos
drwx------  3 silva silva  4096 abr  7  2024 .mozilla
drwxrwxr-x  5 silva silva  4096 abr 24 12:09 .msf4
-rwxr-xr-x  1 root  root   6139 abr 24 12:07 msfinstall
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Música
-rw-r--r--  1 silva silva   807 mar 22  2024 .profile
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Público
```

6. Para limpar o conteúdo da consola, use o comando **clear**:

```
-rwxr-xr-x  1 root  root   6139 abr 24 12:07 msfinstall
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Música
-rw-r--r--  1 silva silva   807 mar 22  2024 .profile
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Público
drwx------  5 silva silva  4096 abr  2  2024 snap
drwx------  2 silva silva  4096 abr  7  2024 .ssh
-rw-r--r--  1 silva silva     0 mar 22  2024 .sudo_as_admin_success
drwx------  4 silva silva  4096 abr  7  2024 .thunderbird
drwxr-xr-x  3 silva silva  4096 abr  4  2024 Transferências
drwxr-xr-x  2 silva silva  4096 mar 22  2024 Vídeos
silva@silva-QEMU-Virtual-Machine:~$ clear
```

```
silva@silva-QEMU-Virtual-Machine: ~
silva@silva-QEMU-Virtual-Machine:~$
```

7. Atualmente, estamos na conta do utilizador (conforme foi visto no comando do passo 2). Dentro deste diretório temos acesso ao Desktop (ambiente de trabalho), Documentos, Imagens, ou seja, a vossa pasta pessoal no sistema operativo.

Para conseguir ***navegar para dentro de uma pasta*** (comando genérico em qualquer sítio), deve usar o comando **cd** e de seguida escreva o nome da pasta a aceder:

```
silva@silva-QEMU-Virtual-Machine: ~
silva@silva-QEMU-Virtual-Machine:~$ pwd
/home/silva
silva@silva-QEMU-Virtual-Machine:~$ ls -l
total 80
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Desktop
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Documentos
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Imagens
-rw-r--r-- 1 root  root   1548 abr 19 16:44 invent.gnmap
-rw-r--r-- 1 root  root   5393 abr 19 16:44 invent.nmap
-rw-r--r-- 1 root  root  23019 abr 19 16:44 invent.xml
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Modelos
-rwxr-xr-x 1 root  root   6139 abr 24 12:07 msfinstall
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Música
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Público
drwx------ 5 silva silva  4096 abr  2  2024 snap
drwxr-xr-x 3 silva silva  4096 abr  4  2024 Transferências
drwxr-xr-x 2 silva silva  4096 mar 22  2024 Vídeos
silva@silva-QEMU-Virtual-Machine:~$ cd Desktop/
```

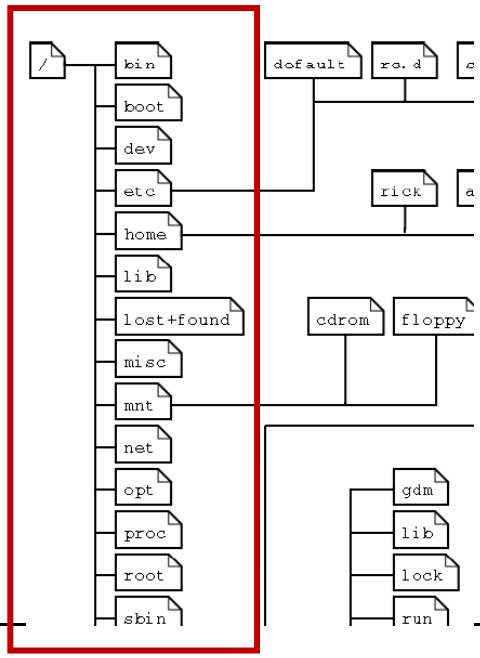
Resultado:

```
silva@silva-QEMU-Virtual-Machine:~$ cd Desktop/
silva@silva-QEMU-Virtual-Machine:~/Desktop$ ls -l
total 0
silva@silva-QEMU-Virtual-Machine:~/Desktop$
```

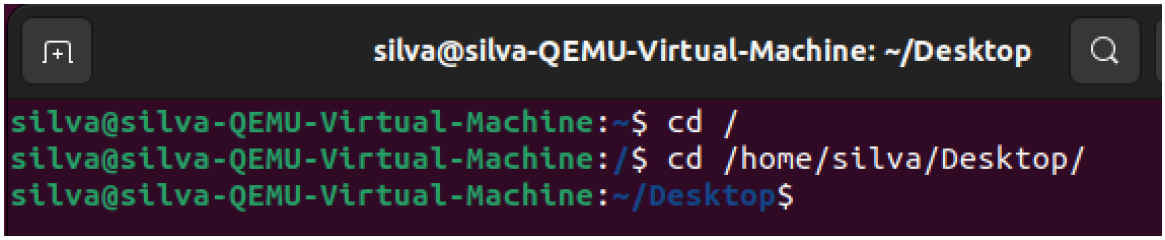
Repare que o nome da pasta onde está atualmente ficou a azul. Como no ambiente de trabalho não existem ficheiro ou pastas o comando ls -l retornou 0.

