

# Desafio: Proteção de dados com ccrypt + Gerenciamento de processos com kill

Rita de Cássia Costa Barbosa

Comando ls usado para listar as informações presentes na minha home, depois cd para entrar no meu diretório pessoal

```
ubuntu@ip-172-31-51-230:~$ ls
ArquivosImportantes  Downloads  Public      snap
Desktop              Music      Templates  thinclient_drives
Documents            Pictures   Videos
ubuntu@ip-172-31-51-230:~$ cd ArquivosImportantes
ubuntu@ip-172-31-51-230:~/ArquivosImportantes$ ls
Senhas
```

Comando mkdir usado para criar um diretório, ls usado para listar, cd usado para entrar no diretório e cat > para criar e acessar um arquivo

```
ubuntu@ip-172-31-51-230:~/ArquivosImportantes$ mkdir documentos_privados
ubuntu@ip-172-31-51-230:~/ArquivosImportantes$ ls
Senhas  documentos_privados
ubuntu@ip-172-31-51-230:~/ArquivosImportantes$ cd documentos_privados
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ls
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ cat >info
rmacoes_confidenciais
Bradesco: 124578963
Itau: 326598741
CPF: 465498362518
Cartão débito:032310
^C
```

Comando cat usado para entrar no arquivo e ccrypt para criptografar o arquivo com uma senha específica

```
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ cat infor
macoes_confidenciais
Bradesco: 124578963
Itau: 326598741
CPF: 465498362518
Cartão débito:032310
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ccrypt in
formacoes_confidenciais
Enter encryption key:
Enter encryption key: (repeat)
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ |
```

## abertura de um segundo terminal

```
ubuntu@ip-172-31-51-230: ~ × + ▾ - □ ×
Memory usage: 5%                               IPv4 address for eth0: 172.31.51.230
Swap usage: 0%

* Ubuntu Pro delivers the most comprehensive open source security and
compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

10 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Mon Oct 16 22:06:54 2023 from 189.18.49.25
ubuntu@ip-172-31-51-230:~$ |

ubuntu@ip-172-31-51-230: ~/ArquivosImportantes/documentos_privados$ cat >info
rmacoes_confidenciais
Bradesco: 124578963
Itau: 326598741
CPF: 465498362518
Cartão débito:032310
^C
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ cat infor
macoes_confidenciais
Bradesco: 124578963
Itau: 326598741
CPF: 465498362518
Cartão débito:032310
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ccrypt in
```

comando ps -aux utilizado para listar todos os processos em execução no sistema.

```
ubuntu@ip-172-31-51-230:~$ ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root             1  0.6  0.1 182960 11764 ?        Ss   22:04   0:06 /sbin/init
root             2  0.0  0.0      0     0 ?        S    22:04   0:00 [kthreadd]
root             3  0.0  0.0      0     0 ?        I<   22:04   0:00 [rcu_gp]
root             4  0.0  0.0      0     0 ?        I<   22:04   0:00 [rcu_par_gp]
root             5  0.0  0.0      0     0 ?        I<   22:04   0:00 [slub_flushwq]
root             6  0.0  0.0      0     0 ?        I<   22:04   0:00 [netns]
root             8  0.0  0.0      0     0 ?        I<   22:04   0:00 [kworker/0:0H-events_highpri]
root            10  0.0  0.0      0     0 ?        I<   22:04   0:00 [mm_percpu_wq]
root            11  0.0  0.0      0     0 ?        I    22:04   0:00 [rcu_tasks_rude_kthread]
root            12  0.0  0.0      0     0 ?        I    22:04   0:00 [rcu_tasks_trace_kthread]
root            13  0.0  0.0      0     0 ?        S    22:04   0:00 [ksoftirqd/0]
root            14  0.0  0.0      0     0 ?        I    22:04   0:00 [rcu_sched]
root            15  0.0  0.0      0     0 ?        S    22:04   0:00 [migration/0]
root            16  0.0  0.0      0     0 ?        S    22:04   0:00 [idle_inject/0]
root            18  0.0  0.0      0     0 ?        S    22:04   0:00 [cpuhp/0]
root            19  0.0  0.0      0     0 ?        S    22:04   0:00 [cpuhp/1]
root            20  0.0  0.0      0     0 ?        S    22:04   0:00 [idle_inject/1]
root            21  0.0  0.0      0     0 ?        S    22:04   0:00 [migration/1]
root            22  0.0  0.0      0     0 ?        S    22:04   0:00 [ksoftirqd/1]
root            24  0.0  0.0      0     0 ?        I<   22:04   0:00 [kworker/1:0H-kblockd]
root            25  0.0  0.0      0     0 ?        S    22:04   0:00 [kdevtmpfs]
root            26  0.0  0.0      0     0 ?        I<   22:04   0:00 [inet_frag_wq]
root            27  0.0  0.0      0     0 ?        S    22:04   0:00 [kauditd]
root            28  0.0  0.0      0     0 ?        I    22:04   0:00 [kworker/1:1-rcu_gp]
root            29  0.0  0.0      0     0 ?        S    22:04   0:00 [khungtaskd]
root            31  0.0  0.0      0     0 ?        S    22:04   0:00 [oom_reaper]
root            32  0.0  0.0      0     0 ?        I<   22:04   0:00 [writeback]
```

