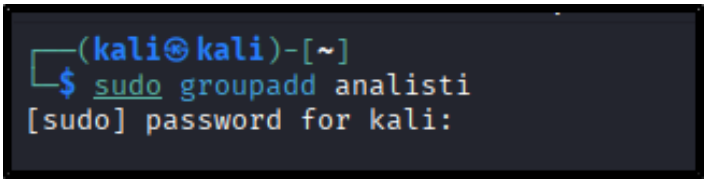
Scenario :

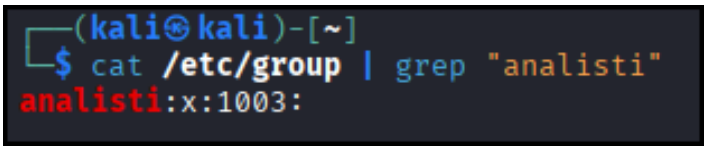
Vogliamo creare una directory `/dati/analytics` dove i membri del gruppo `analisti` possono caricare i loro file , ma non sono in grado di vedere quelli caricati da altri. Andiamo dunque a creare una cartella dove il gruppo ha i permessi di scrittura (`w`) ed esecuzione (`x`), ma non di lettura(`r`).

Configurazione

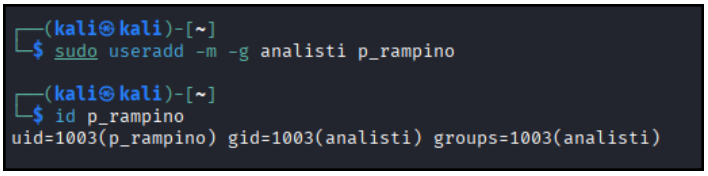
1. Andiamo a creare all'interno della nostra Kali un gruppo chiamato `analisti` attraverso il comando `sudo groupadd analisti`

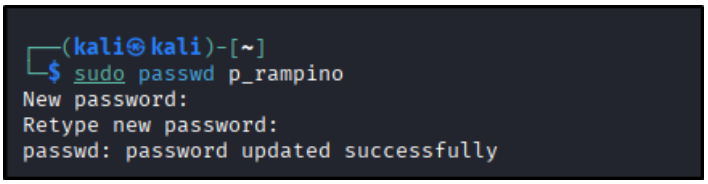
   Tramite `cat /etc/group | grep "analisti"` andiamo a confermare la presenza del gruppo appena creato

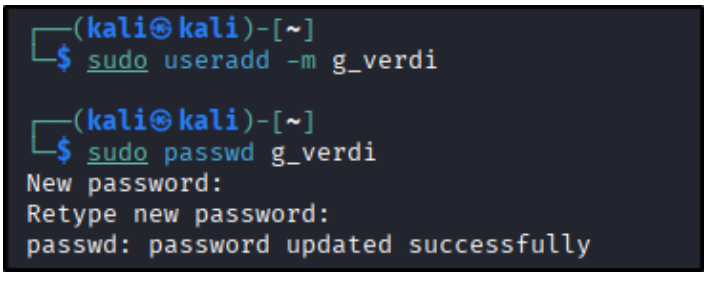
2. Andiamo a creare l'utente `"p_rampino"` e aggiungiamolo al gruppo `analisti` tramite il comando `sudo useradd -m -g analisti p_rampino`
   - `-m` Crea automaticamente la home directory dell'utente cioè `/home/p_rampino`
   - `-g` Imposta analisti come gruppo primario dell'utente cioè quando l'utente crea file o esegue operazioni, il gruppo associato sarà `analisti`

