Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Distribuzioni Linux per il PenTesting e Fondamenti di Linux
Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Comandi di Base

Proprietà dei File – Permessi dei File

- In Linux per **ciascun file** i permessi sono assegnati in base a **tre categorie di utenti**
  - **Owner:** I permessi si applicano solo al proprietario del file e non riguardano gli altri utenti
  - **Group:** I permessi si applicano solo agli utenti appartenenti al gruppo associato al file e non riguardano gli altri utenti
  - **All Users/Others:** I permessi si applicano a tutti gli utenti del sistema che non rientrano nelle altre due categorie

Comandi di Base

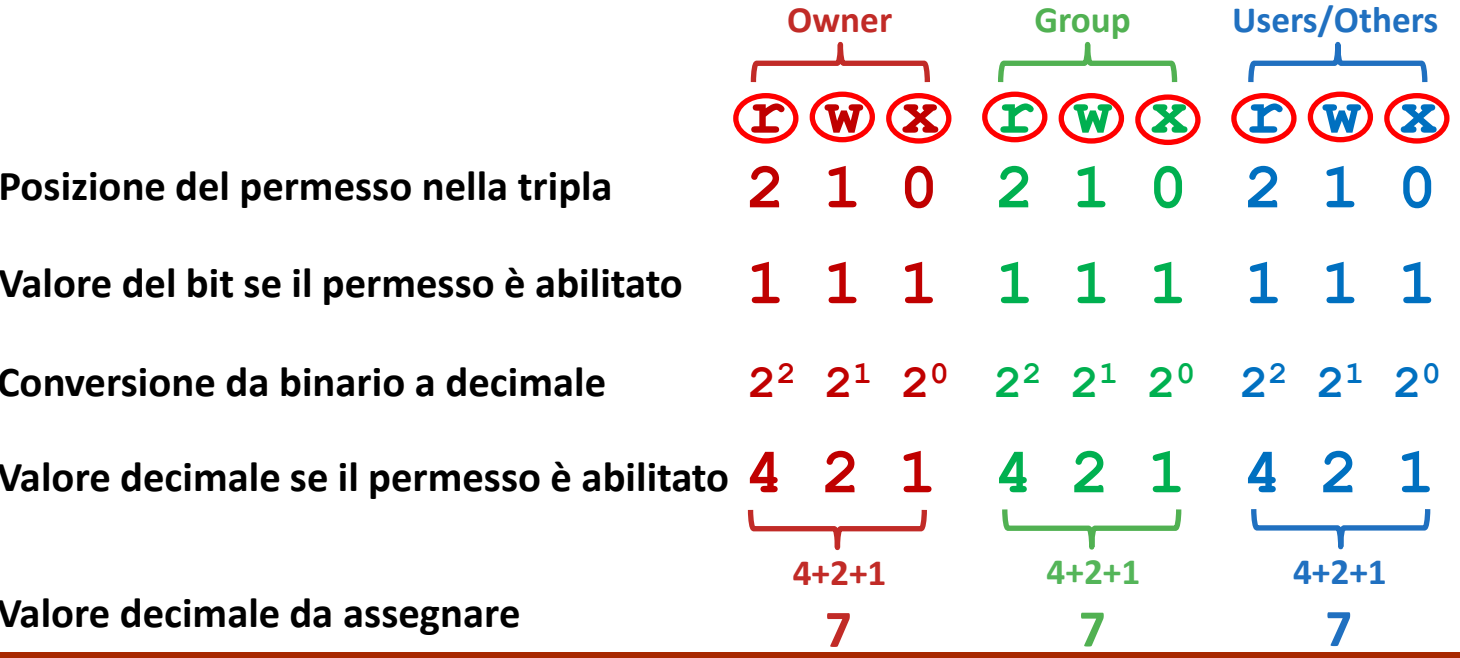
Proprietà dei File – Permessi dei File

- A **ciascuna categoria** di utenti (**Owner**, **Group**, **Others**) sono assegnati tre tipi di permessi (***tripla di permessi***)
  - **Read (`r`):** L'utente può **leggere** i contenuti di un file
  - **Write (`w`):** L'utente può **scrivere** o **modificare** un file
  - **Execute (`x`):** L'utente può **eseguire** un file

Comandi di Base

Proprietà dei File – Permessi dei File

- La **tripla di permessi** è assegnata a ciascuna categoria di utenti tramite un **valore numerico decimale**, basandosi sulla ***Notazione Posizionale***
  - Permesso **ABILITATO** -> **1** in binario
  - Permesso **DISABILITATO** -> **0** in binario



Comandi di Base

Proprietà dei File – Permessi dei File – Esempio 1

- **OWNER**: **tutti** i **permessi abilitati**
  - **`rwx`** → Binario **111** → Decimale 4+2+1 = **7**
- **GROUP**: **abilitati** i **permessi** di **lettura** (**`r`**) e di **scrittura** (**`w`**) ma non quello di esecuzione (**`x`**)
  - **`rw-`** → Binario **110** → Decimale 4+2+0 = **6**
- **OTHERS**: **abilitato** solo il **permesso** di **scrittura** (**`r`**)
  - **`r--`** → Binario **100** → Decimale 4+0+0 = **4**

