

Esercizio sui comandi della shell Linux

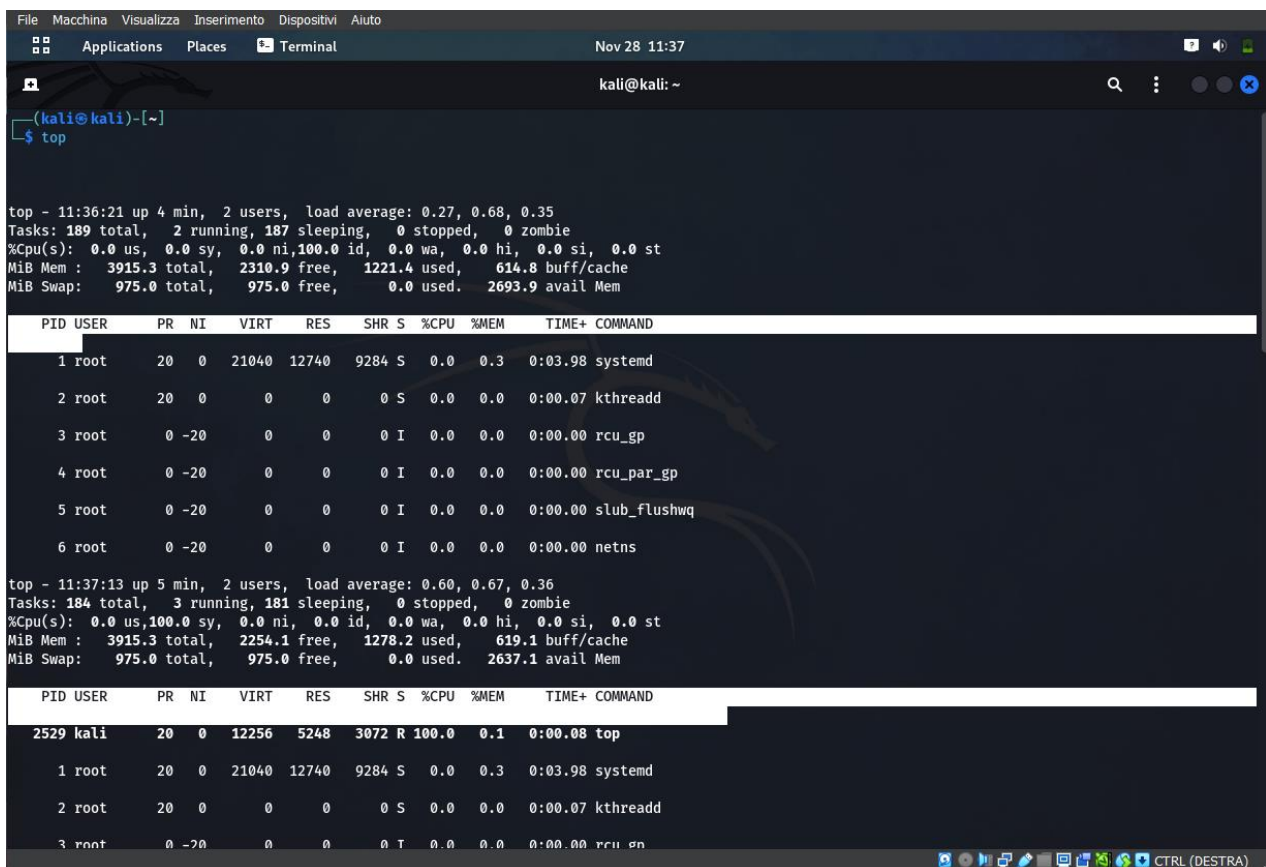
Data: 28/11/2023

Guglielmo Carratello

Controllo dei Processi con il Comando "top"

Abbiamo eseguito il comando “ **top** ” sulla macchina Linux per monitorare i processi attivi. Le colonne principali visualizzate includono:

- PID (Process ID): Identificativo univoco per ogni processo.
- USER: Nome dell'utente proprietario del processo.
- COMMAND: Il comando o il programma che ha generato il processo.



```
(kali@kali)~$ top

top - 11:36:21 up 4 min, 2 users, load average: 0.27, 0.68, 0.35
Tasks: 189 total, 2 running, 187 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3915.3 total, 2310.9 free, 1221.4 used, 614.8 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 2693.9 avail Mem

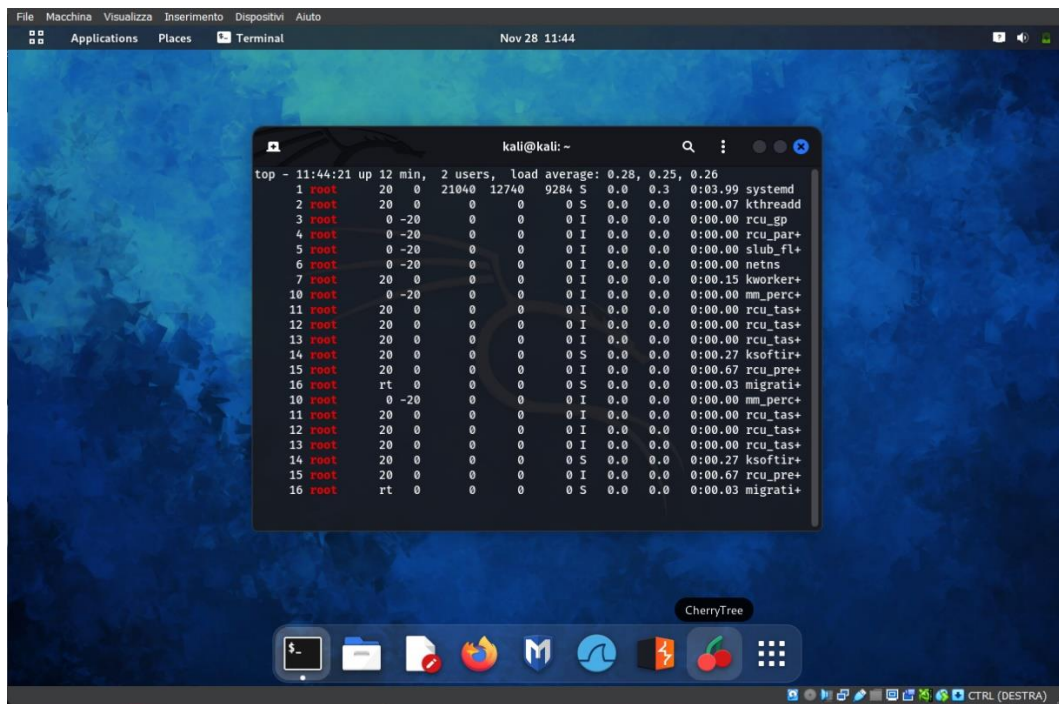
  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
    1 root        20   0   21040   12740  9284  S   0.0   0.3   0:03.98 systemd
    2 root        20   0         0         0      0  S   0.0   0.0   0:00.07 kthreadd
    3 root         0 -20         0         0      0  I   0.0   0.0   0:00.00 rcu_gp
    4 root         0 -20         0         0      0  I   0.0   0.0   0:00.00 rcu_par_gp
    5 root         0 -20         0         0      0  I   0.0   0.0   0:00.00 slub_flushwq
    6 root         0 -20         0         0      0  I   0.0   0.0   0:00.00 netns

top - 11:37:13 up 5 min, 2 users, load average: 0.60, 0.67, 0.36
Tasks: 184 total, 3 running, 181 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us,100.0 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3915.3 total, 2254.1 free, 1278.2 used, 619.1 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 2637.1 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
2529 kali        20   0   12256   5248  3072  R 100.0   0.1   0:00.08 top
    1 root        20   0   21040   12740  9284  S   0.0   0.3   0:03.98 systemd
    2 root        20   0         0         0      0  S   0.0   0.0   0:00.07 kthreadd
    3 root         0 -20         0         0      0  I   0.0   0.0   0:00.00 rcu_gp
```

