

# Logimine



# Süsteemi logidesse kirjutavad

## ■ deemonid (*daemons*)

- httpd, ftpd, smbd
- sshd, telnetd
- crond, atd jne

## ■ süsteemsed utiliidid

- su, sudo, useradd

## ■ tuum

Logide asukoht tavaliselt - /var/log

# Logid võivad olla



- teksti kujul
  - tekstifailis
- kahendkujul
  - kahendfailis
  - andmebaasis

# Kuidas logitakse



- protsess kirjutab logikirje ise faili
- protsess saadab kirje andmebaasimootorile
- protsess saadab kirje logimissüsteemile/logimisindeemonile
  - syslogd (vanemad linuxid)
  - rsyslogd

# (r)syslogd

- tegeleb teksti kujul logidega
- filtreerib välja kordused
- võimaldab kirjutada logisid
  - faili kohaliku arvuti kõvakettale
  - saata syslogd-le teises arvutis (hea!)
  - rsyslogd võib saata mujalegi nt
    - andmebaasi (MySQL, PostgreSQL, Oracle, MS SQL ...)
    - SNMP Trap teadetena SNMP jälgimisjaama
- on küllaltki paindlikult konfigureeritav (/etc/syslog.conf või /etc/rsyslog.conf)
- võrreldes otse faili kirjutamisega võtab arvestatavalt süsteemiressurssi

# **rsyslog.conf** (või **syslog.conf**)



- Iga logikirjega annab programm kaasa info, mille järgi kirje logifaili(de)sse kirjutatakse
  - teenus/alamsüsteem (*facility*)
    - | auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, local0, .., local7
  - logimistase (*priority level*)
    - | debug, info, notice, warning, err, crit, alert, emerg

# Mis logidest edasi saab



- hoida kõik alles?
- kustutada aeg-ajalt?
- lõigata aeg-ajalt lühemaks?
- roteerida!
  - logrotate
    - /etc/logrotate.conf
- archiveerida!

# Milleks kogu see logimine?

- Ülevaade süsteemi tööst
- Ülevaade kasutajate tegevusest (teatud piirini)
  - Võimalik hiljem tuvastada, kes mida teinud on
- Serverprogrammide vea- ja infoteated lähivad logifaili
- Logide analüüsimise programmid alates tavalisest grep-st kuni targa IDS/IPS-ni



# Logi analüüsimine



## ■ logwatch

- Linuxiga kaasas olev logide analüsaator
- Käivitatakse cron-ga kord päevas
- Otsib logidest „ebatavalisi“ kirjeid, teeb statistikat
- Tulemus saadetakse administraatorile e-kirjaga

## ■ fail2ban

- Analüüsib logifaili ning kui leiab kahtlast, nt liiga palju nurjunud sisselogimisi samalt IP-lt, muudab tulemüüri reegleid ja piirab mingiks ajaks sellelt IP-lt ligipääsu
- Sisuliselt IPS (*Intrusion Prevention System*)