`rwxrw-r--` → 764

Comandi di Base

Proprietà dei File – Permessi dei File – Esempio 2

- `rwxrw-rw-` → 766
- `rwxrwxrwx` → 777
- `rwx------` → 700

Comandi di Base

Proprietà dei File – Permessi dei File – Esempio 3

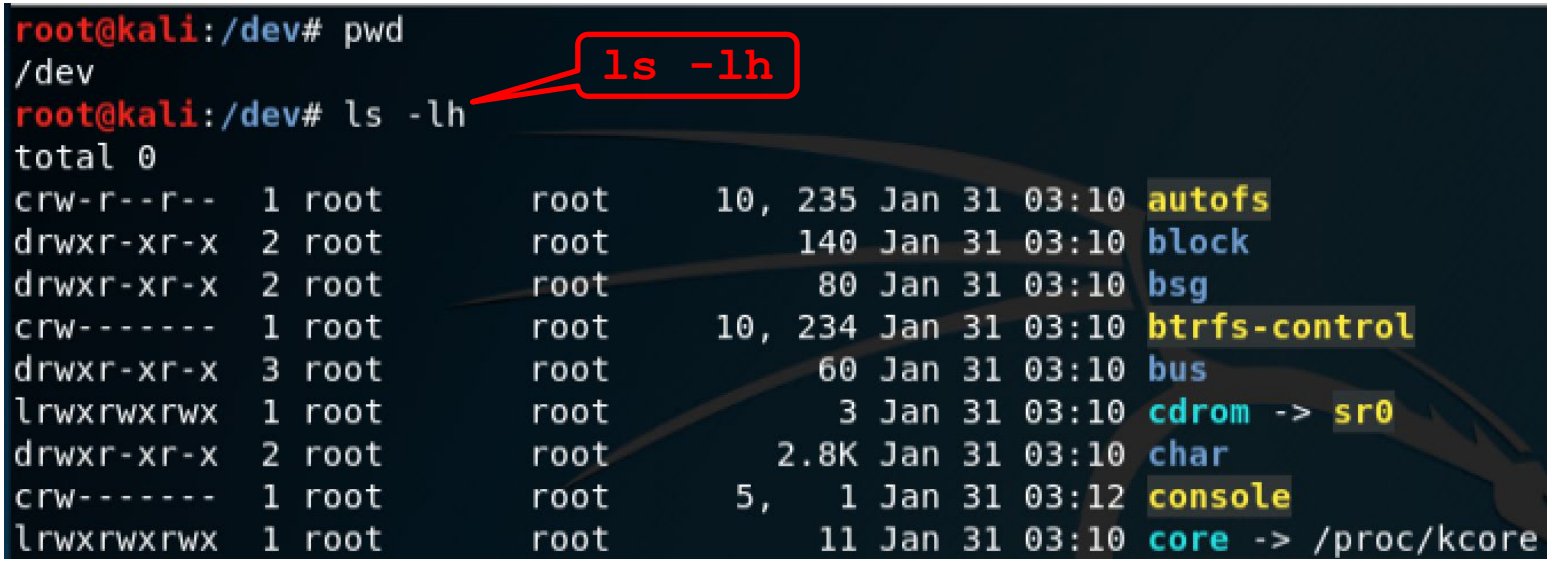
Tipo di File	Permessi del Proprietario	Permessi del Gruppo	Permessi degli Altri	Cosa verrà mostrato	Valore decimale
-	rw-	rw-	r--	-rw-rw-r--	664
d	r--	r--	r--	dr--r--r--	444
l	rwx	rwx	rwx	lrwxrwxrwx	777
s	rwx	r-x	r-x	srwxr-xr-x	755
b	rw-	rw-	---	brw-rw----	660
c	rw-	-w-	---	crw--w----	620

- **-** → Regular file **d** → Directory **l** → Link
- **s** → Socket **b** → Block Device **c** → Character Device

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file



`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Tipologia di file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Permessi associati al file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Numero di hard link

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Utente proprietario del file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Gruppo associato al file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Dimensione del file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Ultima modifica al file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base

Proprietà dei File

- Mediante il comando **`ls`** è possibile visualizzare le proprietà dei file

```
root@kali:/dev# pwd
/dev
root@kali:/dev# ls -lh
total 0
crw-r--r--  1 root       root     10, 235 Jan 31 03:10 autofs
drwxr-xr-x  2 root       root         140 Jan 31 03:10 block
drwxr-xr-x  2 root       root          80 Jan 31 03:10 bsg
crw-------  1 root       root     10, 234 Jan 31 03:10 btrfs-control
drwxr-xr-x  3 root       root          60 Jan 31 03:10 bus
lrwxrwxrwx  1 root       root           3 Jan 31 03:10 cdrom -> sr0
drwxr-xr-x  2 root       root        2.8K Jan 31 03:10 char
crw-------  1 root       root      5,   1 Jan 31 03:12 console
lrwxrwxrwx  1 root       root          11 Jan 31 03:10 core -> /proc/kcore
```

Nome del file

`man ls` (Per avere maggiori informazioni sul comando)

Comandi di Base
Modificare i Permessi dei File

- I principali comandi per modificare i permessi associati ad un file sono i seguenti
  - **`chmod`** Permette di cambiare i permessi di un file
  - **`chown`** Permette di cambiare il proprietario di un file
  - **`chgrp`** Permette di cambiare il gruppo di appartenenza di un file