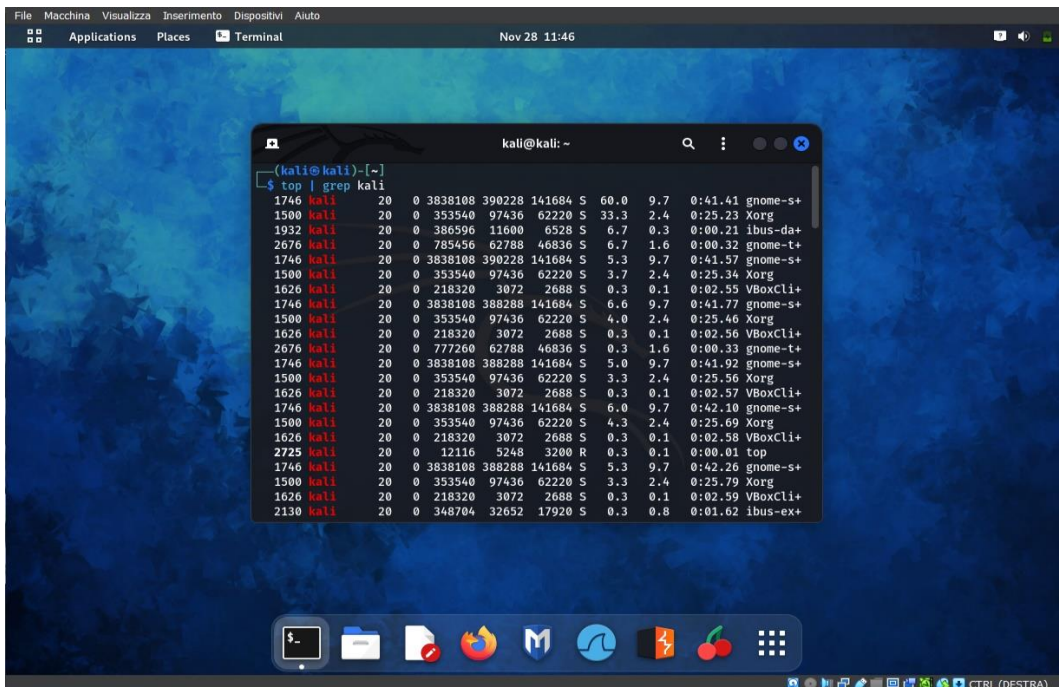
Filtraggio dei Processi per Utente "root"

Abbiamo utilizzato il comando “ **top | grep root** ” per filtrare i risultati e visualizzare solo i processi in esecuzione per l'utente "root". Questo ci consente di ottenere un elenco specifico dei processi associati a tale utente.



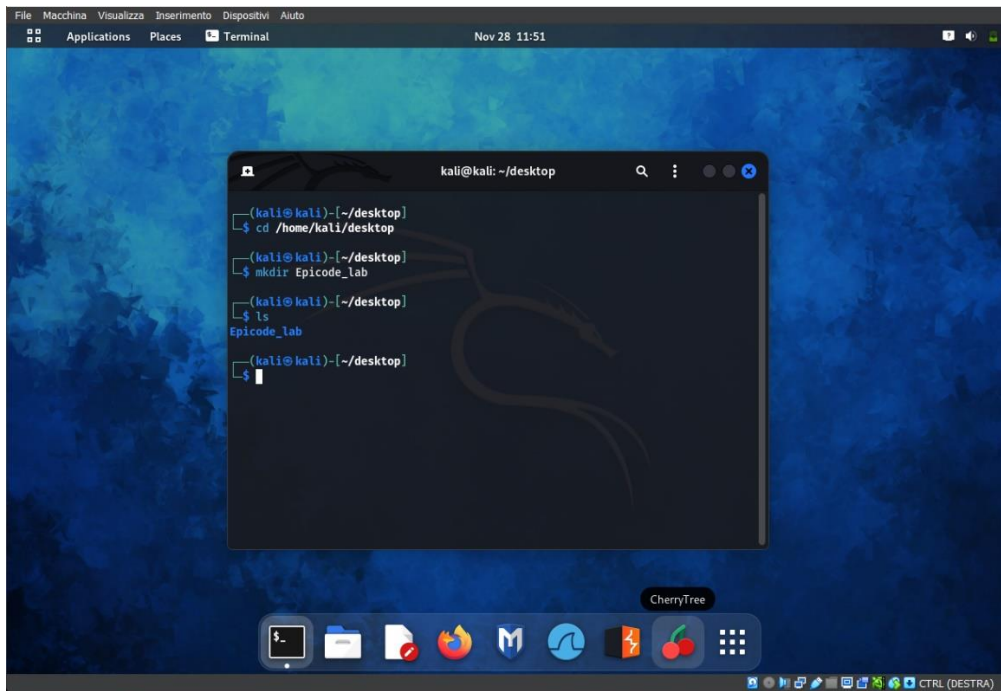
Filtraggio dei Processi per Utente "kali"

Abbiamo ripetuto il processo precedente, questa volta utilizzando il comando “`top | grep kali`” per mostrare solo i processi in esecuzione dall'utente "kali".



