Védelem

Alkalmazások - AppArmor

Tipikus hozzáférés szabályozási megoldások

- DAC – Discretionary Access Control (tetszés szerinti)
  - Minden objektumnak tulajdonosa van, aki szabályozhatja a hozzáférést
  - Pl. állományok
- MAC – Mandatory Access Control (kötelező)
  - Hozzáférés-jogosultság kiosztása előre meghatározott módon

MAC implementáció Ubuntuban

- AppArmor (Application Armor) – alapértelmezett
- SELinux (Security Enhanced Linux)

AppArmor

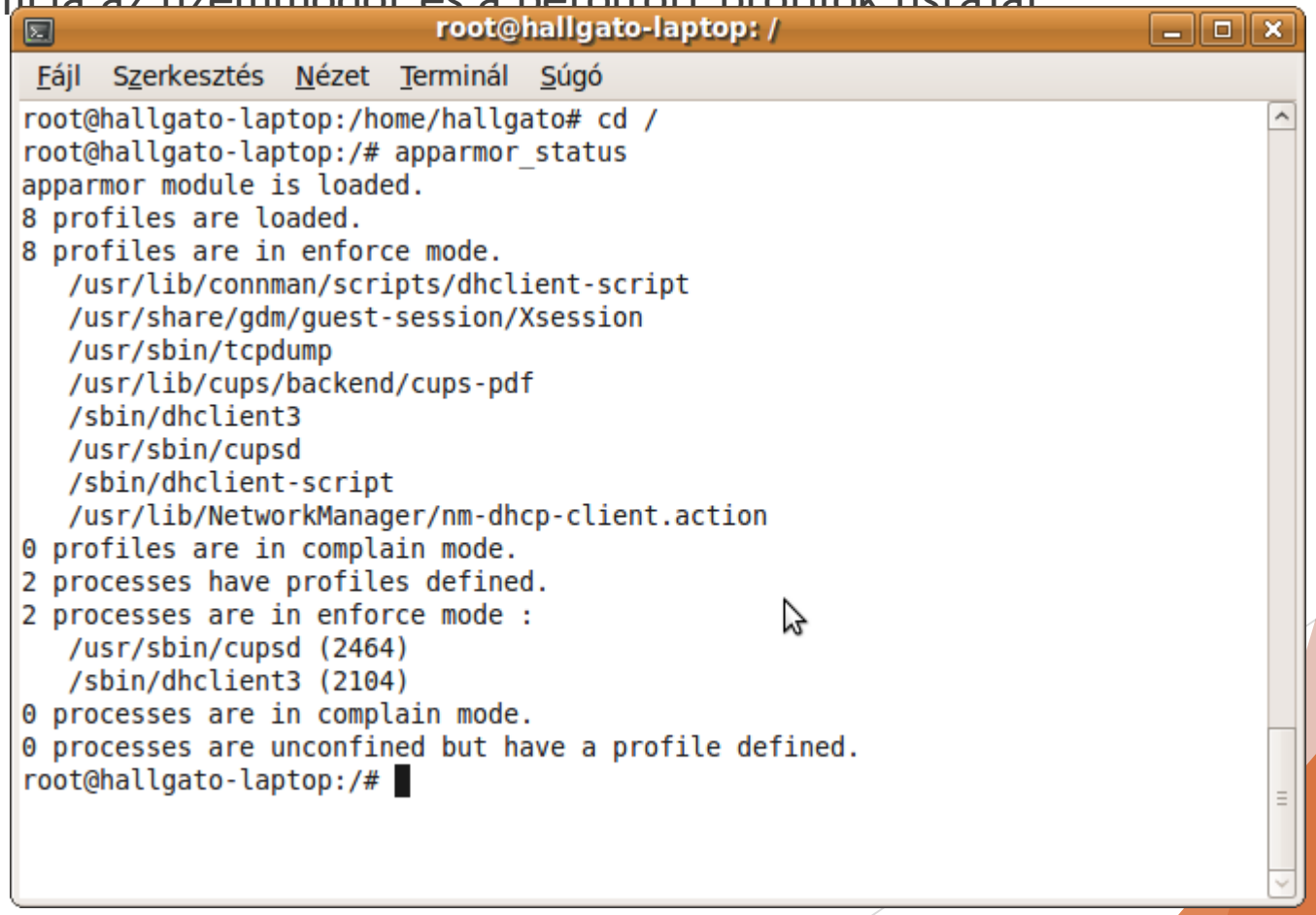
- Név alapú MAC-et megvalósító biztonsági modul
- Elsősorban hálózati alkalmazások védelmére: www, ftp, Samba, CUPS, dhcpkliens
- Szabályozás **biztonsági házirendekkel**
- Csomagok: apparmor, apparmor-utils, apparmor-profiles
- sudo apt-get install apparmor apparmor-utils apparmor-profiles
- Minden szabályozás alá tartozó alkalmazáshoz egy profil állomány (biztonsági házirend)