     Impostiamo la password per l'utente creato tramite `sudo passwd p_rampino`

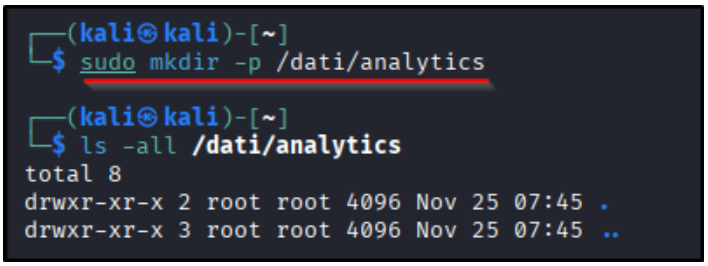
     

     Infine andiamo a creare un altro utente come fatto prima ma non lo inseriamo all'interno del gruppo

Creazione delle Directory

Andiamo a creare la nostra directory tramite `sudo mkdir -p /dati/analytics` e andiamo a controllare i permessi di default che root ha appena creato

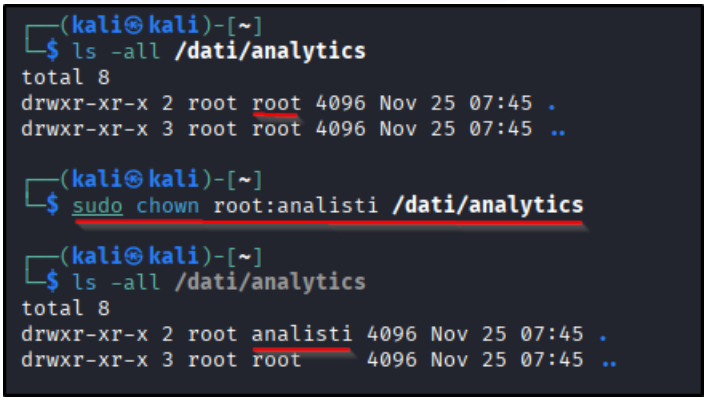


Modifica dei permessi

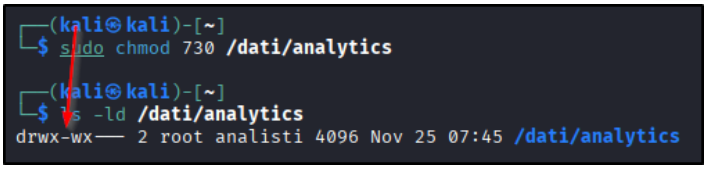
Vogliamo che :

- `Propietario` : *root* (In notazione ottale si traduce in : `r` (4)+ `w` (2) `x` (1)=7)
- `Gruppo` : *analisti* (In notazione ottale : `w` (2) + `x` (1)=3)
- `Permessi` : Vogliamo applicare `rwx` per *root* `wx` per *analisti* `---` per tutti gli altri.

1. Andiamo a cambiare il gruppo propietario della directory tramite `sudo chown root:analisti /dati/analytics`



2. Impostiamo i permessi prima spiegati tramite `sudo chmod 730 /dati/analytics`

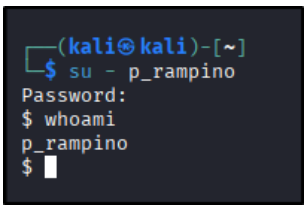


Test Permessi

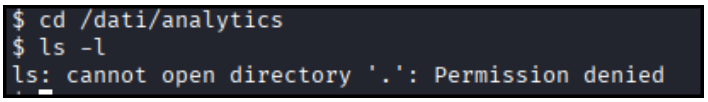
Utente : *p_rampino*

1. Andiamo a testare dapprima con l'utente nel gruppo `p_rampino`. Cambiamo utente tramite `su - p_rampino` e inseriamo la pw precedentemente impostata per tale

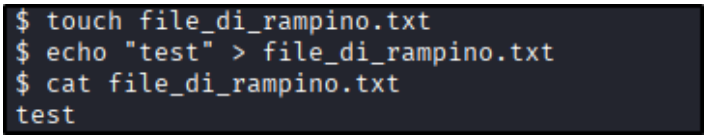
account.