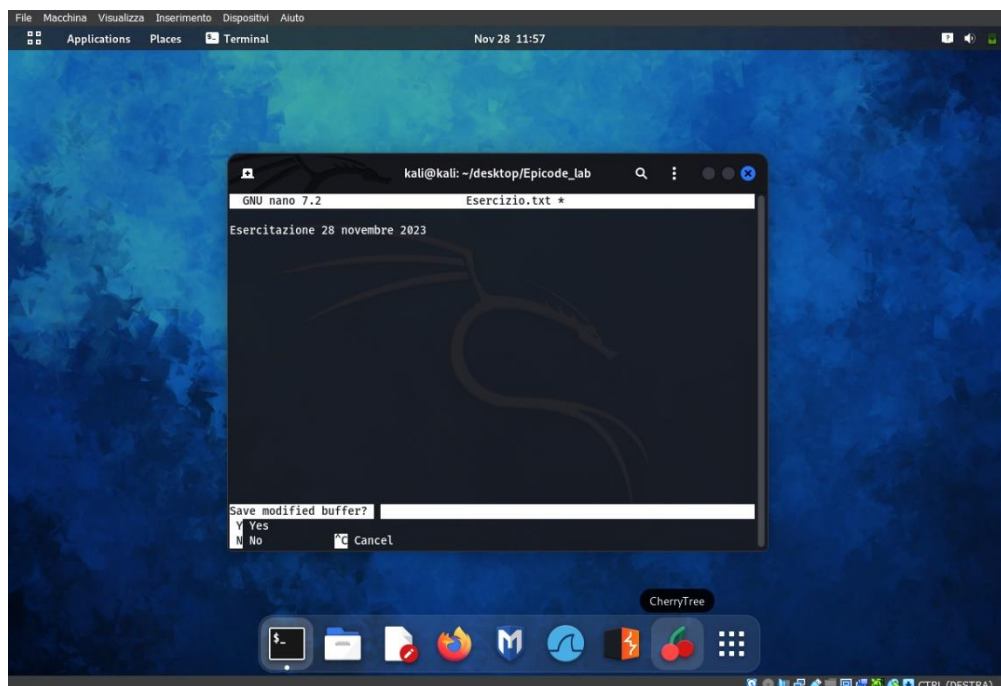
Creazione di una Nuova Directory

Abbiamo creato una nuova directory chiamata "Epicode_Lab" nella directory /home/kali/Desktop utilizzando il comando “`mkdir Epicode_lab`”



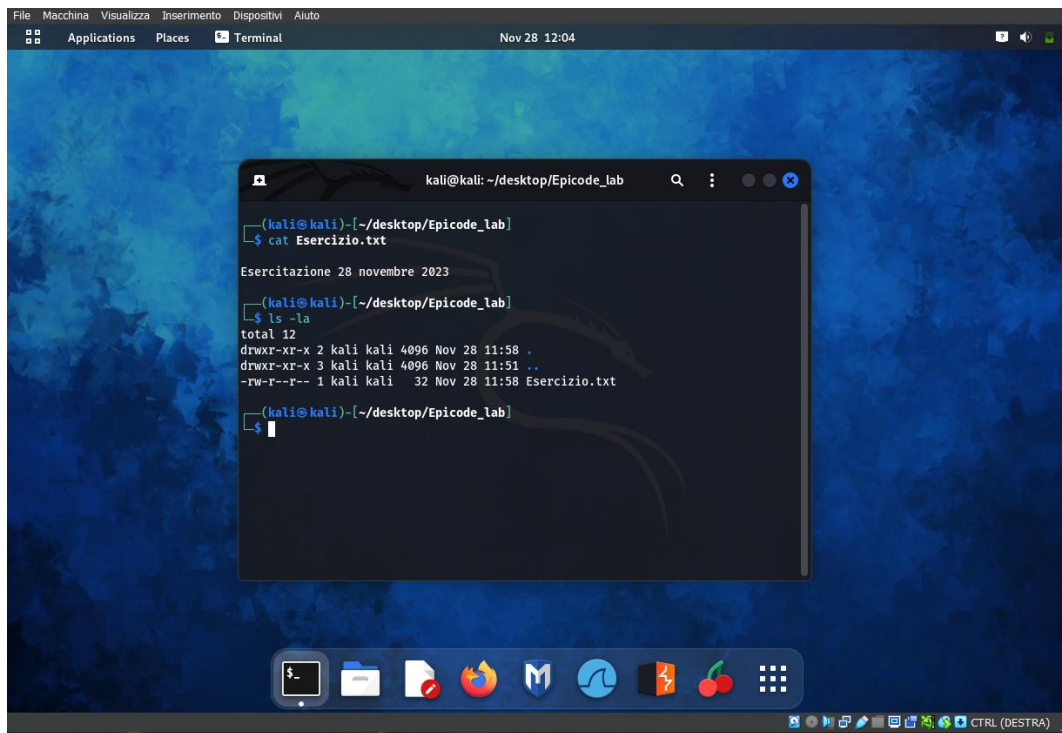
Creazione e Modifica di un File

Siamo entrati nella nuova directory e abbiamo creato il file "**Esercizio.txt**" con l'editor di testo nano. Successivamente, abbiamo modificato il file e utilizzato la sequenza Ctrl+X, e Y per salvarlo.



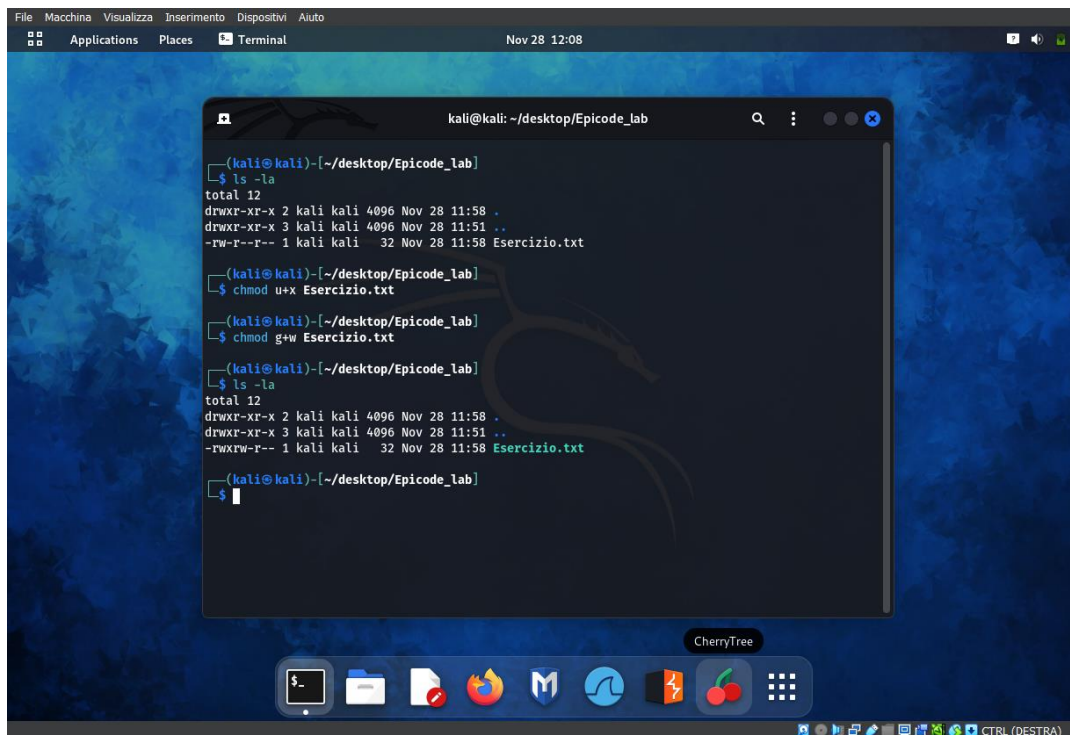
Controllo dei Permessi del File

Abbiamo utilizzato il comando "**cat**" per visualizzare il testo del file che avevamo precedentemente creato e modificato. Successivamente abbiamo utilizzato il comando "**ls -la**" per controllare i permessi del file appena creato, visualizzando le autorizzazioni per utente, gruppo e altri.