8. Imagine que deseja entrar numa hierarquia de pastas. Como tal, vamos fazer os seguintes passos:

a. Vamos posicionar na pasta principal onde estão todos os ficheiros do sistema operativo (raiz), com o comando: **cd /**

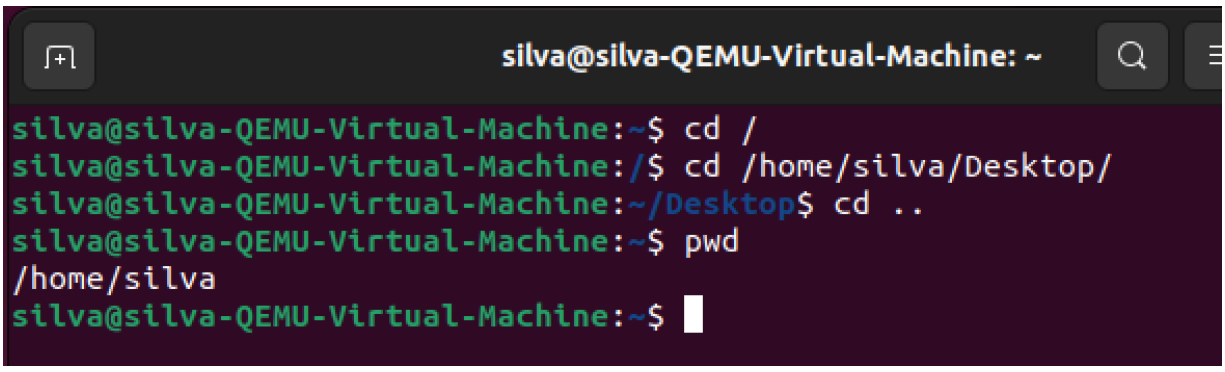


b. Queremos ***navegar até ao ambiente de trabalho que está na nossa pasta pessoal*** (mas funciona para outros mapeamentos). Use o comando **cd /home/<nome_do_utilizador>/Desktop**

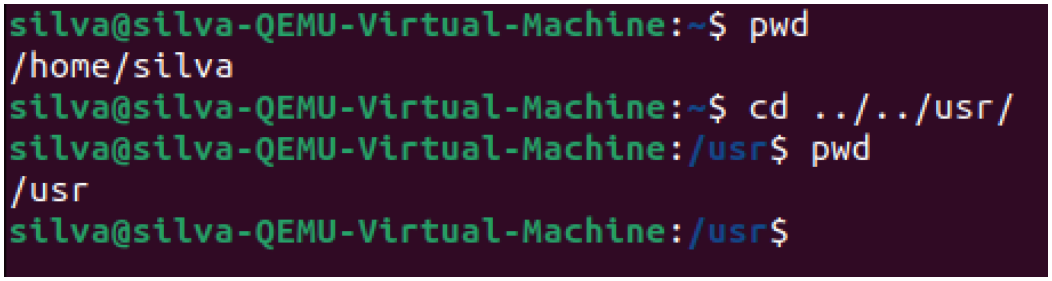


- **Nota Importante 1:** as barras laterais (/) indicam para aceder a uma pasta;
- **Nota Importante 2:** para saber o utilizador, use o comando do passo 1 (whoami);

9. Aproveitando o exercício anterior, se desejar navegar para o diretório anterior, basta usar o comando **cd ..** (cd + espaço + dois pontos):



- **Nota Importante 1:** pode combinar a combinação dos últimos exercícios para navegar livremente. Exemplo:

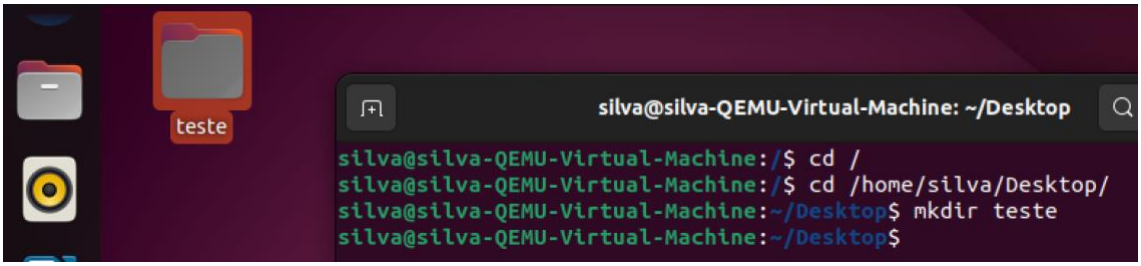


10. Para ***criar pastas***, usamos o comando ***mkdir***. Como estamos no ambiente de trabalho, vamos navegar até ao nosso ambiente de trabalho e criar a pasta com nome teste.

a. Vamos colocar na raiz da pasta principal do SO. Use o comando: **cd /**

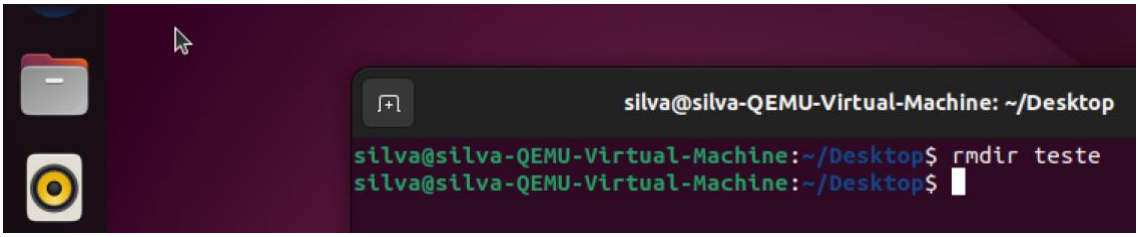
b. Navegar ao nosso ambiente de trabalho: **cd /home/<nome_utilizador>/Desktop**

c. Para criar uma pasta, use o seguinte comando: **mkdir teste**



- ***Nota Importante 1:*** Repare que a pasta foi criada no ambiente de trabalho
- ***Nota Importante 2:*** Também criar uma pasta numa localização dada por si (indicando a navegação do caminho);

11. Para **apagar uma pasta** (desde que esteja no sítio correto), use o comando: ***rmdir <nome_da_pasta> ou também rmdir*** e a localização onde está a pasta (através da navegação de pastas)

