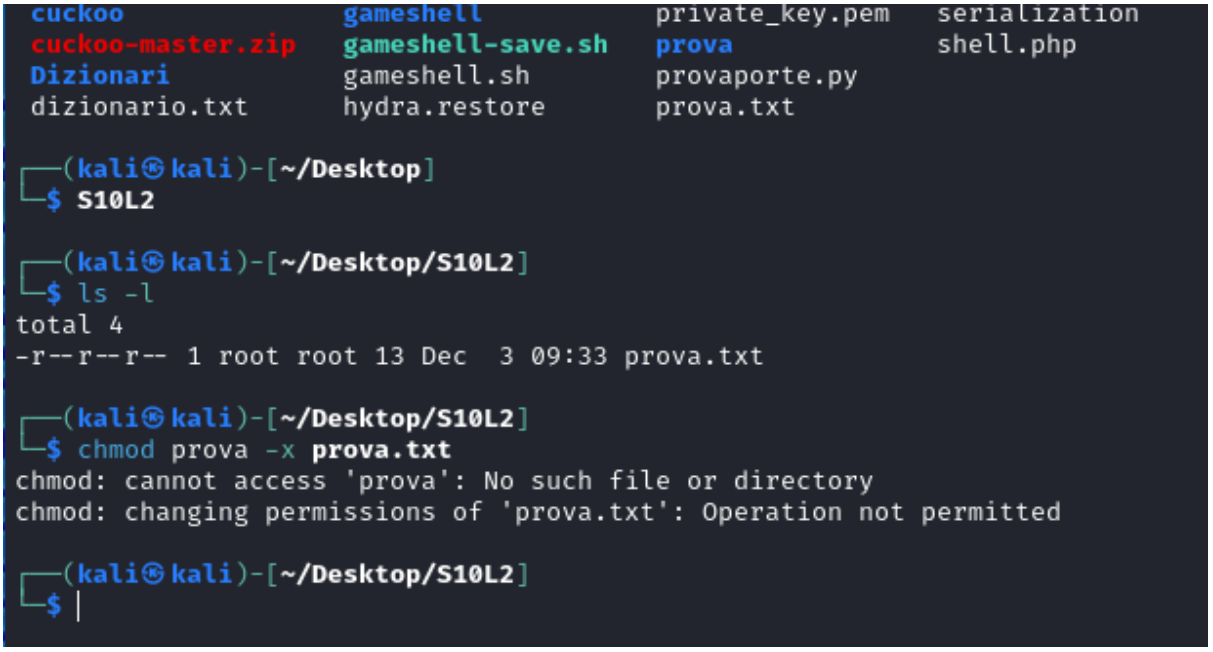
Zurigo 03.12.2024

Oggi andremo a creare un file ed una cartella su Kali Linux e verificheremo come modificare i permessi come abbiamo imparato durante la lezione.



Creata la cartella S10L2 con il comando ls -l andiamo a verificare quali utenti o gruppo di utenti possiede quali permessi.
Ci risulta

- indica che stiamo parlando di un file
r permesso di lettura per lo user in corso (U) user
- permesso di scrittura negato per lo user in corso (U)
- permesso di esecuzione negato per lo user in corso(U)
r permesso di lettura per il gruppo (G)group
- permesso negato di scrittura negato per il gruppo (G)
- permesso negato di esecuzione negato per il gruppo (G)
r permesso di lettura per gli altri (O)other
- permesso di scrittura negato per gli altri (O)
- permesso di esecuzione negato per gli altri (O)

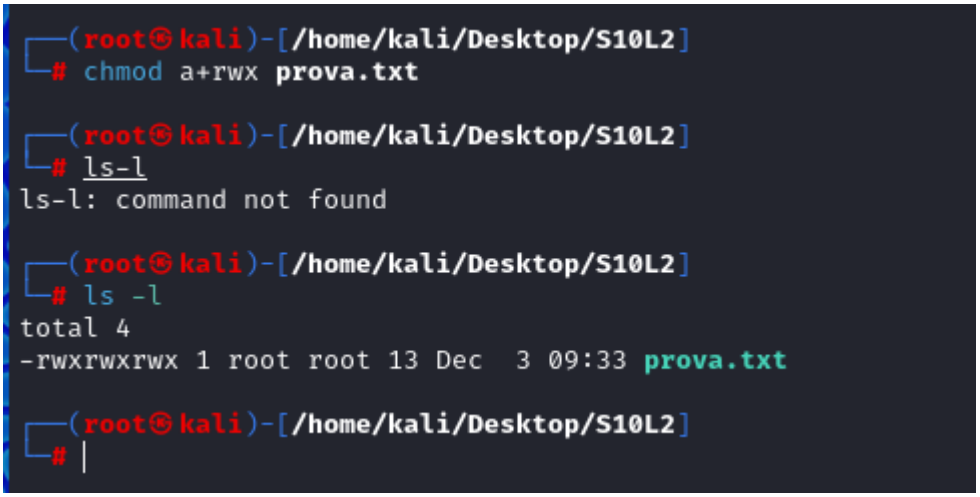
```
cuckoo              gameshell           private_key.pem   serialization
cuckoo-master.zip   gameshell-save.sh   prova             shell.php
Dizionari           gameshell.sh        provaporte.py
dizionario.txt      hydra.restore       prova.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ S10L2

┌──(kali㉿kali)-[~/Desktop/S10L2]
└─$ ls -l
total 4
-r--r--r-- 1 root root 13 Dec  3 09:33 prova.txt

┌──(kali㉿kali)-[~/Desktop/S10L2]
└─$ chmod prova -x prova.txt
chmod: cannot access 'prova': No such file or directory
chmod: changing permissions of 'prova.txt': Operation not permitted

┌──(kali㉿kali)-[~/Desktop/S10L2]
└─$
```

Proviamo a modificare i permessi, ma non ci è permesso perchè non siamo loggati come amministratore(o root).

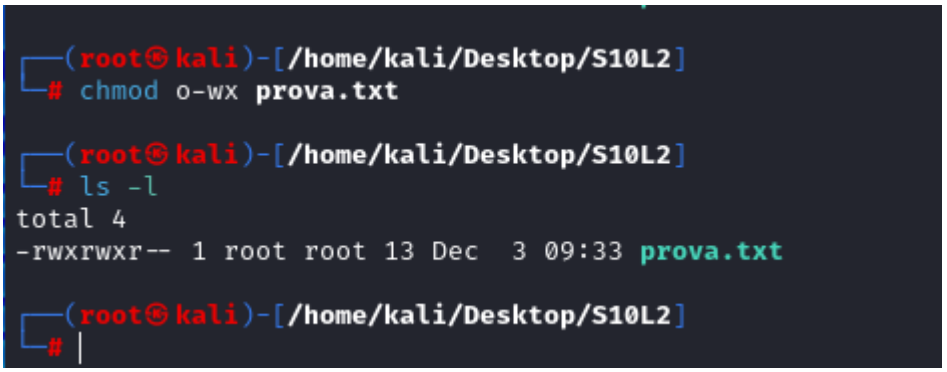
```
┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# chmod a+r prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# ls -l
total 4
-r--r--r-- 1 root root 13 Dec  3 09:33 prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# chmod g+x prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# ls -l
total 4
-r--r-xr-- 1 root root 13 Dec  3 09:33 prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# chmod u+rwx prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─# ls -l
total 4
-rwxr-xr-- 1 root root 13 Dec  3 09:33 prova.txt

┌──(root㉿kali)-[/home/kali/Desktop/S10L2]
└─#
```

Accediamo come amministratore e verifichiamo di nuovo i permessi per il file.
Con il comando chmod g+x prova.txt andremo a dare al gruppo i permessi di esecuzione ed infatti rilanciando il comando ls -l otteniamo
-r–r-xr–

Ora diamo all'utente tutti i permessi col comando chmod u+rwx prova.txt ed otteniamo -rwxr-xr–



con il comando chmod a+rwx prova.txt possiamo dare a tutti(utente, gruppo ed altri) i privilegi di lettura (r) scrittura(w) ed esecuzione(x) ed infatti otteniamo -rwxrwxrwx



Decidiamo di escludere gli altri utenti dalle scrittura e dall'esecuzione.

L'importanza della Gestione degli Utenti e dei Privilegi nella Cybersecurity

La gestione efficace degli utenti e dei privilegi rappresenta uno dei pilastri fondamentali della cybersecurity moderna. Un sistema di gestione degli accessi ben strutturato è in grado di minimizzare i rischi connessi agli attacchi informatici, proteggendo i dati sensibili e le infrastrutture critiche.

Perché è così importante?

- **Principio del privilegio minimo:** Assegnare agli utenti solo i privilegi strettamente necessari per svolgere le loro attività limita la superficie di attacco, riducendo le opportunità per gli attacchi.
- **Prevenzione delle escalation di privilegi:** Un attaccante che riesce a compromettere un account con pochi privilegi non può facilmente scalare a privilegi più elevati se gli accessi sono ben gestiti.

- **Rilevamento delle minacce:** Monitorando l'attività degli utenti e i loro accessi, è possibile individuare comportamenti anomali che potrebbero indicare un attacco in corso.
- **Conformità normativa:** Molte normative in materia di protezione dei dati (come il GDPR) richiedono una gestione rigorosa degli accessi per garantire la sicurezza delle informazioni personali.
- **Continuità operativa:** Un sistema di gestione degli accessi ben progettato assicura che solo gli utenti autorizzati possano accedere alle risorse critiche, garantendo la continuità operativa in caso di incidenti.

Elementi chiave di una buona gestione degli utenti e dei privilegi:

- **Autenticazione forte:** Utilizzare metodi di autenticazione a più fattori (MFA) per verificare l'identità degli utenti.
- **Autorizzazioni granulari:** Assegnare permessi specifici a ciascun utente o gruppo, in base alle loro funzioni.
- **Revisione periodica degli accessi:** Verificare regolarmente che gli utenti abbiano ancora bisogno dei privilegi assegnati e revocare quelli non più necessari.
- **Monitoraggio delle attività:** Tenere traccia delle azioni degli utenti per rilevare eventuali anomalie.
- **Gestione delle password:** Implementare politiche password robuste e utilizzare strumenti di gestione delle password.
- **Segmentazione di rete:** Dividere la rete in zone di sicurezza per limitare la propagazione di eventuali attacchi.

In conclusione

Una gestione efficace degli utenti e dei privilegi è essenziale per proteggere le organizzazioni dalle minacce informatiche sempre più sofisticate. Investendo in soluzioni di sicurezza adeguate e adottando best practice, è possibile ridurre significativamente il rischio di incidenti informatici e garantire la protezione dei dati sensibili.