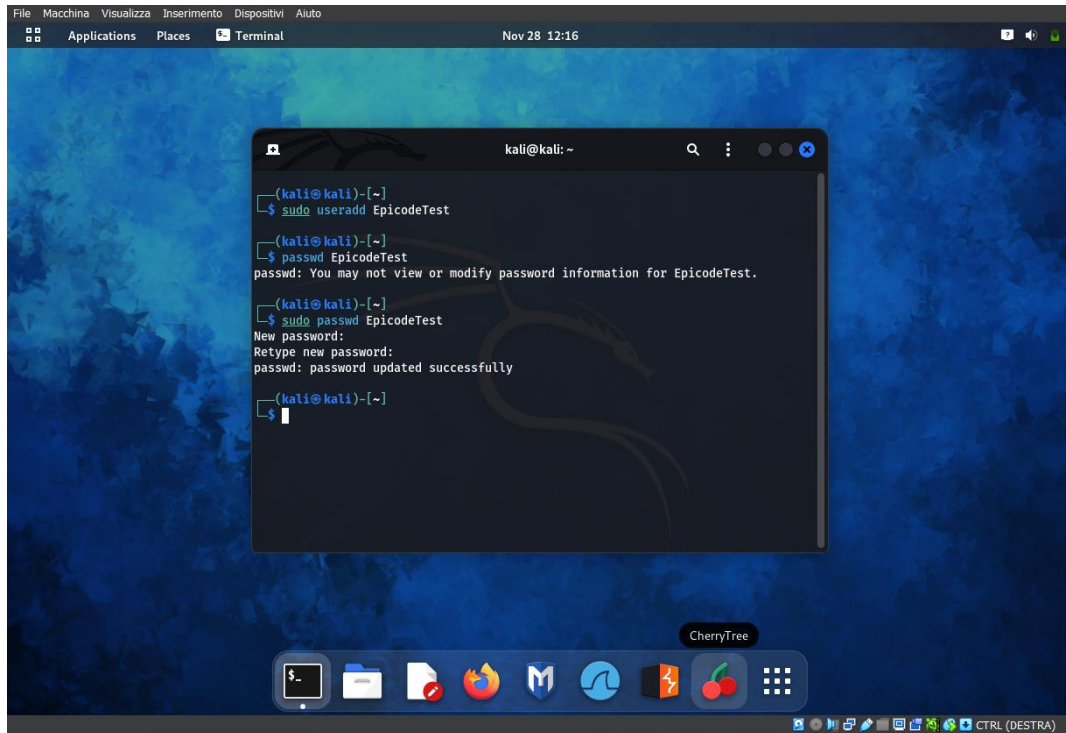
Modifica dei Privilegi del File

Abbiamo modificato i privilegi del file con il comando “ `chmod u+x Esercizio.txt` ” ed il comando “ `chmod g+w` ” per garantire al proprietario tutti i privilegi dell’user (r,w,x), al gruppo (r,w), e agli altri solo la lettura (r).



Creazione di un Nuovo Utente

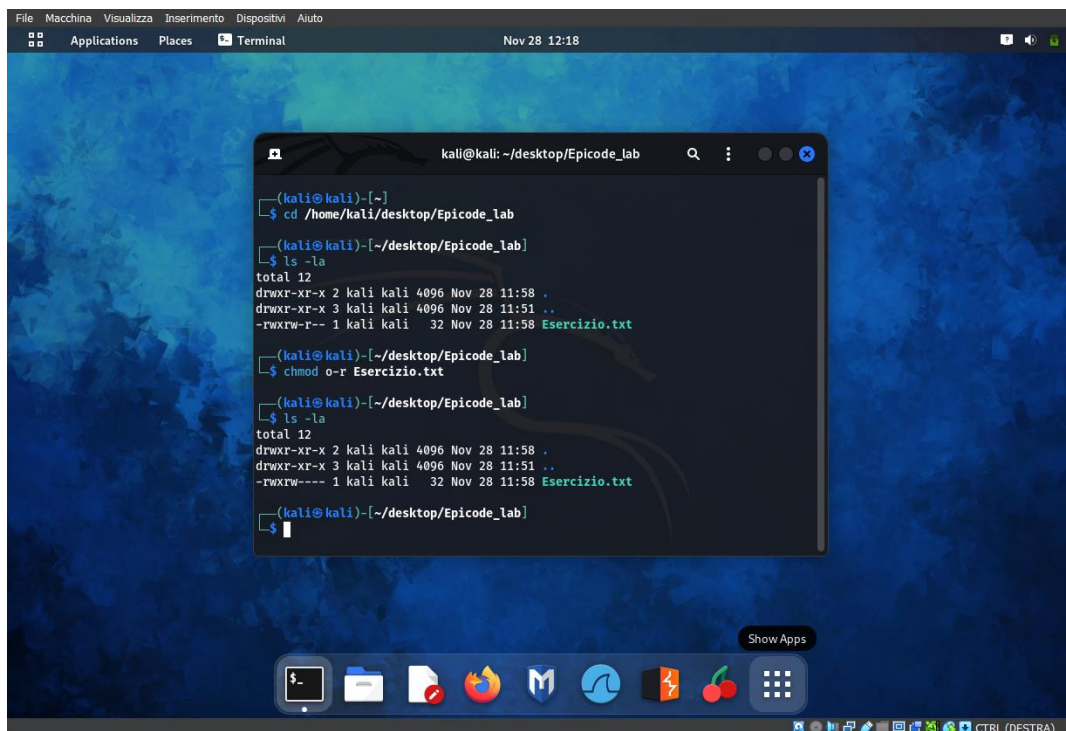
Abbiamo creato un nuovo utente con il comando “ **sudo useradd** ” chiamandolo **EpicodeTest**. Abbiamo utilizzato il comando sudo prima di useradd perché per poter creare un nuovo utente necessitiamo dei privilegi da amministratore ed assegnato una password utilizzando il comando “ **passwd** ”.



```
kali@kali: ~  
$ sudo useradd EpicodeTest  
$ passwd EpicodeTest  
passwd: You may not view or modify password information for EpicodeTest.  
$ sudo passwd EpicodeTest  
New password:  
Retype new password:  
passwd: password updated successfully  
$
```