Per maggiori informazioni su tali comandi, utilizzare **`man nomecomando`**

Comandi di Base

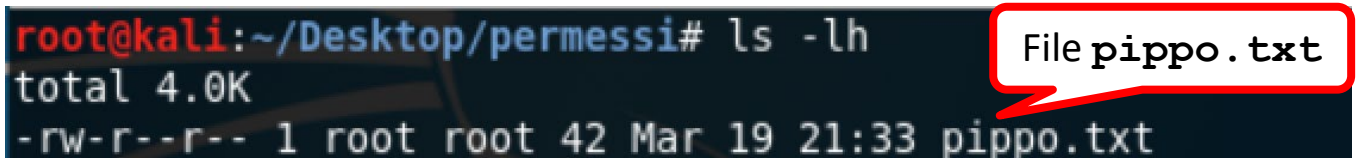
Modificare i Permessi dei File – Esempio 1

```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

Regular file

Comandi di Base

Modificare i Permessi dei File – Esempio 1



Comandi di Base

Modificare i Permessi dei File – Esempio 1

Comandi di Base

Modificare i Permessi dei File – Esempio 1

Comandi di Base

Modificare i Permessi dei File – Esempio 1

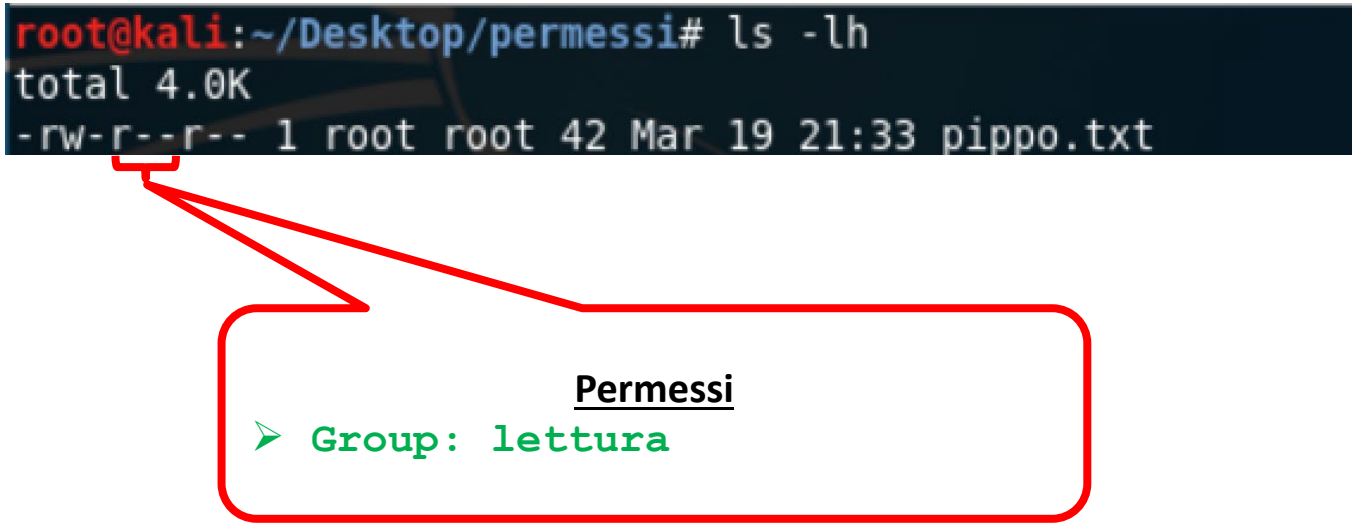
```
root@kali:~/Desktop/permessi# ls -lh
total 4.0K
-rw-r--r-- 1 root root 42 Mar 19 21:33 pippo.txt
```

Permessi

- **Owner: lettura e scrittura**

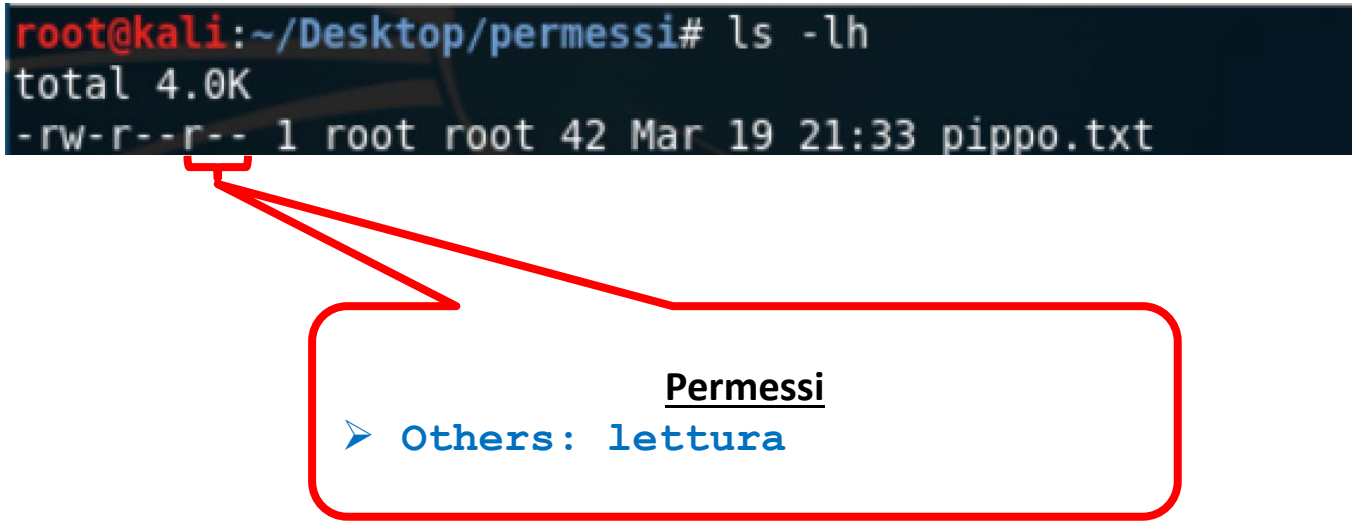
Comandi di Base

Modificare i Permessi dei File – Esempio 1



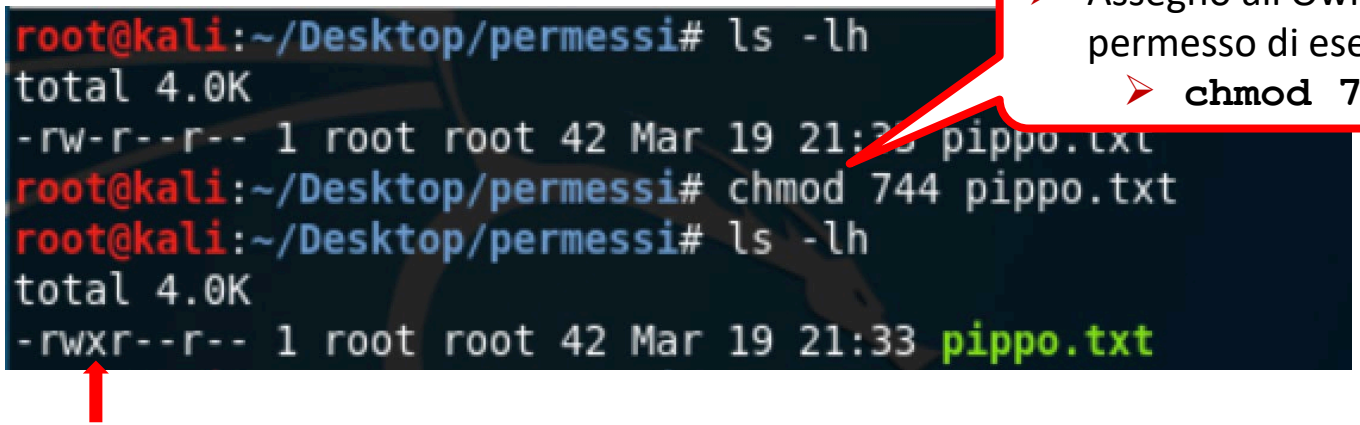
Comandi di Base

Modificare i Permessi dei File – Esempio 1



Comandi di Base

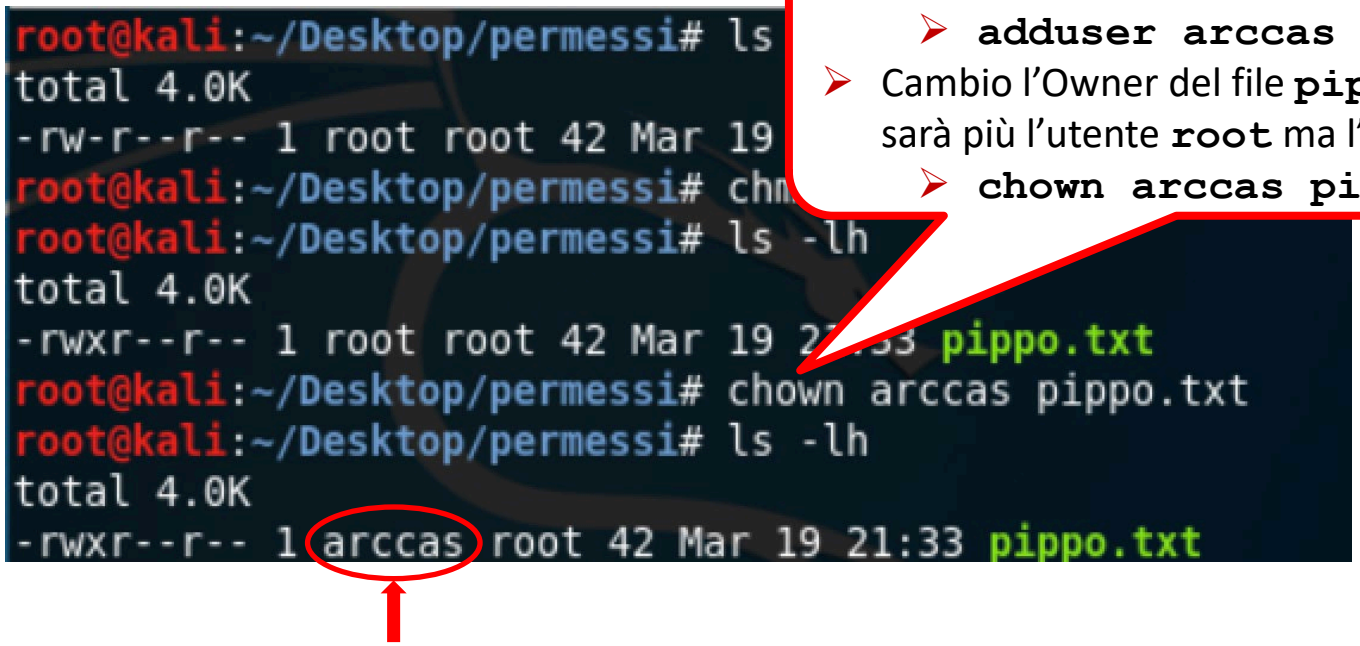
Modificare i Permessi dei File – Esempio 1



- Assegno all'Owner anche il permesso di esecuzione
  - **`chmod 744 pippo.txt`**

Comandi di Base

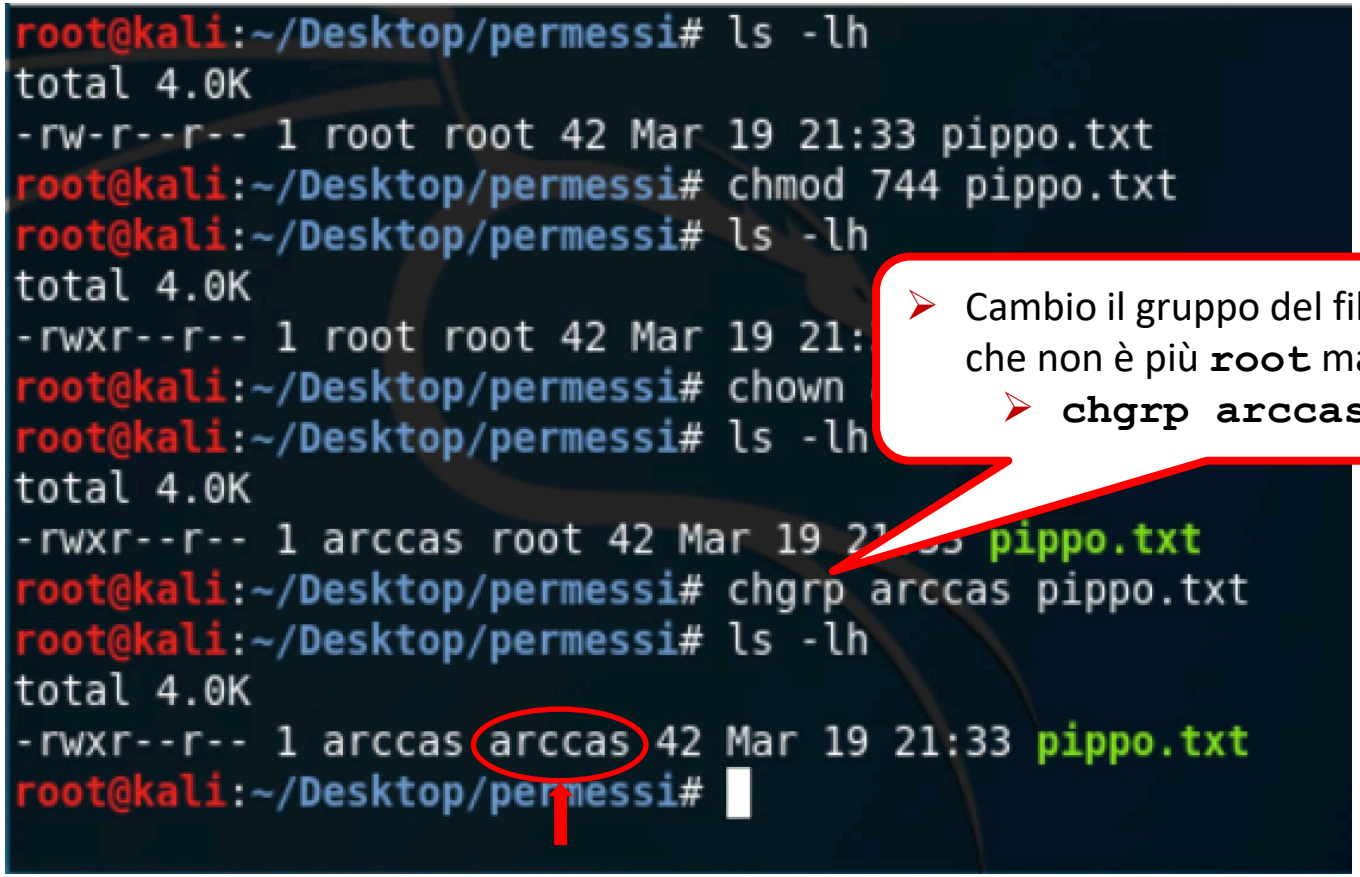
Modificare i Permessi dei File – Esempio 2



- Creo un nuovo utente di sistema (**arccas**)
  - **adduser arccas**
- Cambio l'Owner del file **pippo.txt**, che non sarà più l'utente **root** ma l'utente **arccas**
  - **chown arccas pippo.txt**

Comandi di Base

Modificare i Permessi dei File – Esempio 3



- Cambio il gruppo del file **`pippo.txt`**, che non è più **`root`** ma **`arccas`**
  - **`chgrp arccas pippo.txt`**

Comandi di Base

Processi

- Mediante il comando **ps** è possibile visualizzare i processi in esecuzione

man ps (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Utente proprietario del processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Process ID (PID)

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Percentuale di CPU utilizzata dal processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Rapporto tra la quantità di memoria utilizzata dal processo e la memoria fisica disponibile sulla macchina

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Virtual Memory Size (VSZ): Memoria virtuale che un processo può usare

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Resident Set Size (RSS): memoria fisica («non swapped») che un processo ha usato

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

TeleTYpewrite (TTY) Terminal che controlla il processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Status e priorità del processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Ora di inizio o data del processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

Tempo di utilizzo totale della CPU

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi

- Mediante il comando **`ps`** è possibile visualizzare i processi in esecuzione

