Gestione dei Permessi di Lettura, Scrittura ed Esecuzione in Linux

---

Executive Summary

Il presente report descrive la gestione dei permessi dei file in ambiente Linux. Attraverso l'uso della riga di comando, viene analizzato come un amministratore di sistema possa configurare e amministrare correttamente gli accessi alle risorse.

Obiettivo

Configurare e gestire i permessi di lettura, scrittura ed esecuzione per file o directory in un sistema Linux.

Strumenti Laboratorio

- **Kali:** macchina host

Fase1 – Creazione cartella e shell

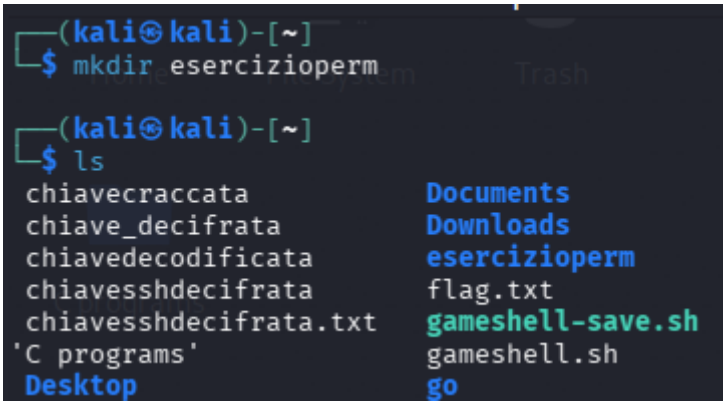

**Fig.1 Creazione cartella*

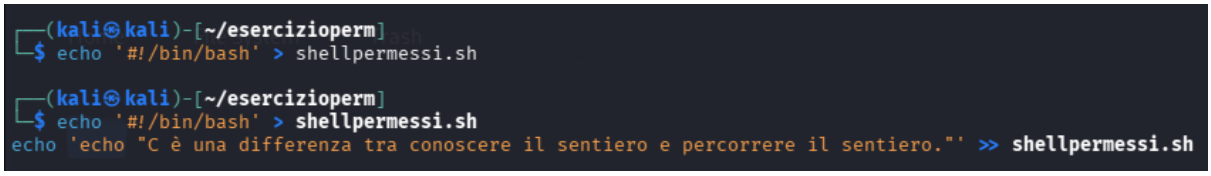

Fig.2 Creazione shell

La fase iniziale dell'esercitazione ha previsto la configurazione dell'ambiente di lavoro tramite la creazione di una directory dedicata(**`esercizioperm`**). All'interno di quest'ultima è stata generata una shell (**`shellpermessi.sh`**), utilizzato come caso studio per l'analisi dei permessi.

Fase2 – Verifica permessi

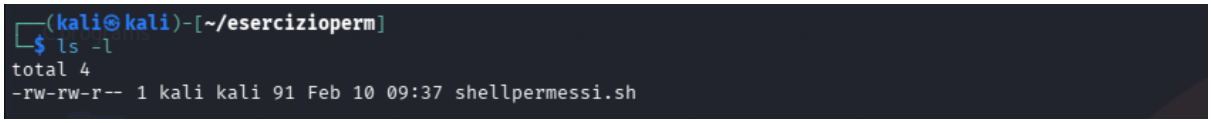

**Fig.3 Verifica permessi pre-modifica*

Prima di procedere con le modifiche, è stata effettuata un'analisi dei permessi correnti del file tramite il comando **`ls -l`**. Dallo stato iniziale si osserva che l'utente **kali** dispone dei privilegi di lettura e scrittura, così come il **gruppo**, mentre agli utenti **esterni** è consentita la sola lettura.