Gestione dei Privilegi del File per l'Utente Corrente

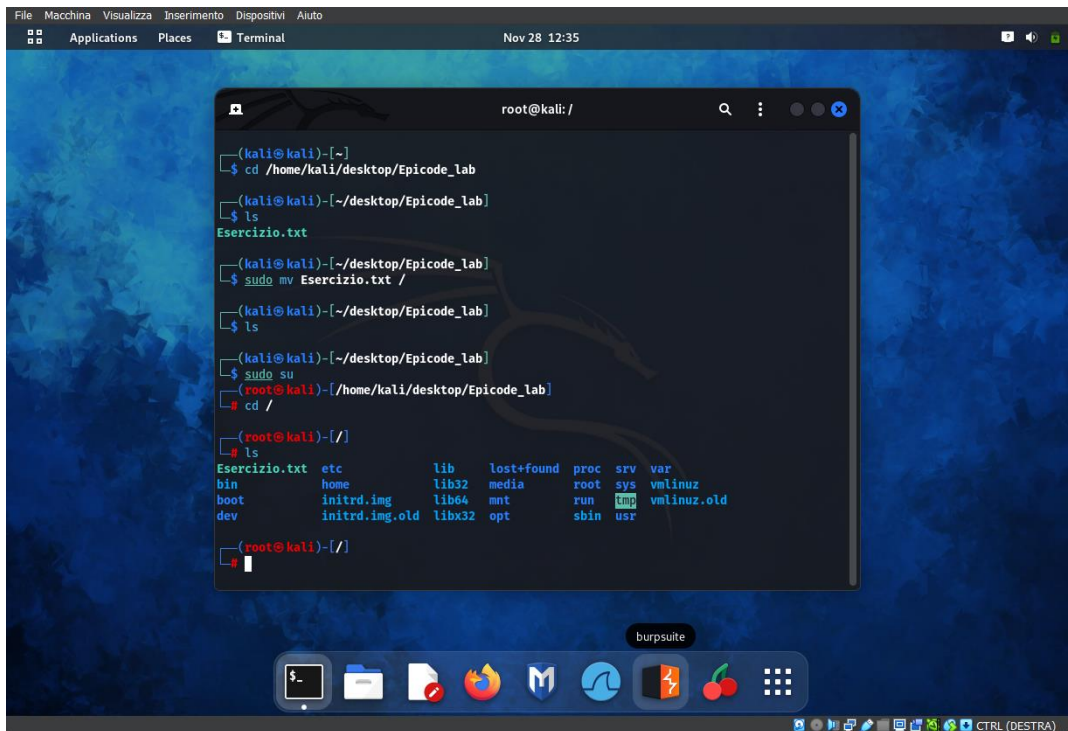
Abbiamo cambiato i privilegi del file .txt in modo che "altri utenti" non siano abilitati alla lettura.



```
kali@kali: ~/desktop/Epicode_lab  
$ cd /home/kali/desktop/Epicode_lab  
$ ls -la  
total 12  
drwxr-xr-x 2 kali kali 4096 Nov 28 11:58 .  
drwxr-xr-x 3 kali kali 4096 Nov 28 11:51 ..  
-rwxrwx-- 1 kali kali 32 Nov 28 11:58 Esercizio.txt  
$ chmod o-r Esercizio.txt  
$ ls -la  
total 12  
drwxr-xr-x 2 kali kali 4096 Nov 28 11:58 .  
drwxr-xr-x 3 kali kali 4096 Nov 28 11:51 ..  
-rwxrwx---- 1 kali kali 32 Nov 28 11:58 Esercizio.txt  
$
```

Spostamento del File nella Directory di Root

Abbiamo spostato il file nella directory di **root** (/) utilizzando il comando “**mv**”.



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Places Terminal Nov 28 12:35

root@kali: /

(kali@kali)-[~]
$ cd /home/kali/desktop/Epicode_lab

(kali@kali)-[~/desktop/Epicode_lab]
$ ls
Esercizio.txt

(kali@kali)-[~/desktop/Epicode_lab]
$ sudo mv Esercizio.txt /

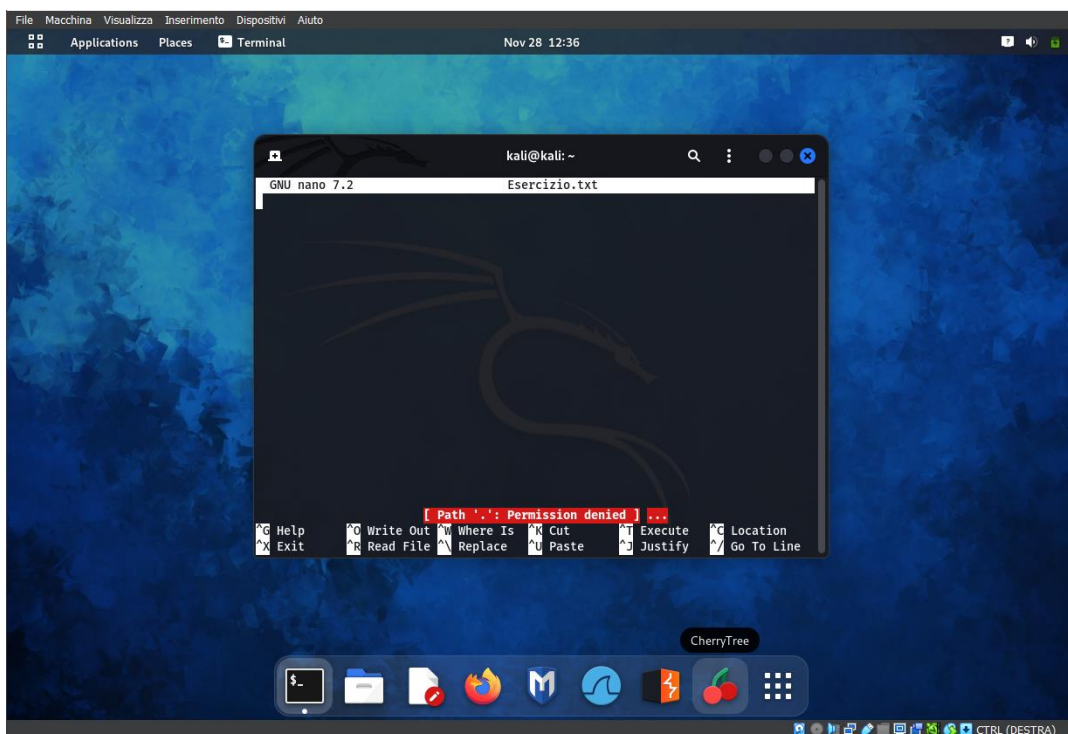
(kali@kali)-[~/desktop/Epicode_lab]
$ ls

