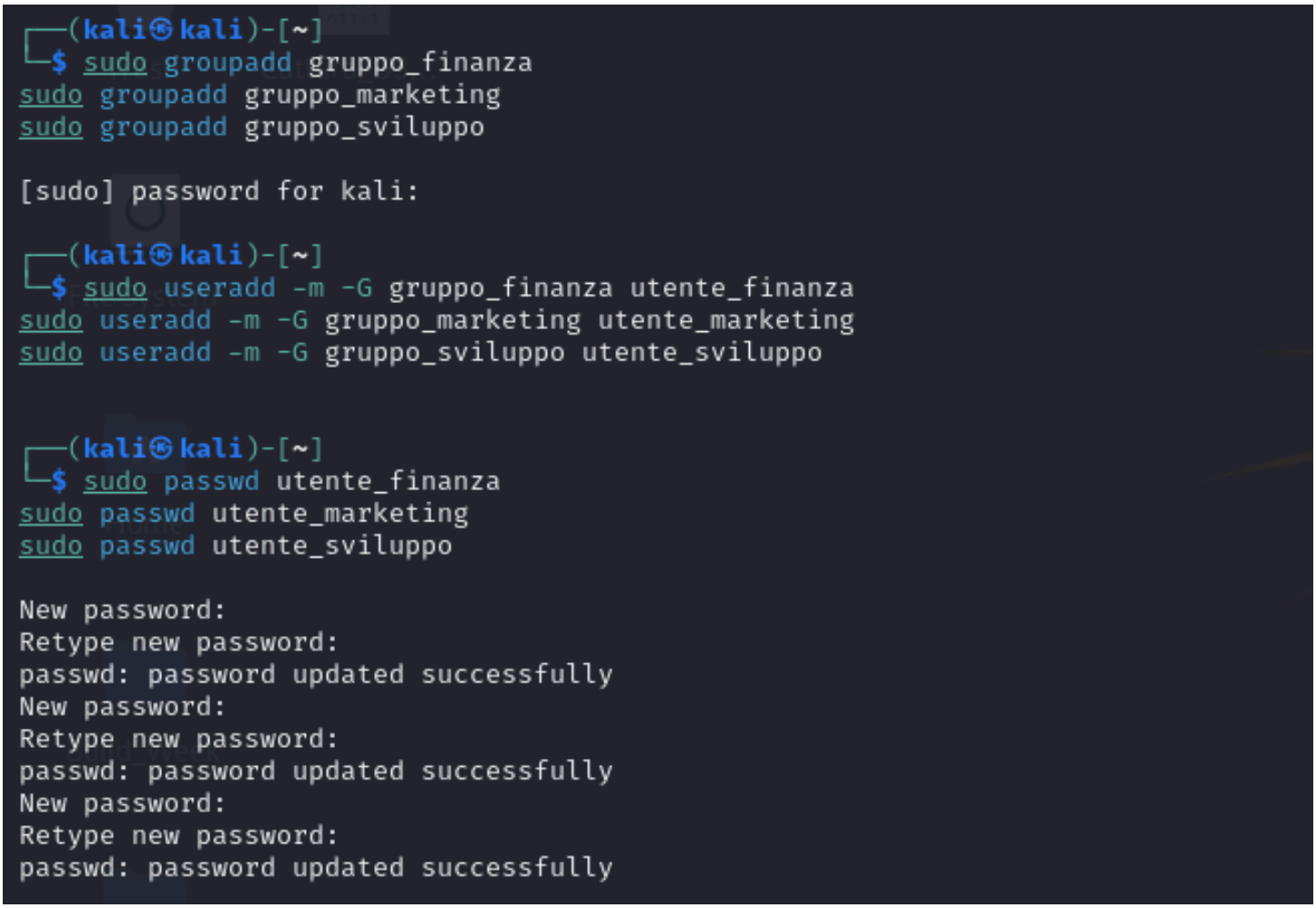
Gestione dei Permessi in un Ambiente Aziendale Linux: Creazione e Configurazione di Gruppi e Accessi

Introduzione:
In questo progetto, ho creato una struttura di directory e assegnato permessi personalizzati per un ambiente aziendale simulato su Linux. La struttura segue una logica gerarchica, con un sistema di gestione dei permessi che rispetta una struttura organizzativa tipica di un'azienda. Ogni settore (finanza, marketing, sviluppo) ha utenti e gruppi associati ai ruoli aziendali, con l'obiettivo di configurare un sistema sicuro ed efficiente per controllare l'accesso a file e cartelle in base ai permessi richiesti.
L'approccio segue una politica di gestione dei permessi basata su ruoli (RBAC).