Fase3 – Modifica permessi

**Fig.4 Cambio permessi shell*

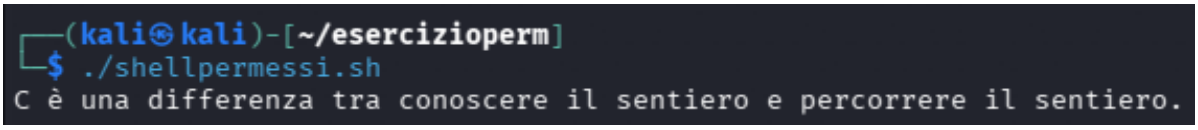

**Fig.5 Esecuzione shell Kali*

Dopo l'esecuzione del comando **`chmod 750 shellpermessi.sh`**, i permessi del file sono stati aggiornati in:

- **Kali(`rwx`):** Può leggere (**`r`**), modificare (**`w`**) ed eseguire (**`x`**) il file.
- **Gruppo(`rx`):** Possono leggere (**`r`**) ed eseguire (**`x`**) lo script, ma non possono modificarlo.
- **Altri(–): Non** hanno **alcun permesso**. Non possono né leggere, né scrivere, né eseguire il file.

In ultima analisi, è stata verificata la corretta funzionalità eseguendo lo script dall'utente **kali**, validando definitivamente la configurazione dei permessi impostati.

Fase4 – Analisi risultati

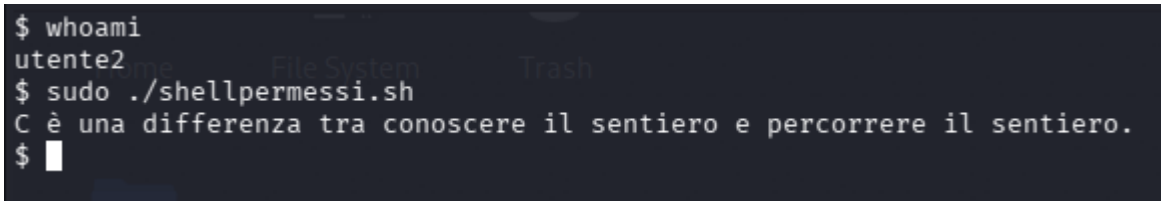

**Fig.6 Esecuzione shell utente2*

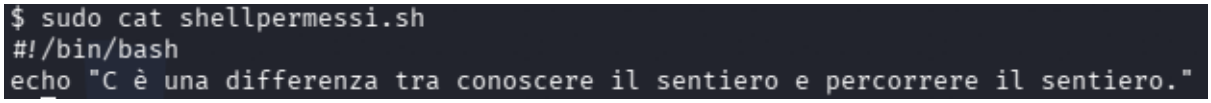

**Fig.7 Lettura shell utente2*

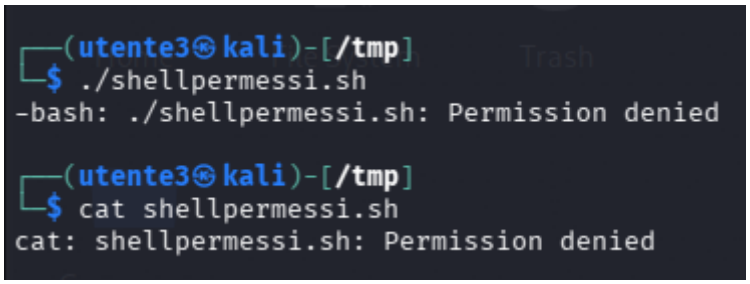

**Fig.8 Esecuzione e lettura shell utente3*

Sono stati eseguiti test di verifica utilizzando un account appartenente al gruppo (**utente2**) e un account privo di privilegi specifici (**utente3**), confermando l'efficacia della configurazione impostata. Come previsto dai permessi impostati, l'**utente2** è stato in grado di leggere ed eseguire lo script con successo. Al contrario, all'**utente3** è stato negato l'accesso a

qualsiasi operazione sul file, confermando con successo le restrizioni dei permessi applicati.

Conclusione

In conclusione, il documento ha dimostrato che l'uso del comando **`chmod 750`** assicura un'efficace protezione dei dati. I test hanno confermato che l'interazione con lo script è riservata ai soli utenti autorizzati: mentre l'utente principale mantiene il controllo totale, i membri del gruppo possono leggere ed eseguire il file senza poterlo modificare. Al contrario, l'accesso è stato totalmente negato agli utenti esterni per evitare operazioni non autorizzate. Ciò conferma l'importanza di una corretta configurazione dei privilegi per mantenere il sistema sicuro e ordinato