```
root@kali:/dev# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4 182380  9028 ?        Ss   03:10   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S    03:10   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   03:10   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   03:10   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   03:10   0:00 [mm_percpu_wq]
```

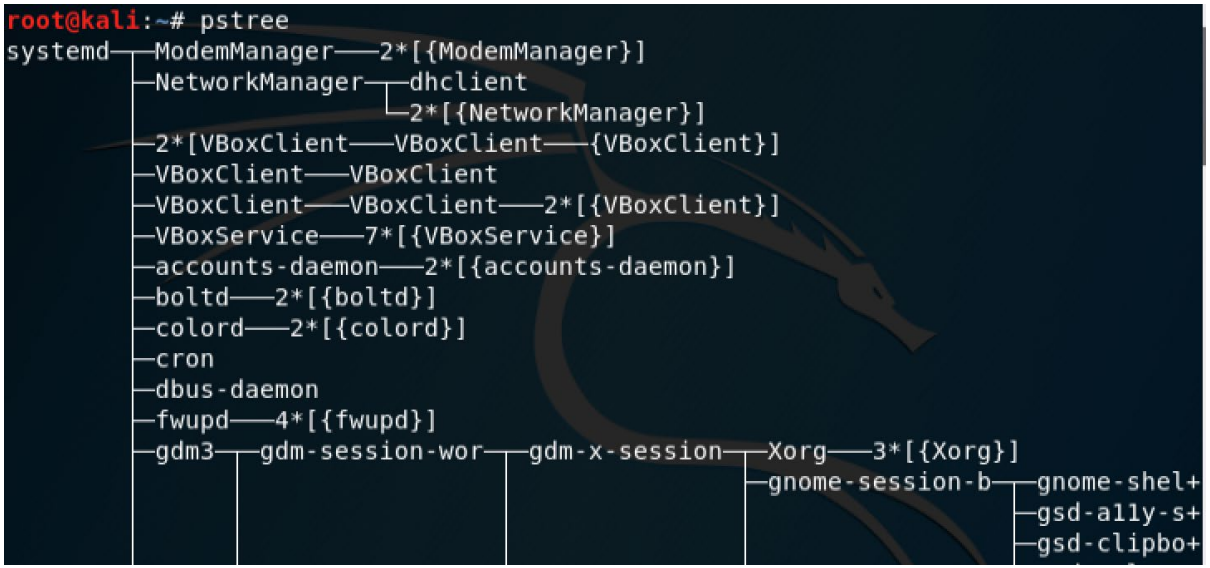
Nome del processo

`man ps` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi – Visualizzazione ad Albero

- Mediante il comando **`pstree`** è possibile visualizzare l'«albero dei processi» in esecuzione



`man pstree` (Per avere maggiori informazioni sul comando)

Comandi di Base

Processi – Invio di Segnali

- Mediante il comando **`kill`** è possibile inviare un **segnale** ad un processo specificando il *Process ID (PID)* di tale processo