comando ccat ~/documentos\_privados/informacoes\_confidenciais.txt.cpt  
utilizado para simular um processo de invasão do arquivo criptografado no  
terminal principal

```
Enter encryption key: (repeat)
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ccat ~/do
cumentos_privados/informacoes_confidenciais.txt.cpt
Enter decryption key: |
```

utilizando o segundo terminal e novamente o comando ps -aux para  
identificar a utilização do comando ccat, reconhecido como PID 1373

```
gdm 957 0.0 0.2 332408 16640 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-keyboard
gdm 958 0.0 0.2 332708 16640 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-wacom
gdm 960 0.0 0.0 309880 7808 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-housekeeping
gdm 963 0.0 0.1 317296 9600 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-sound
gdm 966 0.0 0.2 373420 16256 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-datetime
gdm 972 0.0 0.1 384000 8448 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-smartcard
gdm 973 0.0 0.0 234104 6144 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-screensaver-proxy
gdm 974 0.0 0.1 463760 10368 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-sharing
gdm 997 0.0 0.1 340172 14976 tty1 SL+ 22:05 0:00 /usr/libexec/gsd-printer
colord 1026 0.0 0.1 243112 13216 ? Ssl 22:05 0:00 /usr/libexec/colord
gdm 1034 0.0 0.0 238460 7680 tty1 SL+ 22:05 0:00 /usr/libexec/gvfsd
gdm 1056 0.0 0.0 161296 7296 tty1 SL 22:05 0:00 /usr/libexec/ibus-memconf
gdm 1066 0.0 0.0 235076 7424 tty1 SL+ 22:05 0:00 /usr/libexec/ibus-portal
gdm 1079 0.0 0.0 161296 7296 tty1 SL 22:05 0:00 /usr/libexec/ibus-engine-simple
root 1110 0.0 0.1 170804 10496 ? Ss 22:06 0:00 sshd: ubuntu [priv]
ubuntu 1113 0.0 0.1 17208 9728 ? Ss 22:06 0:00 /lib/systemd/systemd --user
ubuntu 1114 0.0 0.0 120476 5712 ? S 22:06 0:00 (sd-pam)
ubuntu 1120 0.0 0.0 37232 6272 ? Ssl 22:06 0:00 /usr/bin/pipewire
ubuntu 1121 0.0 0.0 21256 6784 ? Ssl 22:06 0:00 /usr/bin/pipewire-media-session
ubuntu 1122 0.0 0.2 283912 18176 ? Ssl 22:06 0:00 /usr/bin/pulseaudio --daemonize=no --log-target=journal
ubuntu 1140 0.0 0.0 8296 4480 ? Ss 22:06 0:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activati
ubuntu 1222 0.0 0.0 17216 7800 ? S 22:06 0:00 sshd: ubuntu@pts/0
ubuntu 1225 0.0 0.0 9100 5120 pts/0 Ss 22:06 0:00 -bash
root 1240 0.0 0.0 0 0 ? I< 22:06 0:00 [tls-strp]
root 1298 0.0 0.0 0 0 ? I 22:16 0:00 [kworker/1:0-cgroup_destroy]
root 1304 0.0 0.1 17080 10624 ? Ss 22:19 0:00 sshd: ubuntu [priv]
root 1323 0.0 0.0 0 0 ? I 22:19 0:00 [kworker/1:2-events]
ubuntu 1360 0.0 0.0 17212 7704 ? R 22:19 0:00 sshd: ubuntu@pts/1
ubuntu 1361 0.0 0.0 9100 5120 pts/1 Ss 22:19 0:00 -bash
ubuntu 1373 0.0 0.0 6448 2176 pts/0 S+ 22:22 0:00 ccat /home/ubuntu/documentos_privados/informacoes_confidenciais.txt.cpt
ubuntu 1375 0.0 0.0 10728 3456 pts/1 R+ 22:24 0:00 ps -aux
ubuntu@ip-172-31-51-230:~$
```

Utilizando o segundo terminal para matar o processo de PID 1373 com o  
comando kill -9

```
/ubuntu/documentos_privados/informacoes_confidenciais.txt.cpt
ubuntu 1375 0.0 0.0 10728 3456 pts/1 R+ 22:24 0:00
ubuntu@ip-172-31-51-230:~$ kill -9 1373
ubuntu@ip-172-31-51-230:~$ |
```

No terminal original pode-se ver a mensagem que o processo foi encerrado

```
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ccat ~/do
cumentos_privados/informacoes_confidenciais.txt.cpt
Enter decryption key: Killed
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ |
```

Mesmo utilizando o comando ccat novamente, por questão de segurança a  
proteção de dados não permite que você acesse aquele conteúdo

```
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ ccat ~/do
cumentos_privados/informacoes_confidenciais.txt.cpt
Enter decryption key:
ccat: /home/ubuntu/documentos_privados/informacoes_confidenciais.txt.cpt: No
such file or directory
ubuntu@ip-172-31-51-230:~/ArquivosImportantes/documentos_privados$ |
```