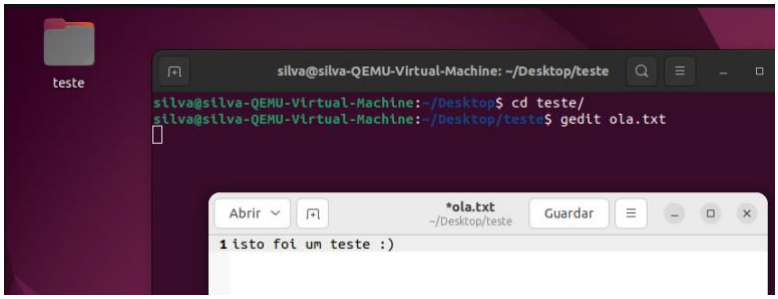


- ***Nota Importante:*** Repare que a pasta foi eliminada do ambiente de trabalho

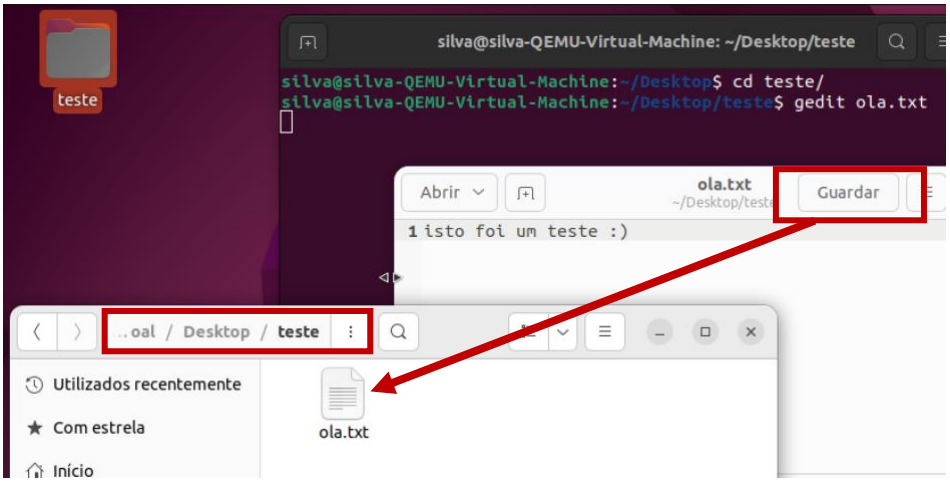
12. Volte a criar novamente a pasta que apagou.

13. Aceda dentro da pasta que criou no passo anterior.

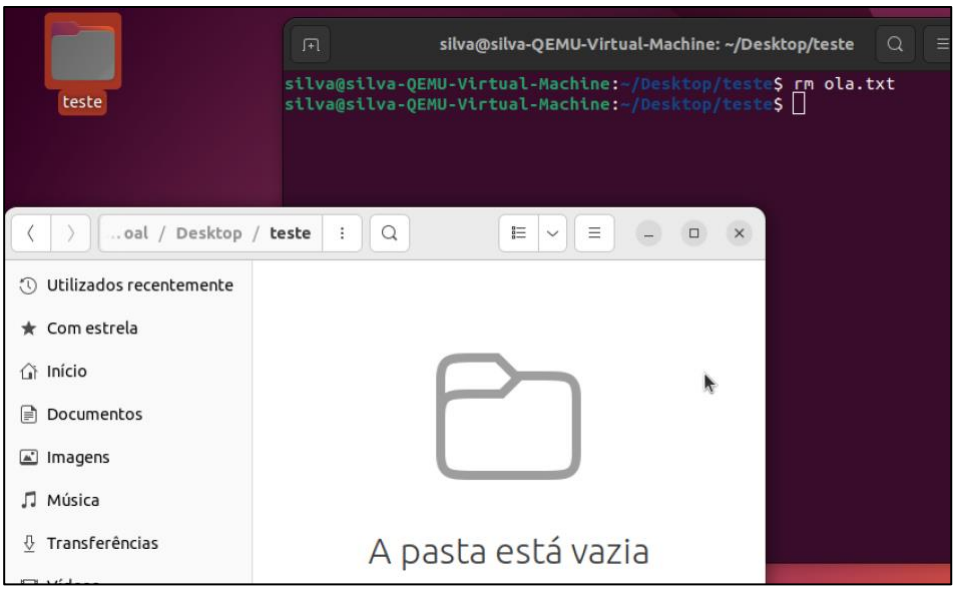
14. Para **criar ficheiros de texto**, use o comando **gedit** nome_do_ficheiro. Exemplo: **gedit ola.txt**



Ao clicar no botão guardar, este cria o ficheiro na localização:



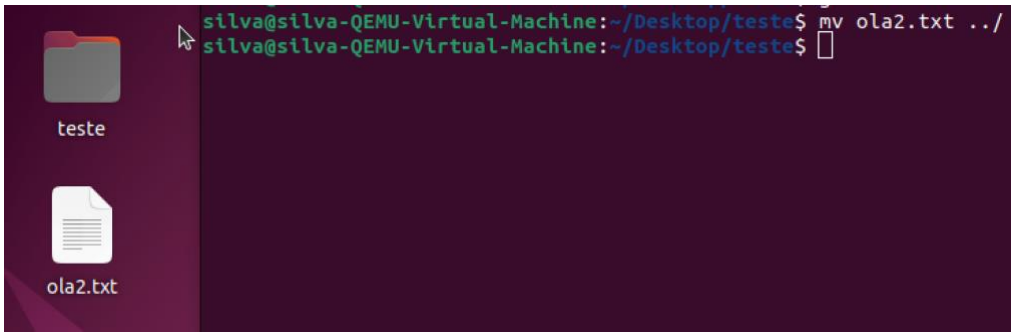
15. Para remover ficheiros, use o comando **rm** <nome_do_ficheiro> ou **rm** e localização onde está o ficheiro (através da navegação de pastas):



16. Volte a criar um ficheiro dentro da pasta teste, mas desta vez com o nome “ola2.txt”:

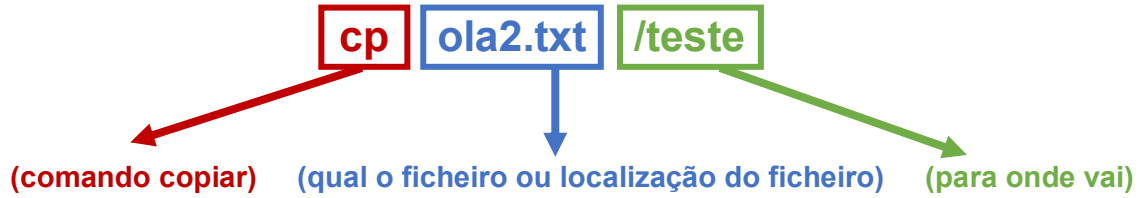