```
KILL(1)                          User Commands                          KILL(1)

NAME
       kill - send a signal to a process

SYNOPSIS
       kill [options] <pid> [...]

DESCRIPTION
       The  default  signal  for kill is TERM.  Use -l or -L to list available
       signals.  Particularly useful signals include  HUP,  INT,  KILL,  STOP,
       CONT,  and  0.   Alternate  signals may be specified in three ways: -9,
       -SIGKILL or -KILL.  Negative PID values may be  used  to  choose  whole
       process  groups; see the PGID column in ps command output.  A PID of -1
       is special; it indicates all processes except the kill  process  itself
       and init.
```

Comandi di Base

Processi – Invio di Segnali

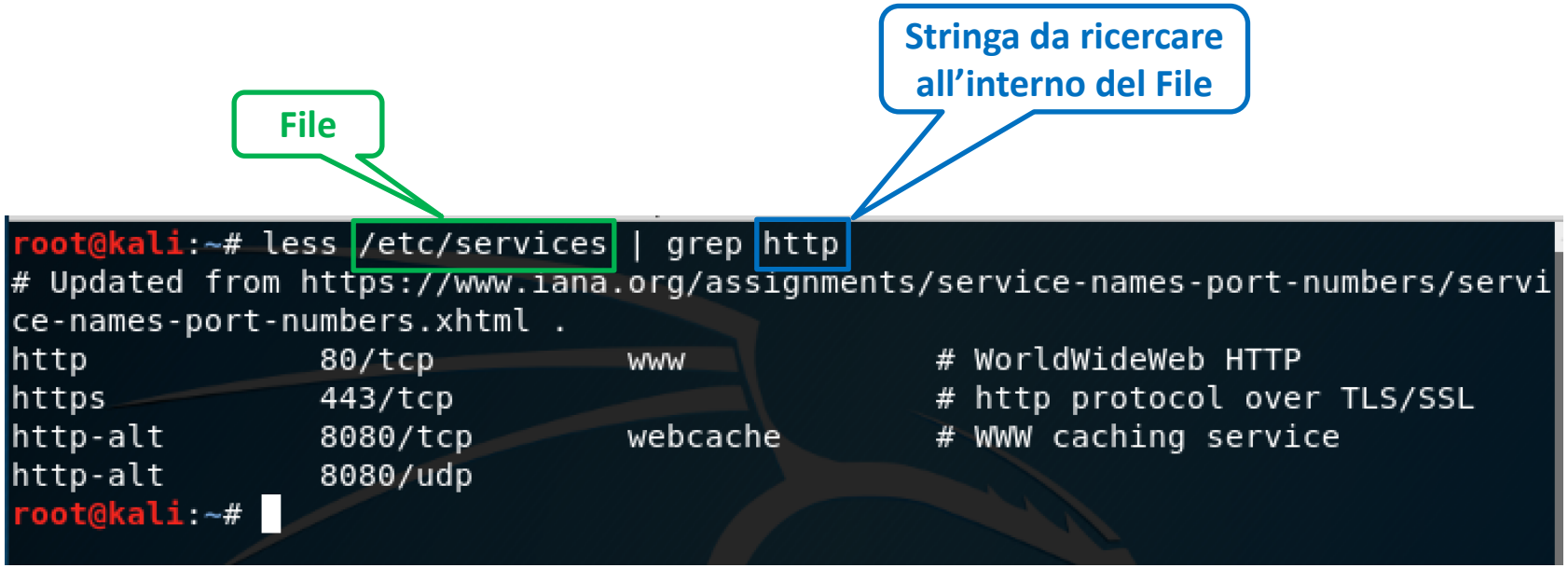
- Mediante il comando **`killall`** è possibile arrestare un processo specificando il nome di tale processo

```
KILLALL(1)                      User Commands                      KILLALL(1)

NAME
       killall - kill processes by name

SYNOPSIS
       killall [-Z, --context pattern] [-e, --exact] [-g, --process-group]
       [-i, --interactive] [-n, --ns PID] [-o, --older-than TIME]
       [-q, --quiet] [-r, --regexp] [-s, --signal SIGNAL, -SIGNAL] [-u, --user
       user] [-v, --verbose] [-w, --wait] [-y, --younger-than TIME] [-I, --ig-
       nore-case] [-V, --version] [--] name ...
       killall -l
       killall -V, --version

DESCRIPTION
       killall  sends  a  signal to all processes running any of the specified
       commands.  If no signal name is specified, SIGTERM is sent.

       Signals can be specified either by name (e.g.  -HUP or -SIGHUP)  or  by
       number (e.g.  -1) or by option -s.

       If  the command name is not regular expression (option -r) and contains
       a slash (/), processes executing that particular file will be  selected
```

Comandi di Base

Ricerca di Stringhe nei File – Esempio

- Ricerca di stringhe all'interno di file
  - Comando **`grep`**



Esempio

Comandi di Base

Ricerca di Stringhe nei File – Esempio

- Ricerca di stringhe all'interno di file
  - Comando **`grep`**

- Il comando **`less`** permette di leggere un file
  - Per maggiori informazioni **`man less`**

- L'operatore **|** è detto **pipe** e permette di inviare informazioni tra processi
  - L'output del processo a sinistra della pipe diventa input di quello a destra

```
root@kali:~# less /etc/services | grep http
# Updated from https://www.iana.org/assignments/service-names-port-numbers/servi
ce-names-port-numbers.xhtml .
http            80/tcp          www             # WorldWideWeb HTTP
https           443/tcp                         # http protocol over TLS/SSL
http-alt        8080/tcp        webcache        # WWW caching service
http-alt        8080/udp
root@kali:~#
```

Esempio

Comandi di Base

Ricerca di Stringhe nei File – Esempio

- Ricerca di stringhe all'interno di file
  - Comando **grep**

- Il comando **less** permette di leggere un file
  - Per maggiori informazioni **man less**

- Il comando **grep** stampa le linee di un file contenenti la stringa o il pattern cercato
  - Per maggiori informazioni **man grep**