(kali@kali)-[~/desktop/Epicode_lab]
$ sudo su
(root@kali)-[~/home/kali/desktop/Epicode_lab]
# cd /

(root@kali)-[/]
# ls
Esercizio.txt  etc          lib          lost+found    proc          srv          var
bin            home         lib32        media         root          sys         vmlinuz
boot          initrd.img  lib64        mnt           run           tmp         vmlinuz.old
dev           initrd.img.old libx32       opt           sbin          usr
```

Cambio Utente e Tentativo di Accesso al File

Abbiamo cambiato utente con il comando “**su EpicodeTest**” e provato ad aprire il file.txt in lettura con “**nano Esercizio.txt**”. Abbiamo ricevuto un errore in quanto il nuovo utente non ha i privilegi necessari.



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Places Terminal Nov 28 12:36

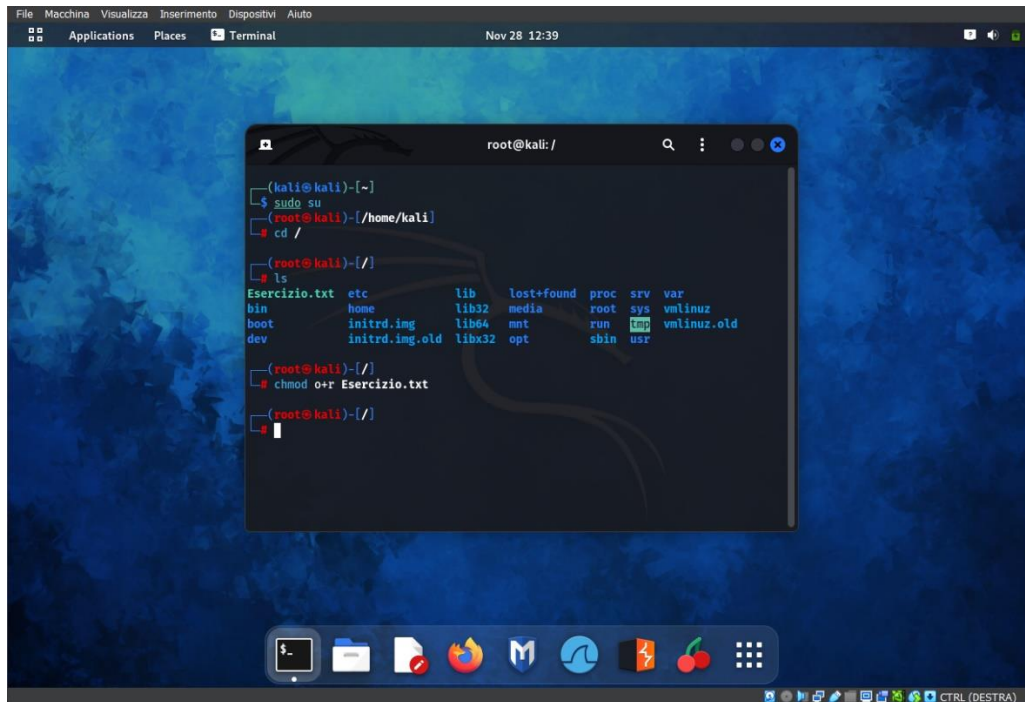
kali@kali: ~
GNU nano 7.2 Esercizio.txt

[ Path './': Permission denied ] ...

^G Help ^O Write Out ^W Where Is ^K Cut ^E Execute ^L Location
^X Exit ^R Read File ^M Replace ^U Paste ^J Justify ^_ Go To Line
```

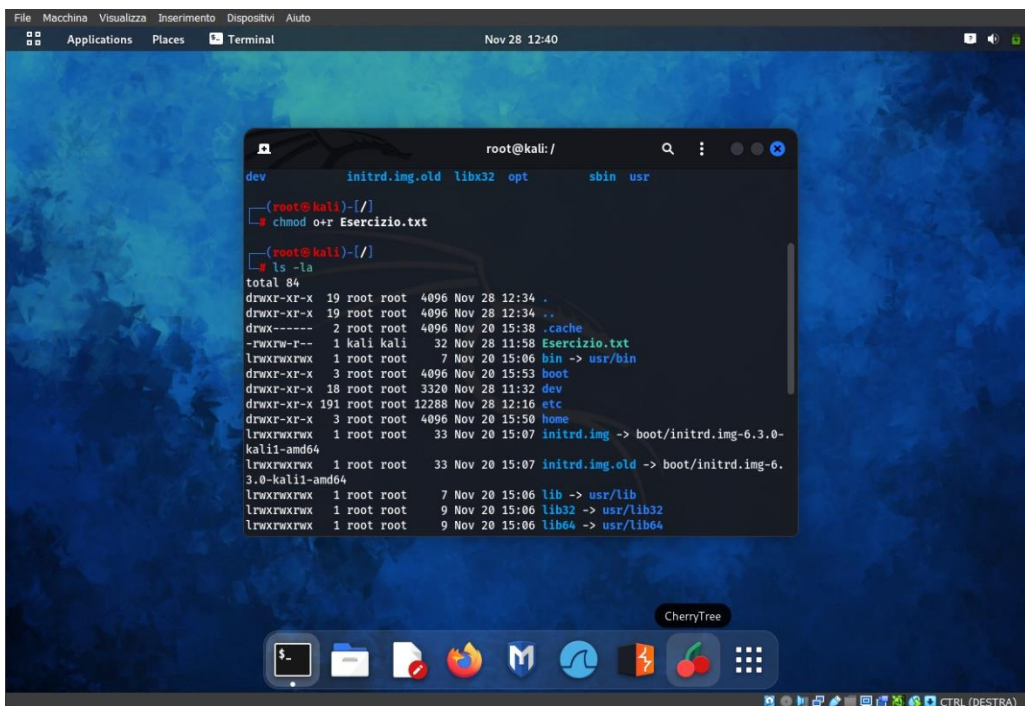

Modifica dei Permessi per Consentire l'Accesso

Abbiamo modificato i permessi del file per consentire al nuovo utente la lettura, quindi siamo tornati con l'utente di partenza, preso i privilegi da amministratore con il comando “**sudo su**” perché il file si trova nella directory del **root**, quindi necessitiamo dei privilegi da amministratore e ripetuto il tentativo di apertura del file entrando nuovamente con il nuovo utente **EpicodeTest** ed andando a vedere se riusciamo a leggere il file con il comando “**nano Esercizio.txt**”.