1. **Creazione dei Gruppi e Utenti Privilegiati**

- **Gruppi principali**: Per ogni dipartimento dell'azienda, sono stati creati i gruppi principali:
  - gruppo_finanza
  - gruppo_marketing
  - gruppo_sviluppo
- **Gruppi secondari**: I gruppi secondari sono stati creati per i manager e gli employee, che si aggiungono ai gruppi principali dei rispettivi dipartimenti:
  - Manager:
    - manager_finanza, manager_marketing, manager_sviluppo
  - Employee:
    - employee_finanza, employee_marketing, employee_sviluppo
- **Utenti**:
  - **Capo dipartimento**(ha accesso completo ai file del dipartimento):
    - utente_finanza, utente_marketing, utente_sviluppo
  - **Manager**(ha permessi di lettura, scrittura ed esecuzione sui file del proprio dipartimento):
    - manager_finanza, manager_marketing, manager_sviluppo
  - **Employee**(ha permessi limitati, principalmente lettura e scrittura su file specifici):
    - employee_finanza, employee_marketing, employee_sviluppo



2. Creazione delle Directory e Gestione dei Permessi

Ogni dipartimento ha una directory dedicata sotto /azienda/progetti/, che contiene file e cartelle di lavoro.

- **Directory:**
  - /azienda/progetti/finanza
  - /azienda/progetti/marketing
  - /azienda/progetti/sviluppo

Ho configurato le directory in modo che:

- Capo dipartimento ha accesso completo (lettura, scrittura, esecuzione).
- Manager ha permessi di lettura, scrittura ed esecuzione sulle directory relative ai loro settori.
- Employee ha solo permessi di lettura e scrittura sui file, ma non sulle directory.

```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir -p /azienda/{finanza,marketing,sviluppo,documenti}


┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ sudo chown root:gruppo_finanza /azienda/finanza
sudo chmod 770 /azienda/finanza


┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ sudo chown root:gruppo_marketing /azienda/marketing
sudo chmod 770 /azienda/marketing


┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ sudo chown root:gruppo_sviluppo /azienda/sviluppo
sudo chmod 770 /azienda/sviluppo


┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ sudo chmod 775 /azienda/documenti
```

3. Gestione dei Permessi per i File

Per ogni directory, sono stati configurati i permessi per i file:

- Capo dipartimento ha accesso completo a tutti i file all'interno del proprio dipartimento.
- Manager ha permessi di lettura, scrittura ed esecuzione sui file, ma con alcune limitazioni.
- Employee può leggere e scrivere determinati file, ma non può modificare la struttura della directory o accedere a file confidenziali.

Ho utilizzato i comandi chown (per cambiare il proprietario e il gruppo di un file) e chmod (per impostare i permessi di accesso ai file) per applicare questi permessi.

```
┌──(kali㉿kali)-[~]
└─$ sudo touch /azienda/finanza/report_finanziario.txt
sudo chown root:gruppo_finanza /azienda/finanza/report_finanziario.txt
sudo chmod 660 /azienda/finanza/report_finanziario.txt


┌──(kali㉿kali)-[~]
└─$ sudo touch /azienda/marketing/relazione_marketing.txt
sudo chown root:gruppo_marketing /azienda/marketing/relazione_marketing.txt
sudo chmod 660 /azienda/marketing/relazione_marketing.txt


┌──(kali㉿kali)-[~]
└─$ sudo touch /azienda/sviluppo/codice_sviluppo.c
sudo chown root:gruppo_sviluppo /azienda/sviluppo/codice_sviluppo.c
sudo chmod 660 /azienda/sviluppo/codice_sviluppo.c


┌──(kali㉿kali)-[~]
└─$ sudo touch /azienda/documenti/documento_comune.txt
sudo chmod 664 /azienda/documenti/documento_comune.txt
```

Uso di chmod con permessi numerici

Il comando chmod in Linux permette di gestire i permessi di accesso a file e directory. I permessi sono espressi tramite numeri, dove ogni cifra rappresenta una combinazione di lettura (r), scrittura (w) ed esecuzione (x). Ogni permesso ha un valore numerico:

- **r (lettura)** = 4
- **w (scrittura)** = 2
- **x (esecuzione)** = 1

Struttura dei permessi

I permessi vengono assegnati a tre categorie:

1. **Proprietario** (1° cifra)
2. **Gruppo** (2° cifra)
3. **Altri** (3° cifra)

Ogni cifra è la somma dei permessi per quella categoria. Ad esempio:

- **rwx** (lettura, scrittura, esecuzione) = 4 + 2 + 1 = 7
- **rw-** (lettura e scrittura) = 4 + 2 = 6
- **r--** (lettura) = 4

ESEMPI:

chmod 755 file.txt:

- Proprietario: lettura + scrittura + esecuzione = **7**
- Gruppo e Altri: lettura + esecuzione = **5**
- Proprietario ha accesso completo, gli altri solo lettura ed esecuzione.

chmod 660 file.txt:

- Proprietario: lettura + scrittura + esecuzione = **7**
- Gruppo e Altri: lettura + esecuzione = **5**
- Il **proprietario** e il **gruppo** possono leggere e modificare il file.