AppArmor

- Indítás: /etc/init.d/apparmor start|stop|restart
- Kiszolgáló (pl. Apache, Samba, SQUID, Postfix) telepítésekor települ a hozzá tartozó profil
- További profilok az apparmor-profiles csomagban
- Üzemmódok
  - Enforce – kikényszerítő
  - Complain - figyelmeztető

apparmor-utils

- apparmor_status – kiírja az üzemmódot és a betöltött profilok listáját



Profil

- Profil módosítása után újratöltés
- cat profil | sudo apparmor_parser –r
- Az összes profil újratöltése
- sudo /etc/init.d/apparmor reload
- Alkalmazási módok
  - enforce – kikényszerített
  - complain - figyelmeztető

Kapcsolók

- **enforce** – kikényszerített módba helyezi az apparmort
- aa_enforce alkalmazás – csak egy profilt (alkalmazást)
- **complain** – figyelmeztető módba helyezi az apparmort
- aa_complain alkalmazás – csak egy profilt (alkalmazást)
- unconfined – kilistázza azokat az alkalmazásokat, amelyeket nem szabályoz az apparmor
- autodep alkalmazás – egy alap profilt készít egy alkalmazáshoz
- audit alkalmazás – naplózza az alkalmazás tevékenységét

Konfigurálás

- Konfigurációs állományok /etc/apparmor
- Profilok /etc/apparmor.d
- A profilnév az alkalmazás teljes elérési útvonalát tartalmazza, /-k helyett pontokkal

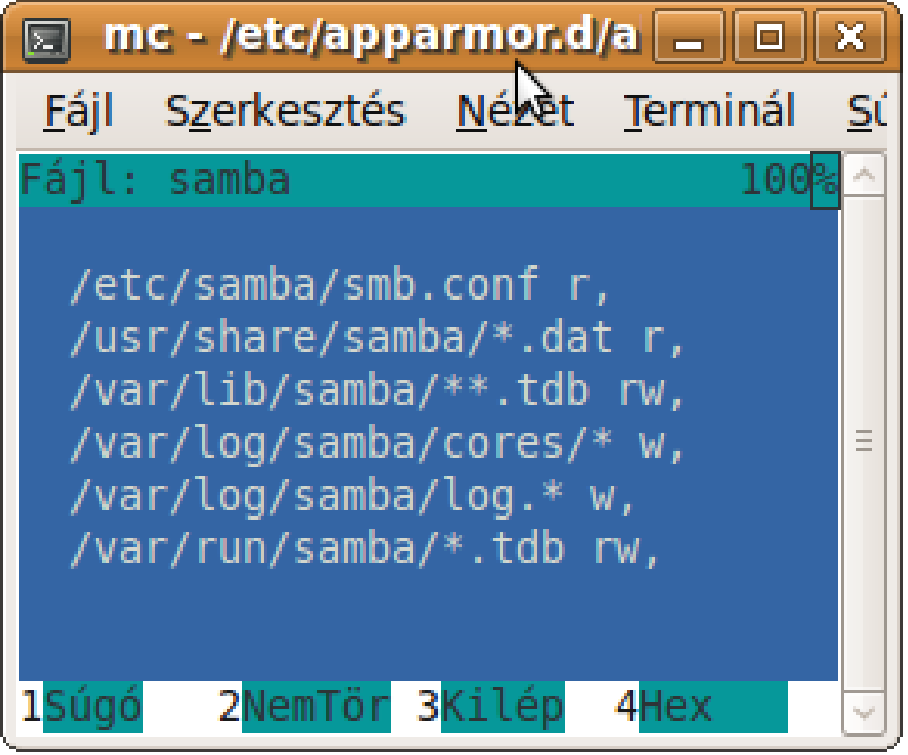
```
root@ubuntu-server:/etc/apparmor.d# ls
abstractions     sbin.syslog-ng                    usr.sbin.dnsmasq
apache2.d        tunables                          usr.sbin.dovecot
bin.ping         usr.bin.chromium-browser          usr.sbin.identd
cache            usr.lib.dovecot.deliver           usr.sbin.mdnsd
disable          usr.lib.dovecot.dovecot-auth      usr.sbin.nmbd
force-complain   usr.lib.dovecot.imap              usr.sbin.nscd
local            usr.lib.dovecot.imap-login        usr.sbin.rsyslogd
program-chunks   usr.lib.dovecot.managesieve-login usr.sbin.smbd
sbin.dhclient    usr.lib.dovecot.pop3              usr.sbin.tcpdump
sbin.klogd       usr.lib.dovecot.pop3-login        usr.sbin.traceroute
sbin.syslogd     usr.sbin.avahi-daemon
root@ubuntu-server:/etc/apparmor.d# _
```