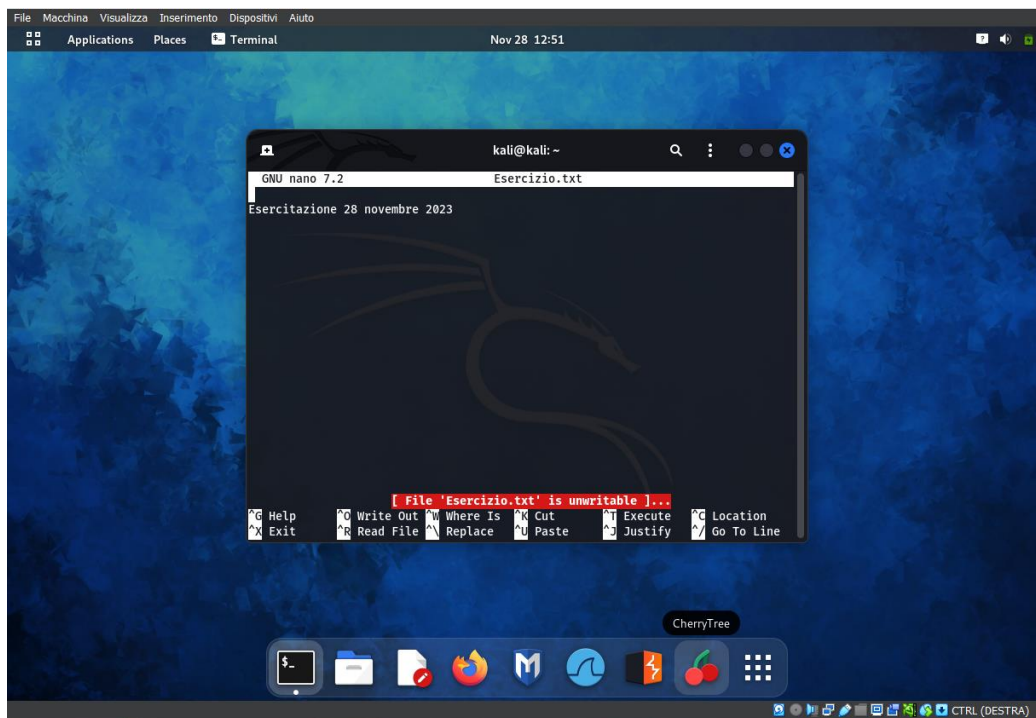
A terminal window on a Kali Linux desktop. The user is root at kali. They run 'ls' showing the root directory contents. Then they run 'chmod o+r Esercizio.txt' to add read permissions for others to the file 'Esercizio.txt' in the root directory.

```
root@kali: /  
(kali@kali)-[~]  
$ sudo su  
(root@kali)-[/home/kali]  
$ cd /  
(root@kali)-[/]  
$ ls  
Esercizio.txt  etc      lib      lost+found  proc  srv  var  
bin            home     lib32     media       root  sys  vmlinuz  
boot          initrd.img  lib64     mnt         run   tmp  vmlinuz.old  
dev           initrd.img.old  libx32    opt         sbin  usr  
(root@kali)-[/]  
$ chmod o+r Esercizio.txt  
(root@kali)-[/]  
$
```



A terminal window on a Kali Linux desktop. The user is root at kali. They run 'ls -la' showing detailed file permissions and ownership for the root directory. The output shows that 'Esercizio.txt' is owned by 'kali' and has permissions 'drwxrwxrwx'.

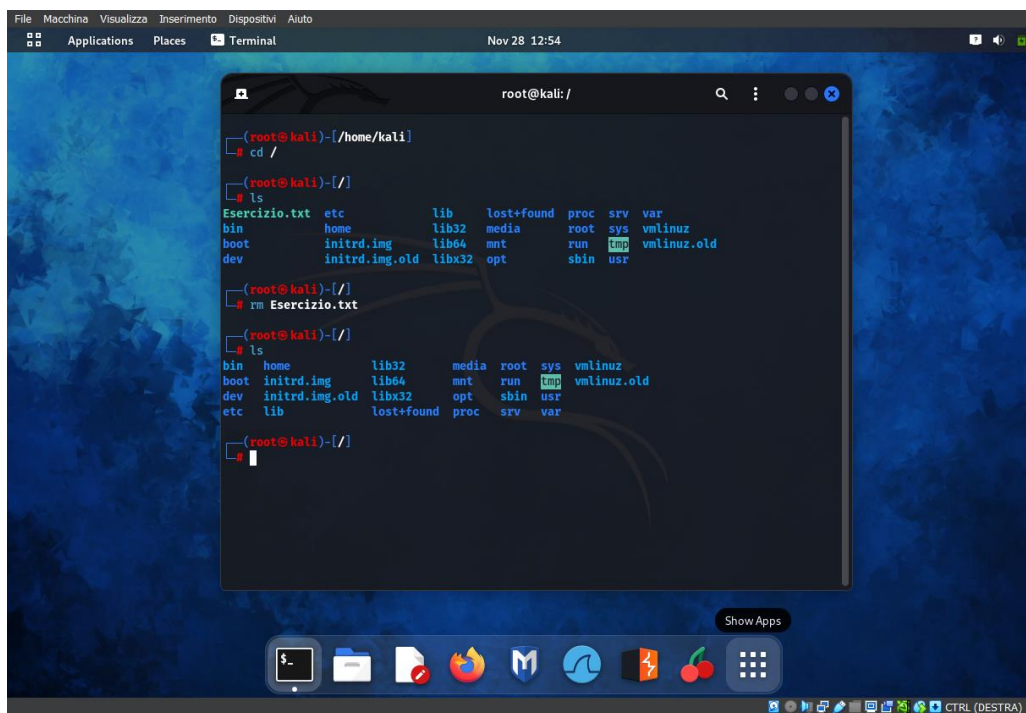
```
root@kali: /  
(root@kali)-[/]  
$ chmod o+r Esercizio.txt  
(root@kali)-[/]  
$ ls -la  
total 84  
drwxr-xr-x 19 root root 4096 Nov 28 12:34 .  
drwxr-xr-x 19 root root 4096 Nov 28 12:34 ..  
drwx----- 2 root root 4096 Nov 20 15:38 .cache  
-rwxrwxrwx 1 kali kali 32 Nov 28 11:58 Esercizio.txt  
lrwxrwxrwx 1 root root 7 Nov 20 15:06 bin -> usr/bin  
drwxr-xr-x 3 root root 4096 Nov 20 15:53 boot  
drwxr-xr-x 18 root root 3320 Nov 28 11:32 dev  
drwxr-xr-x 191 root root 12288 Nov 28 12:16 etc  
drwxr-xr-x 3 root root 4096 Nov 20 15:50 home  
lrwxrwxrwx 1 root root 33 Nov 20 15:07 initrd.img -> boot/initrd.img-6.3.0-kali1-amd64  
lrwxrwxrwx 1 root root 33 Nov 20 15:07 initrd.img.old -> boot/initrd.img-6.3.0-kali1-amd64  
lrwxrwxrwx 1 root root 7 Nov 20 15:06 lib -> usr/lib  
lrwxrwxrwx 1 root root 9 Nov 20 15:06 lib32 -> usr/lib32  
lrwxrwxrwx 1 root root 9 Nov 20 15:06 lib64 -> usr/lib64
```



