Algebra
visoko učilište

SELinux (Security Enhanced Linux)

www.racunarstvo.hr

SELinux (Security Enhanced Linux)

- MAC (Mandatory Access Control) sustav na Linuxu
- SELinux ima tri načina rada:

1. Enforcing - uključen i radi;
2. Permissive - uključen, ali se koristi za *debugging* pravila koja bi u Enforcing načinu rada uzrokovali zabranu pristupa nekom sadržaju;
3. Disabled - isključen

Algebra
visoka škola
za primijenjeno
računarstvo

SELinux privremena i trajna konfiguracija načina rada

- promjenom konfiguracijske datoteke /etc/sysconfig/selinux trajno se mijenja način rada (Disabled, Enforcing, Permissive)
- ako prebacujemo iz Disabled u Enforcing/Permissive ili obrnuto, potreban restart
- Trenutna promjena stanja:

[root@OOS2 ~]# setenforce 0/1

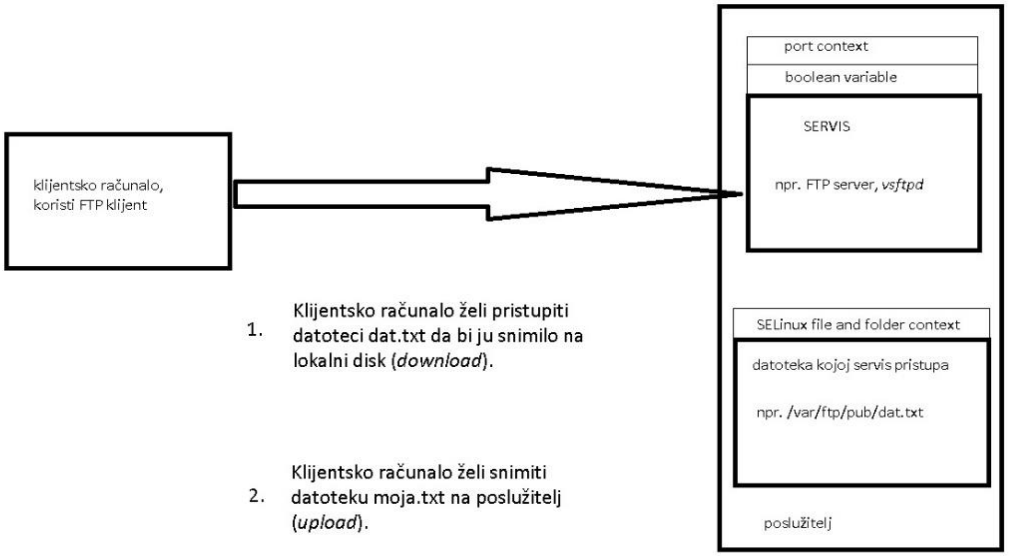
(0=Permissive, 1=Enforcing)

SELinux elementi konfiguracije

Na osnovnoj razini, SELinux se bavi sa tri osnovna elementa:

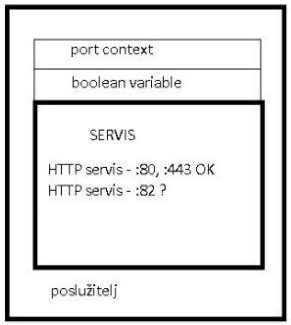
- 1. sigurnosnim kontekstima za datoteke i direktorije
- 2. sigurnosnim kontekstima za portove
- 3. *boolean* varijablama koje prate "sigurnosno osjetljive" opcije servisa

Grafički prikaz rada SELinux-a



FTP klijent pokušava pristupiti datoteci da bi ju snimio, ili da bi snimio sadržaj na FTP server. Da li bi SELinux trebao dopustiti snimanje datoteke u *Enforcing* načinu rada?

SELinux sigurnosni konteksti za portove



HTTP servis ima dozvolu za npr. zauzimanje portova 80 i 443 (njemu potrebni portovi za normalan rad). Što ako mi, kao sistem administratori, tražimo od HTTP servisa da zauzme i port 82?

HTTP poslužitelj pokušava zauzeti port koji mu ne pripada. Da li bi mu SELinux to trebao dopustiti ako je uključen (u Enforcing načinu rada)?