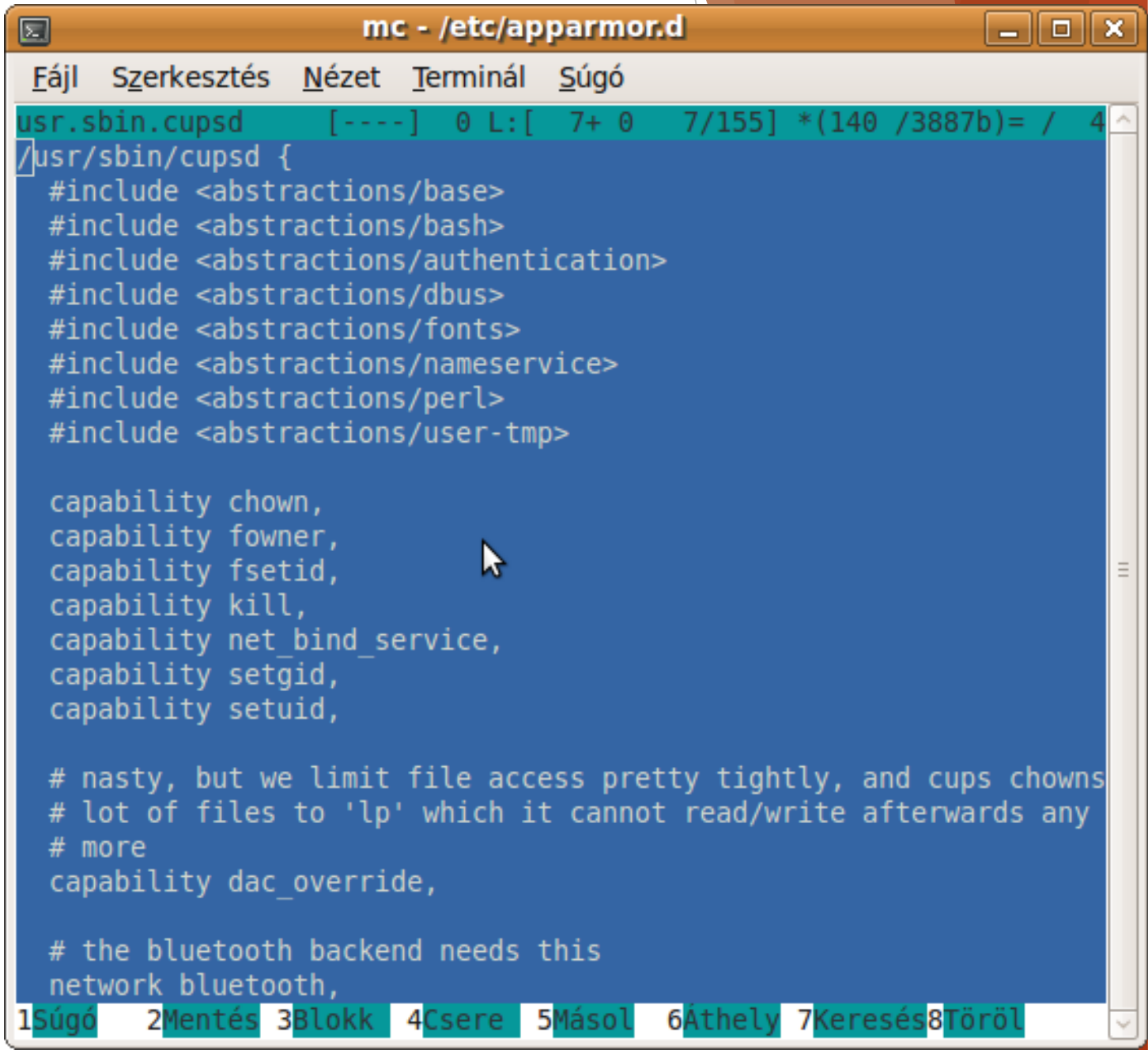
Könyvtárak

- **abstractions, tunables** – olyan profil szabályokat tartalmaz, amelyeket több profil közösen használ
- **disable** - az ide belinkelt profilok le vannak tiltva
- **force-complain**

Profil tartalma

- **Útvonal** – milyen állományokhoz férhet hozzá az alkalmazás
- Ha az útvonal *-ban végződik, akkor az adott könyvtár összes állományára vonatkozik
- Jogosultságok r,w,x,l (link), stb.
- Pl. /var/log/samba/log.* w, - az alkalmazás írhatja a samba könyvtár összes log. kezdetű állományát
- **Képesség** (Capability) – milyen privilégiumokat használhat a folyamat
- Pl. capability chown – lecserélheti egy fájl felhasználói- és csoport tulajdonosát





- include – direktívával illesztik be a hivatkozásokat

Források

- **A quick guide to AppArmor profile Language**
  http://wiki.apparmor.net/index.php/QuickProfileLanguage

- **AppArmor**
  https://wiki.ubuntu.com/AppArmor

- **Ubuntu Manual - AppArmor**
  http://manpages.ubuntu.com/manpages/utopic/man5/apparmor.d.5.html