```
root@kali:~# less /etc/services | grep http
# Updated from https://www.iana.org/assignments/service-names-port-numbers/servi
ce-names-port-numbers.xhtml .
http            80/tcp          www             # WorldWideWeb HTTP
https           443/tcp                         # http protocol over TLS/SSL
http-alt        8080/tcp        webcache        # WWW caching service
http-alt        8080/udp
root@kali:~#
```

Esempio

Comandi di Base

Ricerca di File

- Comando **`locate`**
  - Prima di eseguire il comando è necessario aggiornare il database di sistema su cui tale comando andrà ad effettuare la ricerca
    - Comando **`updatedb`**

- **Esempio**
  - **`updatedb`**
  - **`locate named.conf`**

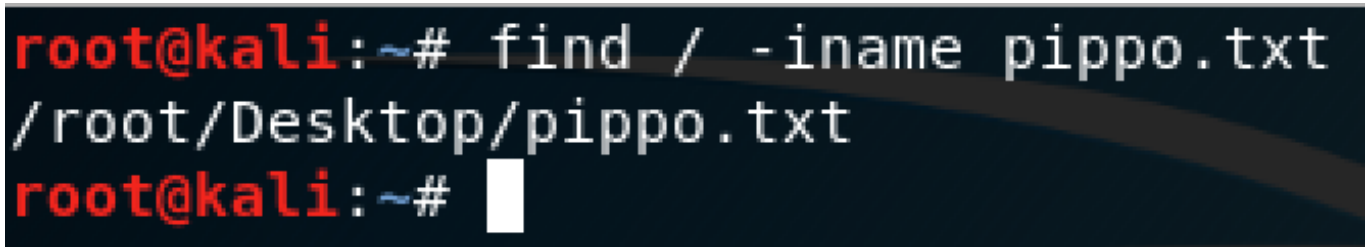
```
root@kali:~# updatedb
root@kali:~# locate named.conf
/usr/share/samba/setup/named.conf
/usr/share/samba/setup/named.conf.dlz
/usr/share/samba/setup/named.conf.update
root@kali:~#
```

Comandi di Base

Ricerca di File

- Comando **`find`**

- **Esempio**
  - **`find / -iname pippo.txt`**

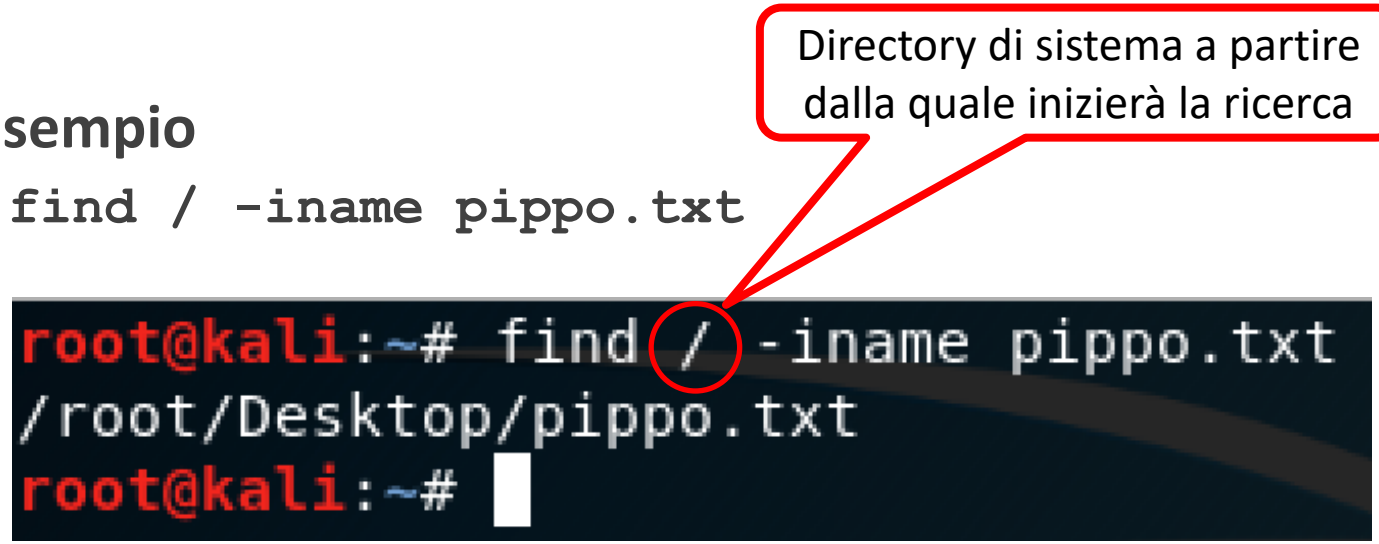


Comandi di Base

Ricerca di File

- Comando **`find`**

- **Esempio**
  - `find / -iname pippo.txt`



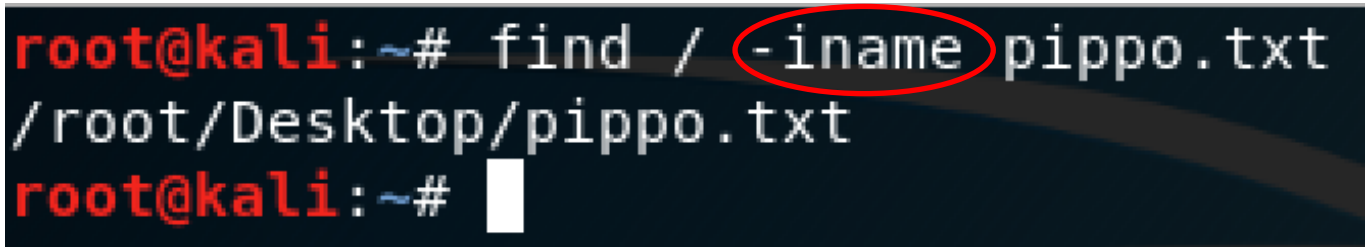
Comandi di Base

Ricerca di File

- Comando **`find`**

- **Esempio**
  - `find / -iname pippo.txt`

La ricerca avviene in maniera **case insensitive**

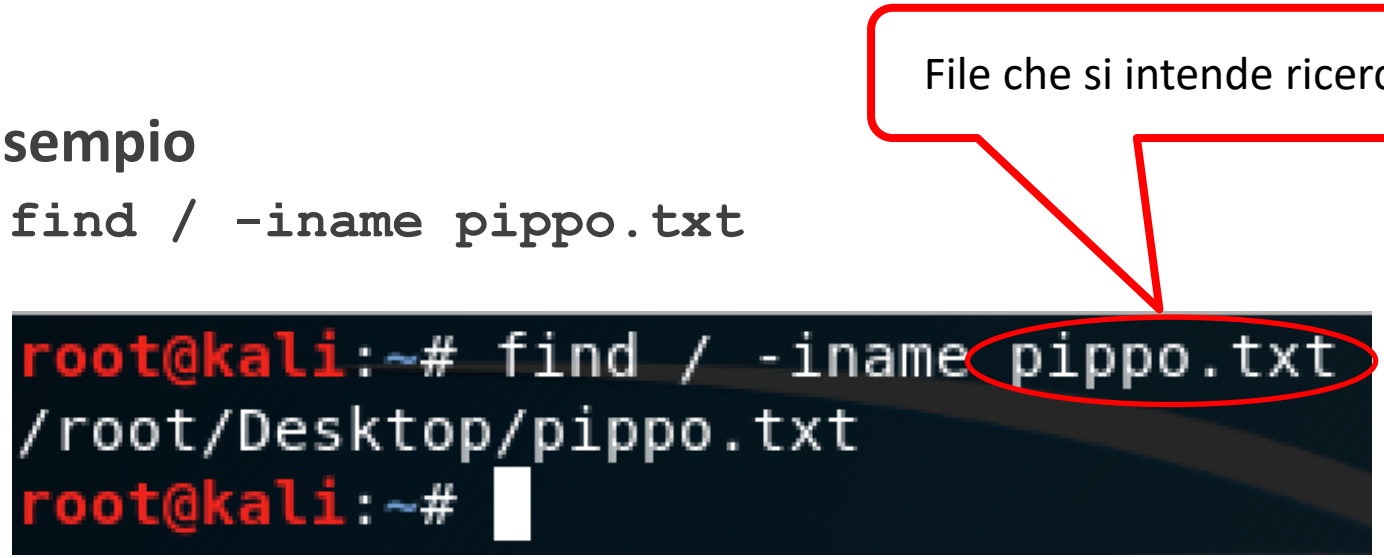


Comandi di Base

Ricerca di File

- Comando **`find`**

- **Esempio**
  - `find / -iname pippo.txt`



Comandi di Base

Ricerca di File Eseguibili e Man Page

- Mediante il comando **`whereis`** è possibile effettuare la ricerca di un file eseguibile (comando di sistema) e della relativa *man page*

- **Esempio**
  - **`whereis dd`**