Verifica dei permessi

```
┌──(kali㉿kali)-[~]
└─$ ls -ld /azienda/finanza /azienda/marketing /azienda/sviluppo /azienda/documenti

drwxrwxr-x 2 root root            4096 Dec  3 14:37 /azienda/documenti
drwxrwx--- 2 root gruppo_finanza  4096 Dec  3 14:37 /azienda/finanza
drwxrwx--- 2 root gruppo_marketing 4096 Dec  3 14:37 /azienda/marketing
drwxrwx--- 2 root gruppo_sviluppo 4096 Dec  3 14:37 /azienda/sviluppo

┌──(kali㉿kali)-[~]
└─$ ls -l /azienda/finanza/report_finanziario.txt /azienda/marketing/relazione_marketing.txt /azienda/sviluppo/codice_sviluppo.c /azienda/documenti/documento_comune.txt

ls: cannot access '/azienda/finanza/report_finanziario.txt': Permission denied
ls: cannot access '/azienda/marketing/relazione_marketing.txt': Permission denied
ls: cannot access '/azienda/sviluppo/codice_sviluppo.c': Permission denied
-rw-rw-r-- 1 root root 0 Dec  3 14:37 /azienda/documenti/documento_comune.txt

┌──(kali㉿kali)-[~]
└─$ sudo ls -l /azienda/finanza/report_finanziario.txt /azienda/marketing/relazione_marketing.txt /azienda/sviluppo/codice_sviluppo.c /azienda/documenti/documento_comune.txt

-rw-rw-r-- 1 root root            0 Dec  3 14:37 /azienda/documenti/documento_comune.txt
-rw-rw---- 1 root gruppo_finanza  0 Dec  3 14:37 /azienda/finanza/report_finanziario.txt
-rw-rw---- 1 root gruppo_marketing 0 Dec  3 14:37 /azienda/marketing/relazione_marketing.txt
-rw-rw---- 1 root gruppo_sviluppo 0 Dec  3 14:37 /azienda/sviluppo/codice_sviluppo.c
```

Screenshot per la creazione dei manager e employee

```
┌──(kali㉿kali)-[~]
└─$ # Creiamo i gruppi per i manager e gli employee
sudo groupadd gruppo_manager_finanza
sudo groupadd gruppo_manager_marketing
sudo groupadd gruppo_manager_sviluppo

sudo groupadd gruppo_employee_finanza
sudo groupadd gruppo_employee_marketing
sudo groupadd gruppo_employee_sviluppo

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo groupadd manager_finanza
sudo groupadd manager_marketing
sudo groupadd manager_sviluppo


┌──(kali㉿kali)-[~]
└─$ sudo useradd -m -G gruppo_finanza,manager_finanza manager_finanza
sudo useradd -m -G gruppo_marketing,manager_marketing manager_marketing
sudo useradd -m -G gruppo_sviluppo,manager_sviluppo manager_sviluppo

useradd: group manager_finanza exists - if you want to add this user to that group, use -g.
useradd: group manager_marketing exists - if you want to add this user to that group, use -g.
useradd: group manager_sviluppo exists - if you want to add this user to that group, use -g.

┌──(kali㉿kali)-[~]
└─$ # Aggiungi gli utenti ai gruppi corretti usando -G per gruppi aggiuntivi e -g per il gruppo principale
sudo useradd -m -g gruppo_finanza -G manager_finanza manager_finanza
sudo useradd -m -g gruppo_marketing -G manager_marketing manager_marketing
sudo useradd -m -g gruppo_sviluppo -G manager_sviluppo manager_sviluppo


┌──(kali㉿kali)-[~]
└─$ sudo groupadd employee_finanza
sudo groupadd employee_marketing
sudo groupadd employee_sviluppo


┌──(kali㉿kali)-[~]
└─$ # Aggiungi gli utenti "employee" ai gruppi principali dei manager e dei dipartimenti
sudo useradd -m -g manager_finanza -G gruppo_finanza,employee_finanza employee_finanza
sudo useradd -m -g manager_marketing -G gruppo_marketing,employee_marketing employee_marketing
sudo useradd -m -g manager_sviluppo -G gruppo_sviluppo,employee_sviluppo employee_sviluppo
```

5. Conclusione

La struttura che abbiamo implementato simula un ambiente aziendale completo, con una gerarchia chiara dei permessi per ogni dipartimento e per ogni livello di accesso (capo dipartimento, manager, employee). Utilizzando il sistema Linux e i comandi di gestione dei permessi, siamo riusciti a separare le funzioni aziendali e a garantire che ogni gruppo abbia accesso solo alle informazioni rilevanti per il proprio ruolo. Questo approccio ha permesso di proteggere i dati sensibili, ottimizzare l'efficienza operativa e prevenire accessi non autorizzati. La configurazione realizzata rappresenta un esempio pratico di come Linux possa essere utilizzato per gestire in modo sicuro e flessibile una struttura aziendale complessa.