```
silva@silva-QEMU-Virtual-Machine:~/Desktop/teste$ gedit ola2.txt
```

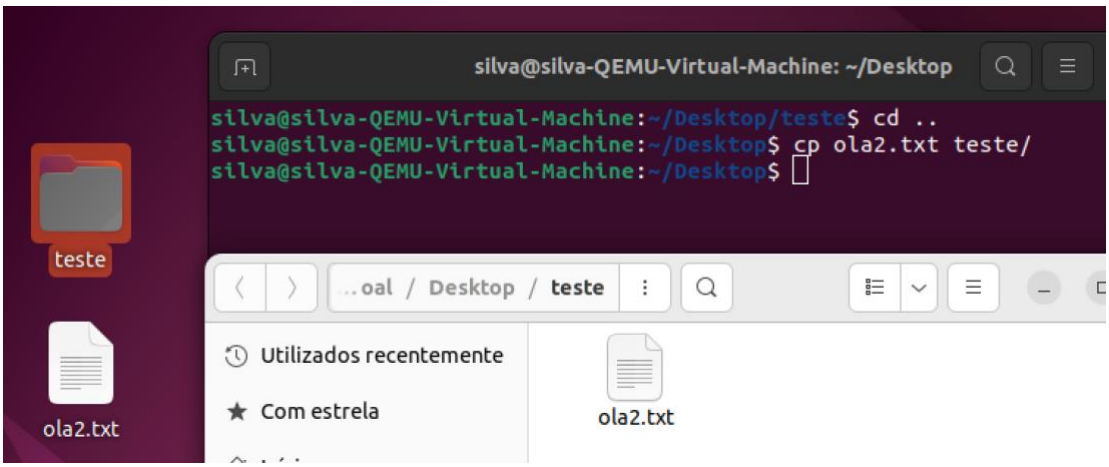
17. Para **mover ficheiros** de um diretório para outro, utilizamos o comando mv (move). Para este objetivo, queremos mover o ficheiro ola2.txt que está dentro da pasta teste ***para*** o ambiente de trabalho. Para este exemplo, certifique que está dentro da pasta teste e use o comando: **mv ola.txt ../**



18. Para **copiar ficheiros** de um diretório para outro, utilizamos o comando cp (copy). Para este objetivo, queremos copiar o ficheiro ola2.txt (que saiu da pasta no exercício anterior), e fazer uma cópia do mesmo para dentro da pasta teste.

Para este exemplo, no ambiente de trabalho (Desktop) e use o comando: **cp ola2.txt /teste**





19. Mudar a password de um utilizador, use o comando ***passwd*** e o nome do utilizador: