# Mérési jegyzőkönyv

Access Control

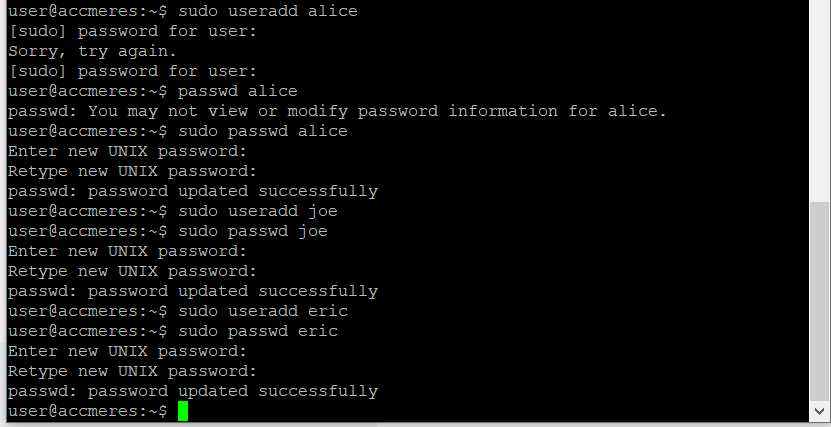
# 2022/2023/2 félév

| A mérőhely (VM) száma: | 10 |
| --- | --- |
| A mérés időpontja: | **2023. 05. 15.** |
| A mérést végezték: | **Wágner Réka (CGUOR8),**  **Rittgasszer Ákos (Z8WK8D)** |
| Ennek a fájlnak a neve: | **ACC\_0515\_10 \_Z8WK8D\_CGUOR8.doc**  (<mérés rövidítése> \_<hónap nap>\_<mérőhely>\_<Neptun1>\_<Neptun2>. doc) |

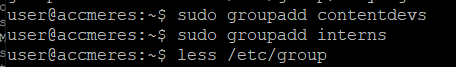
## Megosztott mappa konfigurálása

## Kapcsolódtunk a virtuális géphez:

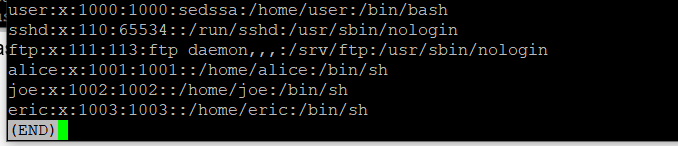
**Felhasználók kezelése**

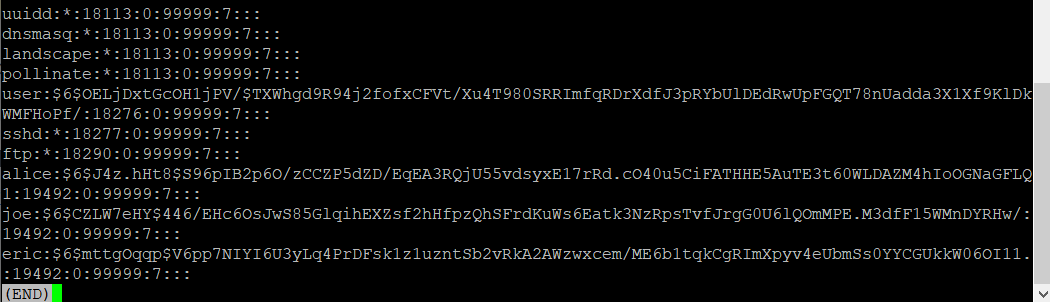
Felvettük a három felhasználót, mindenkinek a neve a jelszava: ****

Hozzáadtuk a szükséges csoportokat:

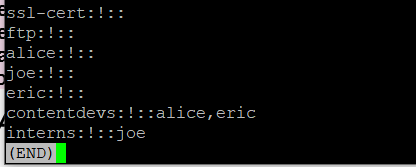
****

Változás a passwd, shadow, group és gshadow file-okban történt.

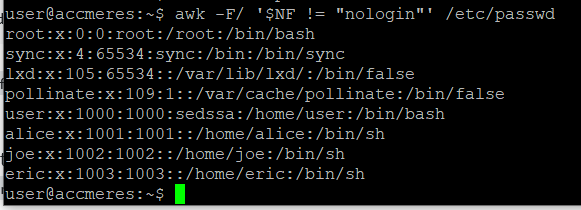
A passwd file-ba bekerültek az újonnan felvett felhasználók:  


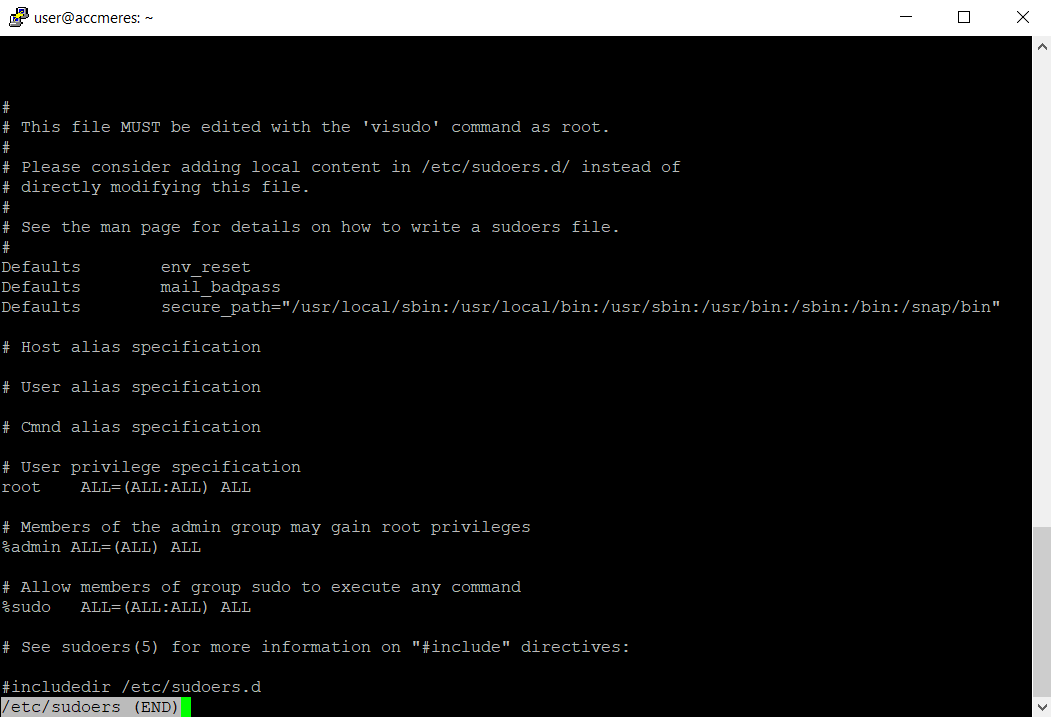
A shadow file:  


A group file, a megadott csoportokkal: ****

A gshadow file:  


Az alábbi felhasználók vannak a gépen (akikkel be lehet jelentkezni), látható a csoport azonosítójuk is:

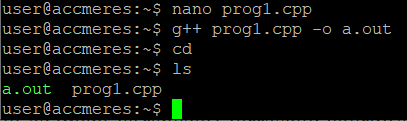


A sudo less /etc/sudoers parancs alapján láthatóak a rendszergazda jogosultságú felhasználók:  


**Mennyi? Harminc. . .**

A passwd file alapján 34 felhasználó van: ****

Létrehoztuk az új file-t és lefordítottuk:

****

Lefuttattuk nem root-ként:

****

Majd root-ként:

****

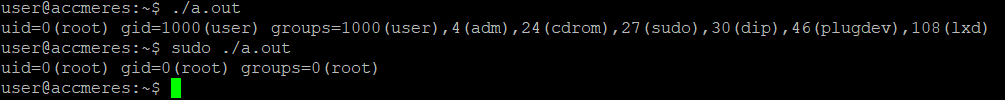
Tulajdonos változtatása root-ra:

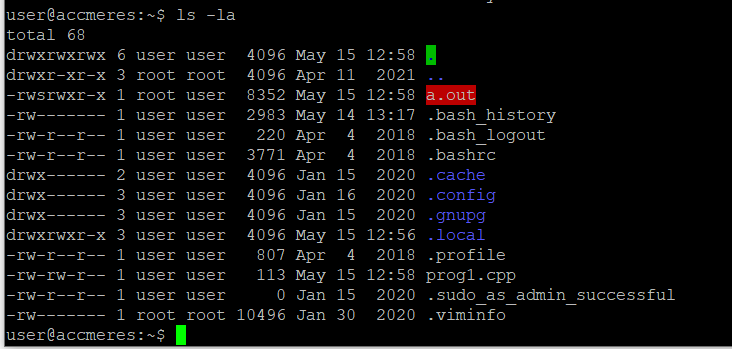
****

Ahhoz, hogy mindig a tulajdonos nevében fusson, a suid bit beállítása szükséges:

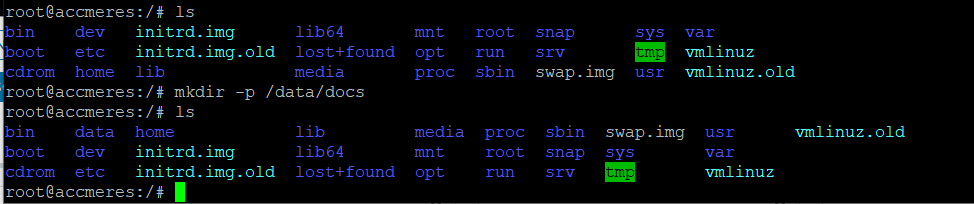
****

Újra futtattuk root-ként és nem root-ként is. Mindkét esetben az uid a root, de ha nem root-ként futtatjuk, akkor a többi adat a futtató felhasználóé:

****

Piros háttérszínnel jelenik meg: ****

**Megosztott mappa létrehozása**

Root-ként létrehoztuk a kért mappát: ****

Majd beállítottuk a tulajdonos felhasználót és csoportot:

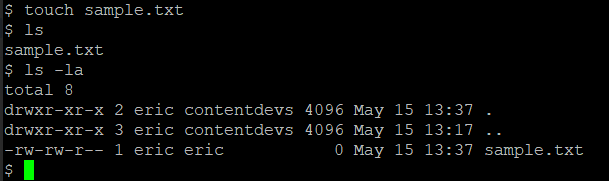
****

Utólag módosítottuk, hogy az előbbi parancs rekurzívan hajtódjon végre. Erről sajnos nem készült kép.

**Mappa megosztása csoporton belül**

Átváltottunk eric-re:

****

Létrehoztunk egy üres szöveges file-t a kért mappában. Látható, hogy a file tulajdonosa eric. A szülő folderek csoportja a contentdevs. A file-on eric-nek és a csoporttagoknak(eric) írási és olvasási jogosultságuk van, a többieknek csak olvasási. ****

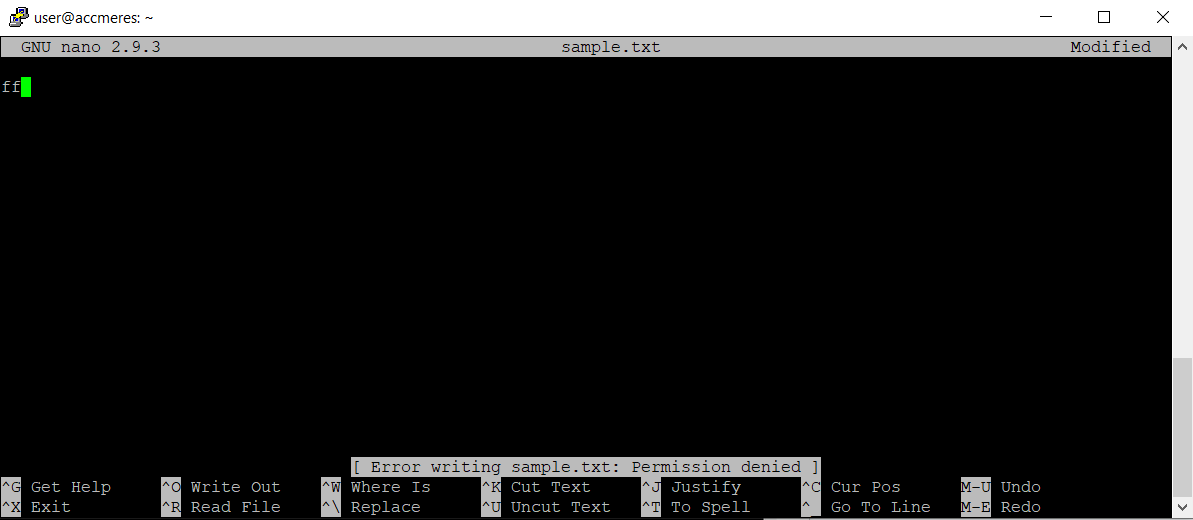
Alice-nek mivel az egyéb jogosultságok érvényesek rá csak olvasási joga van.

Látható, hogy olvasni tudja:

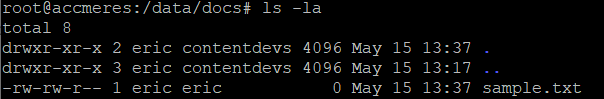
****

****

Illetve írni nincs joga:

****

A jogosultságok is alátámasztják az elöbbieket:

****

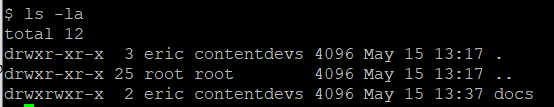
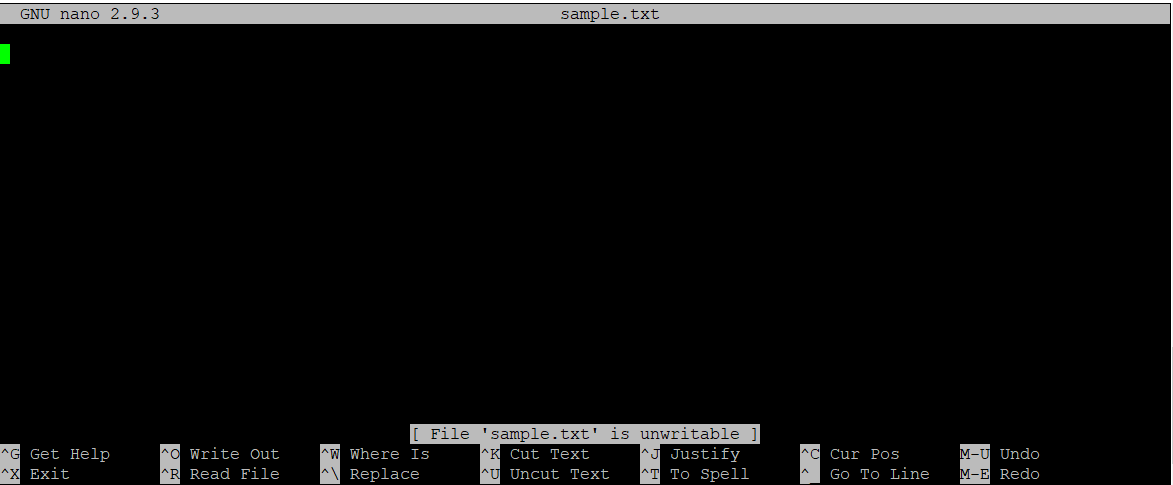
Alice nem tudott új file-t létrehozn, ennek oka, hogy a mappán a tulajdonos csoportnak nincsen írás jogai:

****

A tulajdosnos csoportnak írási jog adás:

****

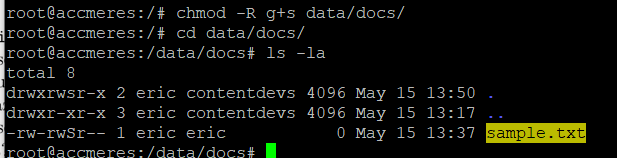
Látható, hogy valóban kaptak írási jogot a mappára:

****Alice továbbra sem tudja módosítani az Eric által létrehozott file-t. Ennek oka, hogy továbbra sincsen írási joga: ****

Ez itt is látható:

****

A probléma orvoslására megoldás lehet a sample.txt tulajdonos csoport módosítása vagy akár suid vagy guid használata.  
  
Átbillentettük a sgid bit-et:

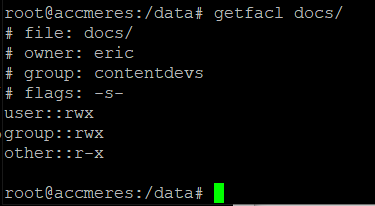


Ekkor már tud file-t létrehozni:****

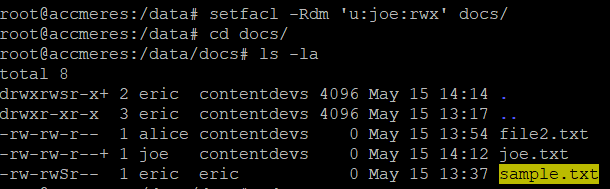
Tudná eric az alice által létrehozott file-t módosítani. Működik a mappa megosztása.