2. Dopo essere entrati nella directory tramite `cd /dati/analytics` ci rendiamo subito conto di non essere in grado di listare la directory in quando non abbiamo i permessi `r`

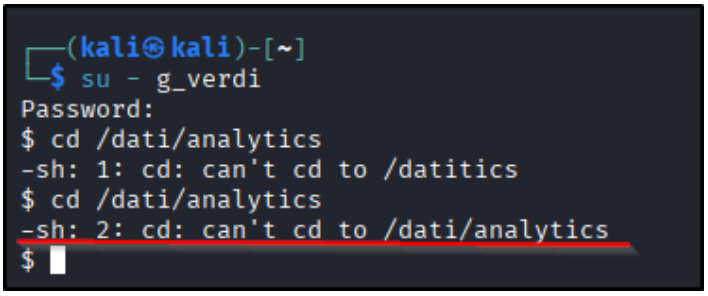


3. Proviamo ora l'operazione di creazione (che deve funzionare grazie ai permessi di `w`) e di lettura del file appena creato (che deve funzionare in quanto è il proprietario del file)



Utente : *g_verdi*

Effettuiamo lo switch dell'utente dopo essere usciti dalla console precedente tramite `su - g_verdi` e proviamo ad effettuare un cd nella cartella `/data/analytics` scopriremo subito che non possiamo effettuare questa operazione



Scelte di Configurazione

- **Creazione gruppo e utenti** : Abbiamo creato un gruppo `analisti` e due utenti test `p_rampino` e `g_verdi`
- **Proprietario** : (`chown root:analisti /dati/analytics`):
  - **Proprietario Utente** : `root` . Avere come proprietario root garantisce che solo l'amministratore possa modificare i permessi o la proprietà della cartella stessa.
  - **Proprietario Gruppo** : `analisti` Applica le regole di gruppo specifiche ai soli membri del team `analisti` .
- **Permessi** : (`chmod 730 /dati/analytics`)
  - **Proprietario** (`7 o rwx`) : `root` ha il pieno controllo per la manutenzione.
  - **Gruppo** (`3 o -wx`) : Principio fondamentale della configurazione scelta.
    - `w` (*scrittura*) : Permette ai membri del gruppo `analisti` di creare nuovi file o eliminare file propri.
    - `x` (*esecuzione*) : Senza questo permesso non si potrebbe nemmeno entrare nella directory tramite `cd`

    - `-` (*lettura mancante*) : Questa è la restrizione applicata , negando il permesso `r` , un utente del gruppo `analisti` non può usare `ls` per vedere quali altri file sono presenti
- **Altri** : (`0 o ---`): Gli utenti che non sono `root` e non sono nel gruppo `analisti` non hanno alcun permesso , massimizzando la sicurezza.

Conclusione

L'impostazione dei permessi `730` (`drwx-wx---`) e la modifica del proprietario (`chown root:analisti`) si sono rivelate efficaci nel raggiungere l'obiettivo prefissato.

L'analisi dei risultati ottenuti durante i test ha confermato la validità delle scelte fatte:

1. **Membri del Gruppo (`p_rampino`):** I test hanno dimostrato che i membri del gruppo `analisti` possono correttamente *accedere* alla directory (permesso `x`) e *creare nuovi file* (permesso `w`). Allo stesso tempo, è stato loro correttamente impedito di *listare* il contenuto (assenza del permesso `r`), proteggendo così la riservatezza dei file caricati da altri.
2. **Altri Utenti (`g_verdi`):** I tentativi di accesso da parte di utenti non autorizzati sono falliti, confermando l'efficacia dei permessi `---` per la categoria "altri".

Questo esercizio pratico ha consolidato la comprensione della distinzione critica tra i permessi `r` , `w` e `x` su una directory e ha dimostrato come la loro corretta gestione sia un pilastro fondamentale per la sicurezza dei dati e l'applicazione di policy di accesso in un ambiente multi-utente.