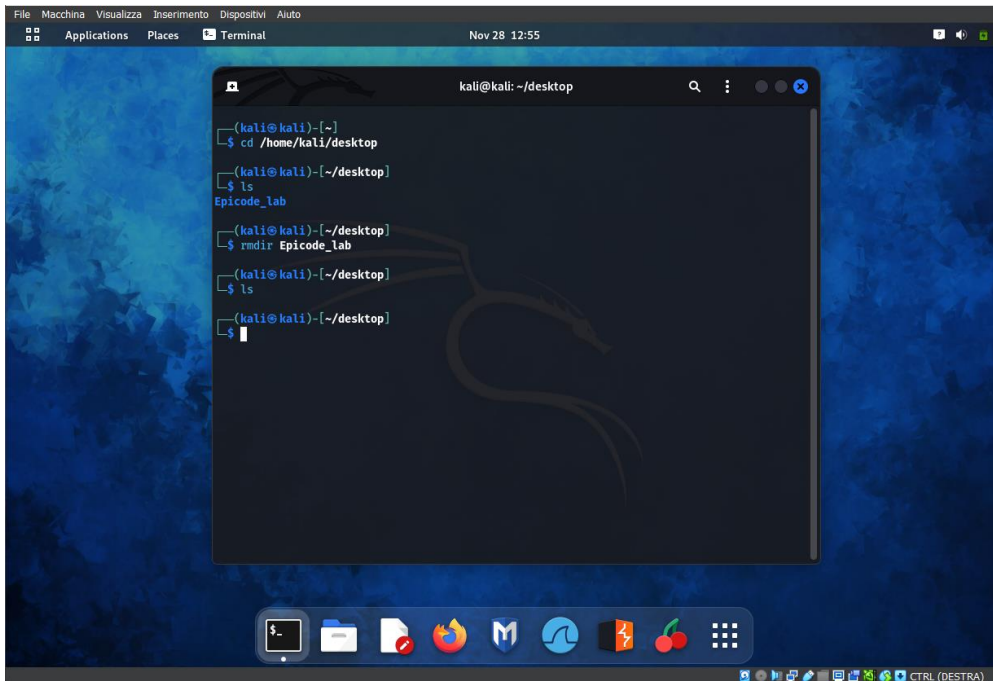
Ripristino dello Scenario Iniziale

Infine, abbiamo rimosso il file, la cartella e l'utente creato, riportando lo scenario allo stato iniziale.

Per prima torniamo con l'utente principale, accediamo a **root** ed andando nella directory **root "/"** eliminiamo il file **Esercizio.txt** precedentemente creato.

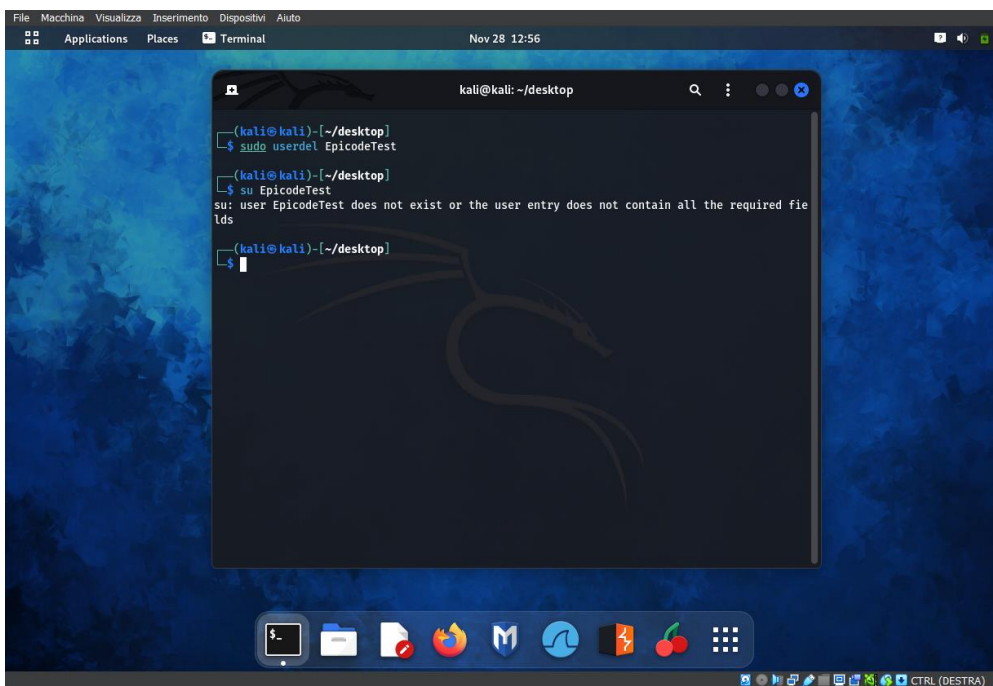


Abbiamo eliminato la cartella **Epicode_lab** con il comando “`rmdir Epicode_lab`”



```
(kali@kali)-[~]
└─$ cd /home/kali/desktop
(kali@kali)-[~/desktop]
└─$ ls
Epicode_lab
(kali@kali)-[~/desktop]
└─$ rmdir Epicode_lab
(kali@kali)-[~/desktop]
└─$ ls
(kali@kali)-[~/desktop]
└─$
```

Ed infine abbiamo rimosso il nuovo utente **EpicodeTest** con il comando “`sudo userdel EpicodeTest`”.



```
(kali@kali)-[~/desktop]
└─$ sudo userdel EpicodeTest
(kali@kali)-[~/desktop]
└─$ su EpicodeTest
su: user EpicodeTest does not exist or the user entry does not contain all the required fields
(kali@kali)-[~/desktop]
└─$
```

Conclusioni:

1. L'utilizzo del comando `top` ci ha fornito una panoramica dettagliata dei processi attivi sulla macchina.

2. Il filtraggio dei processi mediante l'uso di `grep` è un metodo efficace per isolare informazioni specifiche, come i processi associati agli utenti "root" e "kali".
3. La gestione dei permessi attraverso `chmod` è cruciale per garantire la sicurezza e il controllo dell'accesso ai file, fornendo livelli di autorizzazione specifici a utenti, gruppi e altri.
4. La creazione di un nuovo utente con `useradd` e l'assegnazione di una password tramite `passwd` sono operazioni standard per la gestione degli account utente in un sistema Linux.

L'esercizio ha fornito una pratica comprensione delle operazioni di base su Linux, dal monitorare i processi, all'amministrazione dei file e degli utenti. La corretta gestione dei permessi è un aspetto critico per garantire la sicurezza del sistema. L'esperienza acquisita in questo contesto può essere d'aiuto se applicata in scenari più complessi (tipo quelli aziendali) per la gestione avanzata di sistemi Linux.