**Hozzáférés-védelmi lista konfigurálása**

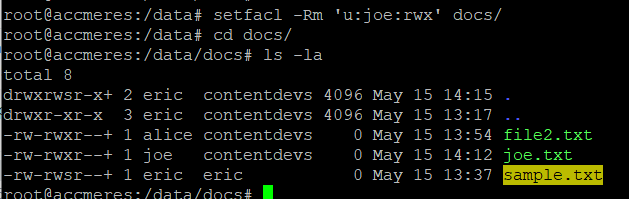
Azért, mert nem szeretné, hogy a csoport minden jogosultságával rendelkezzen. Csak specifikusan a munkához szükséges jogokat akar adni neki, vagyis csak ehhez a mappához akar hozzáférést biztosítani. Az esetlegesen más ehhez, a csoporthoz tartozó mappákhoz nem akar hozzáférést adni.

Telepítve van az acl és a tartalma::  


joe-nak jogosultság adása a régi tartalmakhoz:



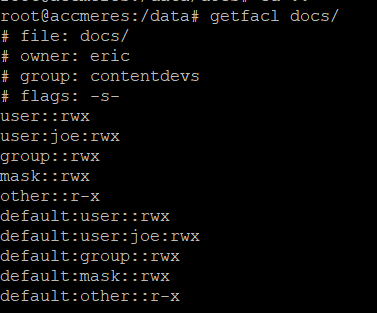
Illetve a jövőben létrejövőkhöz is:



Az újonnan megjelnő karakter, a +. Látható, hogy van olvasási joga:

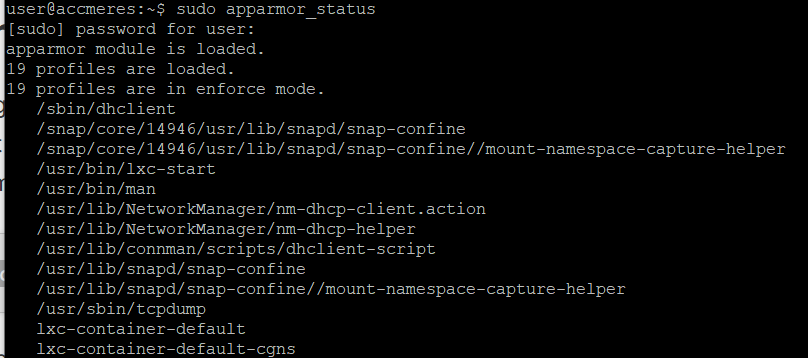


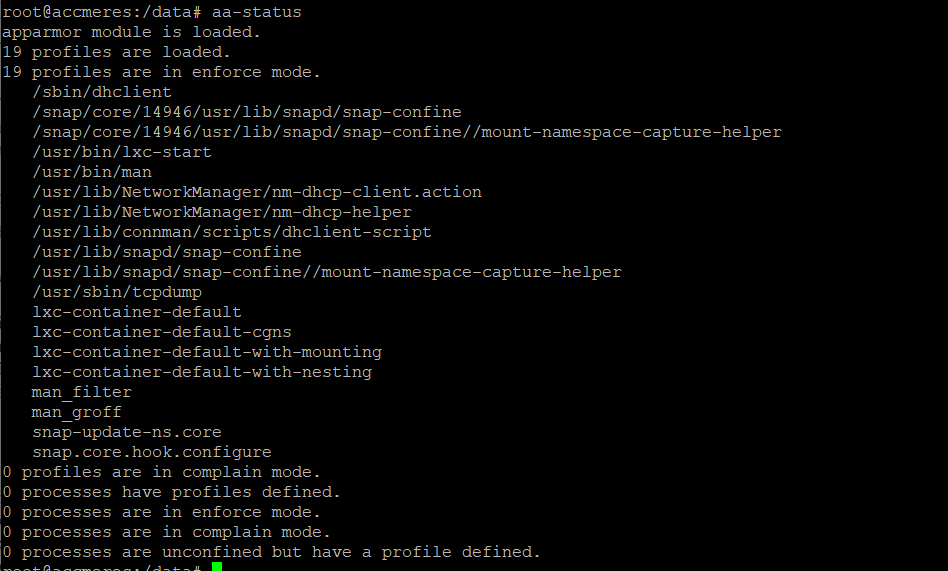
Így néz ki a módosított acl:



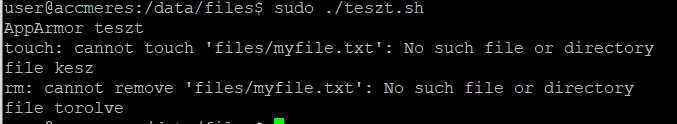
## AppArmor

Telepítve van:



Látható, hogy 19 profil van és 19 van enforcing módban:  


Létrehoztuk a megfelelő mappát és abban a teszt.sh file-t, ami a megadott szkriptet tartalmazza. Futtatás után az alábbi eredményt kaptuk:

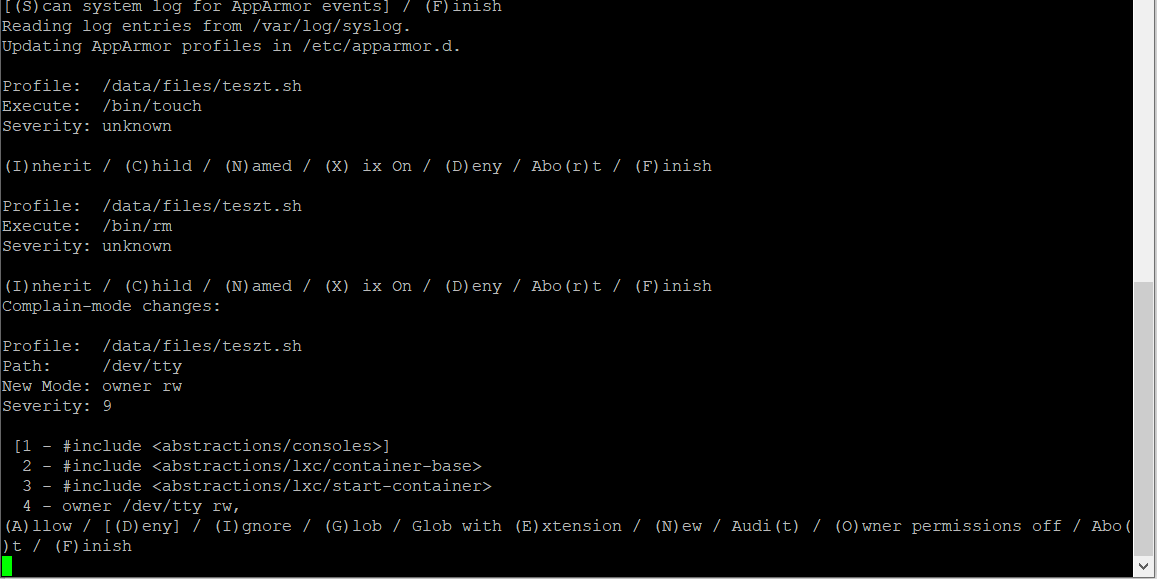


Az eredményből látható, hogy a szkript nem fér hozzá más file-okhoz.

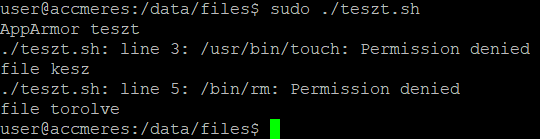
Elindítottuk a profilozást:



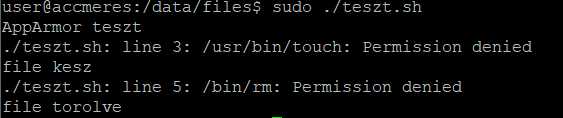
A profilozást követően az AppArmor segítségével adtunk jogosultásgot a touch, a rm és tty parancsok végrehajtásához:



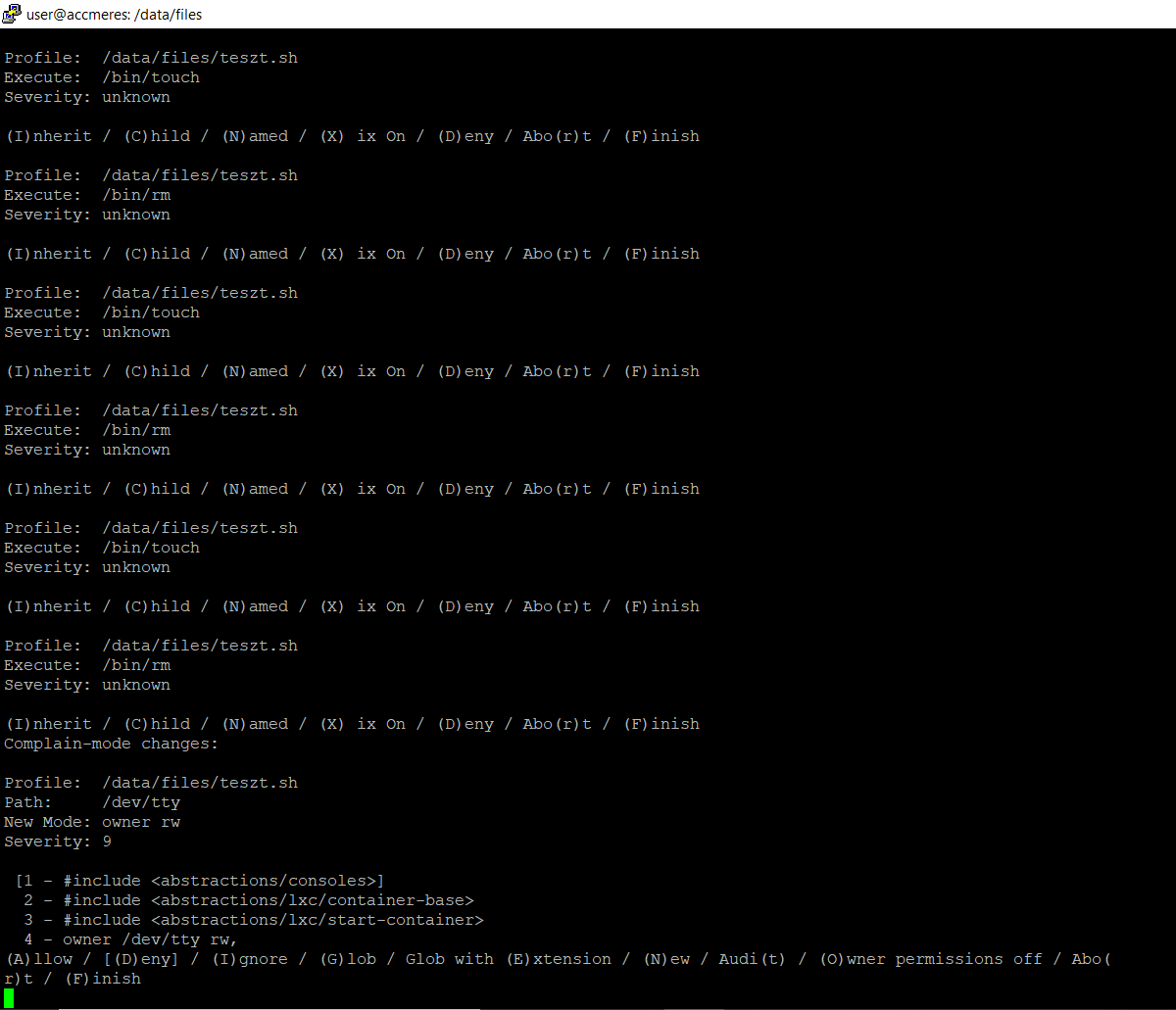
Ezután más hibaüzenetet kaptunk. Ekkor elértük a file-t, de nem volt jogosultságunk a parancsok végrehajtásához.



Átírtuk az elérési útvonalakat. Továbbra is ugyanazt a hibaüzenetet kaptuk:



A profilozást követően hozzáférést adtunk minden kívánt dologhoz. Sajnos a hibaüzenet továbbra sem változott.



Létrehoztuk az új szkriptet a data mappában. Sajnos semmilyen módon nem sikerült futtatni azt.

A scriptben jelen lévő sérülékenység a hello.txt file-on hívott cat műveletből fakad.