```
root@kali:~# whereis dd
dd: /usr/bin/dd /usr/share/man/man1/dd.1.gz
root@kali:~#
```

Comandi di Base

Informazioni sul Sistema

- Il comando **`uptime`** fornisce informazioni sull'*uptime* del sistema

```
root@kali:~# uptime
 17:54:57 up 38 min,  1 user,  load average: 0.15, 0.04, 0.01
root@kali:~#
```

- I comandi **`date`** ed **`ncal`** forniscono informazioni su data, ora e calendario di sistema

```
┌──(root㉿kali)-[~]
└─# ncal
     March 2022
Su      6 13 20 27
Mo      7 14 21 28
Tu  1   8 15 22 29
We  2   9 16 23 30
Th  3 10 17 24 31
Fr  4 11 18 25
Sa  5 12 19 26
```

Comandi di Base

Informazioni sul Sistema

- Il comando **w** fornisce informazioni sugli utenti connessi al sistema

```
root@kali:~# w
 17:58:35 up 42 min,  1 user,  load average: 0.08, 0.03, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     :1       :1               17:16   ?xdm?  14.56s  0.00s /usr/lib/gdm3/g
root@kali:~#
```

- Il comando **finger** fornisce informazioni su un determinato utente registrato al sistema

```
root@kali:~# finger arccas
Login: arccas                           Name: Arcangelo Castiglione
Directory: /home/arccas                 Shell: /bin/bash
Never logged in.
No mail.
No Plan.
root@kali:~#
```

Comandi di Base

Informazioni sul Sistema

- Per ottenere informazioni sul processore utilizzato dal sistema
  - **`cat /proc/cpuinfo`**

```
root@kali:~# cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 70
model name      : Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz
stepping        : 1
cpu MHz         : 2793.532
cache size      : 6144 KB
physical id     : 0
siblings        : 2
core id         : 0
cpu cores       : 2
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
```

Comandi di Base

Informazioni sul Sistema

- Per ottenere informazioni sulla memoria utilizzata dal sistema
  - **`cat /proc/meminfo`**

```
root@kali:~# cat /proc/meminfo
MemTotal:        2043172 kB
MemFree:           91188 kB
MemAvailable:    1089616 kB
Buffers:          296220 kB
Cached:           736192 kB
SwapCached:           28 kB
Active:          1163244 kB
Inactive:         524292 kB
Active(anon):     598912 kB
Inactive(anon):    73696 kB
Active(file):     564332 kB
Inactive(file):   450596 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:       2095100 kB
SwapFree:        2094576 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:        653152 kB
Mapped:           200460 kB
Shmem:             17488 kB
```

Comandi di Base

Informazioni sul Sistema

- Per ottenere informazioni sul processo che ha aperto un determinato file è possibile utilizzare il comando **`lsof`**

- Fornisce numerose altre funzionalità
  - Visualizzare i file aperti da un determinato utente
  - Trovare i processi in esecuzione su una porta specifica
  - Etc

- **Esempio**
  - **`lsof /var/log/messages`**

