HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

7. labor – Engedélyezés, hozzáférés-szabályzás (Linux operációs rendszeren)

VIHIBB01 – Kódolás és IT biztonság (2022)

Ládi Gergő

CrySyS Lab, BME
gergo.ladi@crysys.hu

www.crysys.hu

MŰEGYETEM 1782

Felhasználókezelés – felhasználók

- Minden felhasználónak van egy egyedi azonosítója (UID)
  - … és egy egyedi felhasználóneve
- A felhasználókról tárolt információk a **/etc/passwd** fájlban vannak
  - A fájlt mindenki olvashatja
  - Régebben a felhasználók jelszavainak hashei is itt voltak

```
gergo.ladi@demovm:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
gergo.ladi:x:1001:1001:Gergő Ládi,,,:/home/gergo.ladi:/bin/bash
mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false
redis:x:108:113::/var/lib/redis:/bin/false
```

Felhasználókezelés – felhasználók

- Különleges felhasználó: root (UID=0), mindenhez van joga

- A jelszóhashek a **/etc/shadow** fájlban vannak ($algorithm$salt$hash)
  - A root:root tulajdonában van, --rw------- engedélyekkel

```
gergo.ladi@demovm:~$ sudo cat /etc/shadow
root:!:17804:0:99999:7:::
daemon:*:17804:0:99999:7:::
bin:*:17804:0:99999:7:::
sys:*:17804:0:99999:7:::
sync:*:17804:0:99999:7:::
_apt:*:17804:0:99999:7:::
sshd:*:17804:0:99999:7:::
gergo.ladi:$6$Qfz(...)YZ$sQMCjdFnL.d1o2P(...)NWbu60:17804:0:99999:7:::
mysql:!:17804:0:99999:7:::
redis:*:17805:0:99999:7:::
```

Felhasználókezelés – csoportok

- Minden csoport egyedi csoportazonosítóval (GID) rendelkezik
  - … és minden csoportnak van egy egyedi csoportneve is
- Egy felhasználónak lehet ugyanaz a neve, mint egy csoportnak
- Minden felhasználóhoz tartozik egy csoport, aminek csak ő a tagja
  - Általában ez a felhasználó elsődleges csoportja
- A csoportokról tárolt információk a **/etc/group** fájlban tárolódnak

```
gergo.ladi@demovm:~$ cat /etc/group
root:x:0:
daemon:x:1:
sudo:x:27:gergo.ladi
www-data:x:33:
gergo.ladi:x:1001:
mysql:x:112:
redis:x:113:
```

Hozzáférés-szabályzás

- Minden fájl
- A hozzáférést *engedélyek* szabályozzák
  - A tulajdonosnak (u), a tulajdonos csoportnak (g), és mindenki másnak (o)

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- Az első betű adja meg a fájl típusát
  - Normál fájl (-)
  - Könyvtár (directory) (d)
  - Link (l)
  - Socket (s)
  - Named pipe (p)
  - Eszköz (device) (blokkos: b, karakteres: c)

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- Mindig a felhasználóra leginkább illő számhármas érvényesül
  - Pl.: ha én vagyok a tulajdonos, csak a tulajdonos engedélyei számítanak
  - Ez lehetővé tesz furcsa kombinációkat is, mint pl.: ----rwxrwx

- Az engedélyek leírhatók számokkal is
  - r = 4, w = 2, x = 1
  - 775 megfelelője: -rwxrwxr-x
- Egy fájl jogosultságai a `chmod` paranccsal változtathatók
  - Csak a tulajdonos változtathat (vagy különleges engedéllyel rendelkezők)
- Egy fájl tulajdonosa a `chown` paranccsal változtatható
- Egy fájl tulajdonos csoportja a `chgrp` paranccsal változtatható
  - Utóbbi két parancshoz különleges engedélyek kellenek (vagy root user)

Hozzáférés-szabályzás

- Különleges jogosultsági értékek
  - *setuid* – ha egy futtatható állományra be van állítva, az mindig a tulajdonos nevében fut, függetlenül attól, hogy ki indította el
    - » Pl.: `-rwsrwxr-- root root` mindig root nevében fog futni
    - » Könyvtárakon nincs hatása
    - » Nincs hatása, ha a tulajdonosnak nincs *x* engedélye (ilyenkor nagy S látszik)
  - *setgid* – setuidhoz hasonló, de a tulajdonos csoportot állítja át
    - » Pl.: `-rwxrwsr-- gergo cloudmgmt` úgy fog futni, mintha valaki a *cloudmgmt* csoportból indította volna el, de a tulajdonos felhasználó nem változik
    - » Ha a tulajdonos csoportnak nincs *x* engedélye, nagy S látszik
    - » Ha könyvtárra van beállítva, akkor az ott létrejövő új fájlok tulajdonos csoportja a könyvtáré lesz, és nem pedig a fájlt létrehozó felhasználóé
  - sticky bit – ha be van állítva egy könyvtárra, az itt lévő fájlokat csak a tulajdonosuk törölheti
    - » Pl.: `drwxrwxrwt` könyvtárból mindenki csak a saját fájljait törölheti
    - » Fájlokra közvetlenül nincs hatással
    - » Ha *mindenki más*nak nincs *x* engedélye, nagy T látszik

Hozzáférés-szabályzás

- Alapértelmezett engedélyek
  - Új fájl létrejöttekor annak engedélyei 666 (-rw-rw-rw-) lesznek
  - Könyvtárak esetén ez 777 (drwxrwxrwx)
- Ez a viselkedés az `umask` paranccsal átállítható
  - A maszk értéke kivonódik az alapértelmezett engedélyekből
  - Pl.: ha az umask 022, az új könyvtárak 755-ként (drwxr-xr-x) jönnek létre