```
root@kali:~# lsof /var/log/messages
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF   NODE NAME
rsyslogd 425 root   10w   REG    8,1  6288032 799595 /var/log/messages
```

Comandi di Base

Informazioni sul Sistema

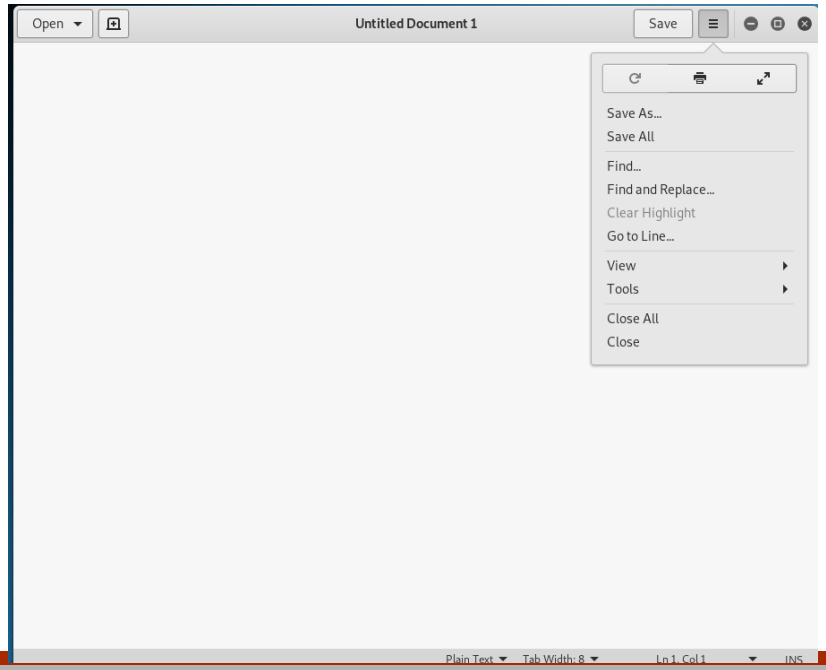
- Per ottenere informazioni sulle interfacce di rete del sistema è possibile utilizzare il comando **`ifconfig`**

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe95:8c5e  prefixlen 64  scopeid 0x20<
        ether 08:00:27:95:8c:5e  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 11059 (10.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80  bytes 9083 (8.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1356 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1356 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Comandi di Base

Editor di Testi - Gedit

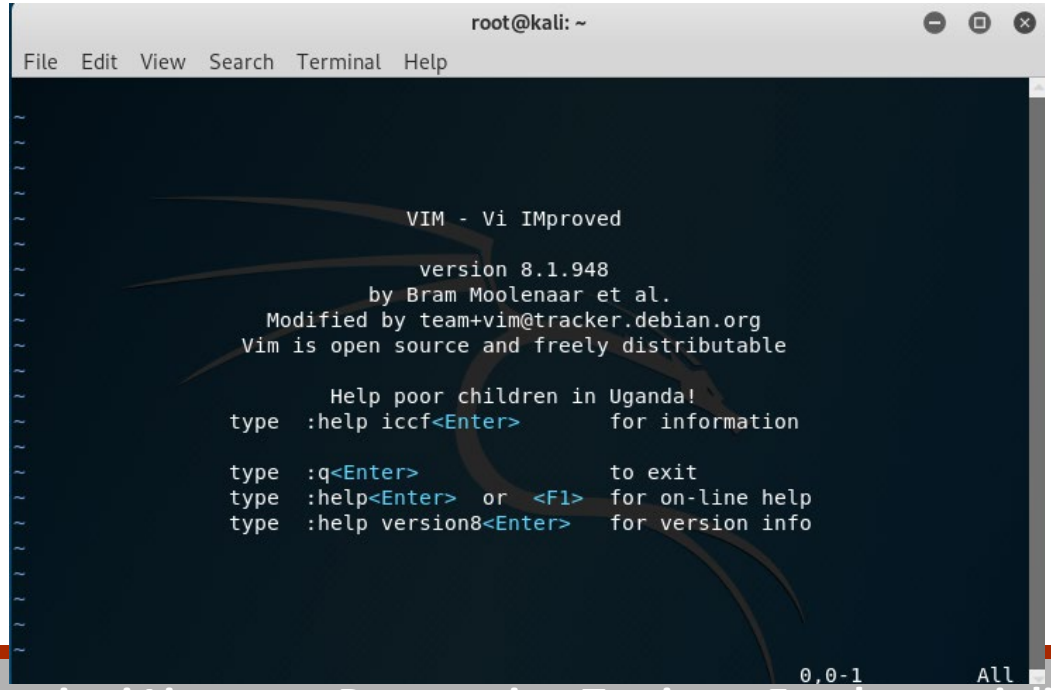
- Utile e comodo editor di testi con interfaccia grafica
- Non presente di default in Kali Linux -> **`apt-get install gedit`**
- Può essere eseguito mediante il comando **`gedit`**



Comandi di Base

Editor di Testi - vim

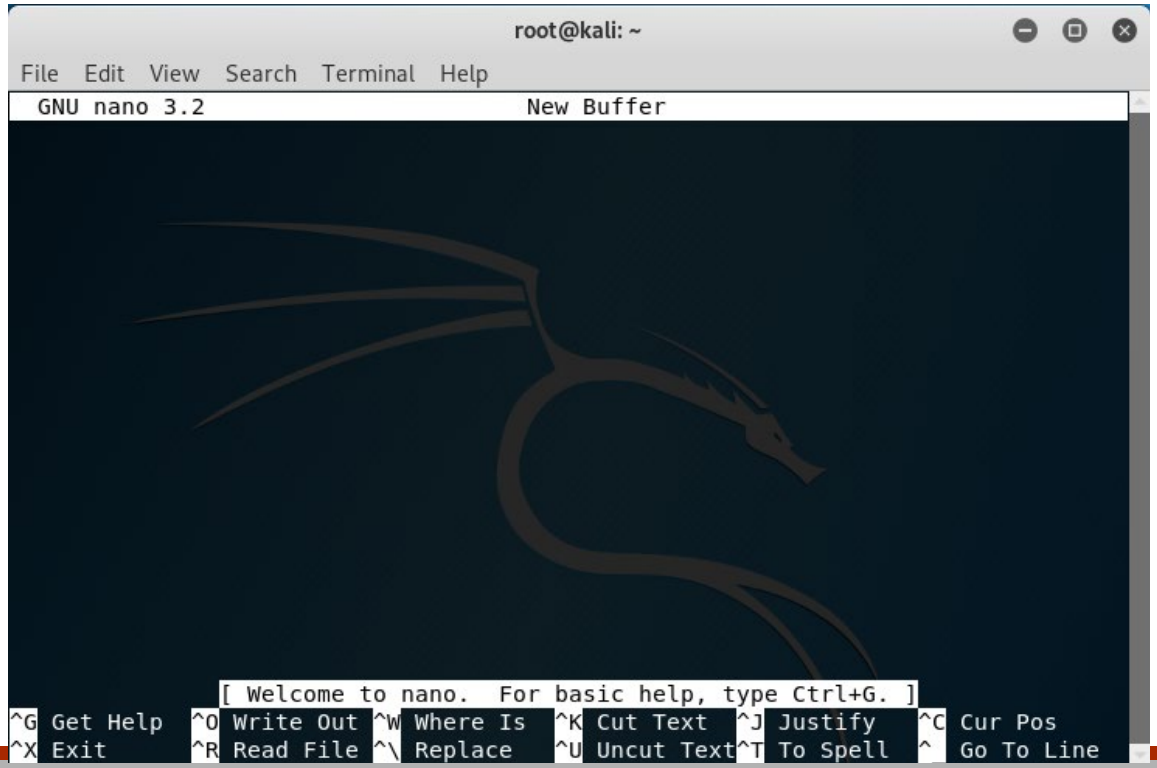
- Editor di testi senza interfaccia grafica
- Può essere eseguito mediante il comando **`vim`**
- In generale è sempre presente sui sistemi UNIX-based



Comandi di Base

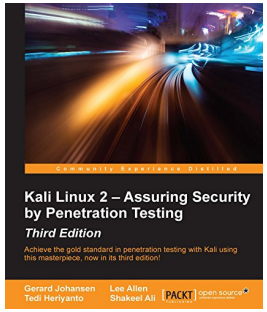
Editor di Testi - nano

- Editor di testi senza interfaccia grafica
- Può essere eseguito mediante il comando **`nano`**

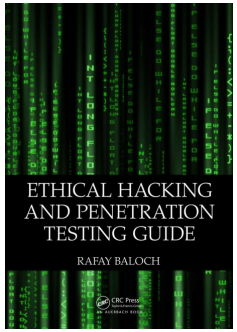


Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 1



- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 2
    - Da pagina 19 a pagina 30 (Escluso «What Is BackTrack»)
    - Da pagina 44 a pagina 47 (Fino a «Removing a File» incluso)



Bibliografia

- **Kali Linux Revealed**
  - https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf
- **Bash Guide for Beginners**
  - https://www.tldp.org/LDP/Bash-Beginners-Guide/Bash-Beginners-Guide.pdf
- **Advanced Bash-Scripting Guide**
  - https://www.tldp.org/LDP/abs/abs-guide.pdf
- **Text Processing Commands**
  - https://www.tldp.org/LDP/abs/html/textproc.html
- **Linux Commands List**
  - https://www.mediacollege.com/linux/command/linux-command.html