

## Linux h2

z)

### Command line:

Komentokehote on ollut olemassa tietokoneiden kehityksen alusta alkaen. Komentokehoteen komennot ovat pysyneet samana vuosikymmeniä ja tulevat pysymään myös jatkossa. Komentokehotteella on nopea työskennellä ja kaikki linux-jakelut käyttävät suurimmalta osin samoja peruskomentoja. Hyvä puoli komentokehotteessa on, ettei tarvitse etsiä graafisen käyttöliittymän tavalla pieniä nappeja, jotka vaihtavat paikkaansa joka päivituksen jälkeen. :)

### Run an Internet Speed Test from the Linux Command Line:

Artikkelissa neuvotaan kuinka ladata ja käyttää verkontestaukseen käytettäviä työkaluja komentoriviltä. Artikkelin kommentteissa keskustellaan kuinka saadaan mahdollisimman luotettavia testaustuloksia. Kommentteissa kerrotaan kuinka osa internetpalvelun tarjoajista tarkoituksellisesti priorisoi tunnettujen testisivustojen liikennettä, jotta internet yhteytesi näyttää nopeamalta mitä se oikeasti on. Kommentteissa joku ehdottaa kuinka nopeutta voisi myös testata luomalla muutama virtuaalikone maantieteellisesti eri alueille ja tekemällä niillä testejä.

Asensin myös itse speedtest-työkalun linux koneelleni ja testasin sen toimintaa. Asensin työkalun komennolla: `sudo apt-get install speedtest-cli`. Itse työkalun starttasin komennolla: `speedtest-cli`. Työkalu kertoo selvästi download ja upload nopeuden.

Linkki keskusteluun löytyy osoitteesta: <https://news.ycombinator.com/item?id=21572308>

a)

`/` tarkoittaa root directorya. Root directory on kaikista ylin paikka koko tiedostorakenteessa. Windows maailmassa samaa voisi tarkoittaisi `C:\`

Root directoryn alta löytyy kaikki tietokoneen tiedostot.

```
walter@waldonboksi:/$ ls
bin    dev    home   initrd.img.old  lib32  libx32  media  opt    root  sbin  sys  tmp  var  vmlinuz.old
boot   etc    initrd.img  lib       lib64  lost+found  mnt    proc   run   srv   testi3  usr  vmlinuz
walter@waldonboksi:/$
```

`/home/` on koti kaikille käyttäjille. Käyttäjäprofiilit löytyvät home-tiedoston alta.

```
walter@waldonboksi:/home$ ls
walter
```

`/home/walter` on walter käyttäjän oma kansio, johon walter voi tallentaa omia tiedostojaan. Käyttäjä kotirosvo ei pääse walterin tiedostoihin.

```
walter@waldonboksi:/home$ ls
kotirosvo  walter
```

**/etc/** sisältää kaikki järjestelmän konfiguraatio tiedostot. Kaikki konfiguroinnit ovat Linux:ssa tiedostoja ja nämä tiedostot sijaitsevat etc-kansion alla.

```
walter@waldonboksi:/etc$ ls
acpi                dbus-1              gshadow-            lighttpd             nsswitch.conf       rc4.d               sudoers
adduser.conf        dconf              gss                 locale.alias         openal              rc5.d               sudoers.d
adjtime             debconf.conf       gtk-2.0             locale.conf          openni2             rc6.d               sudo_logsrvd.conf
aliases             debian_version     gtk-3.0             locale.gen           opt                 rcS.d               sv
alsa                default            hddtemp.db          localtime            os-release          request-key.conf    sysctl.conf
alternatives        deluser.conf       host.conf            logcheck             PackageKit          request-key.d       sysctl.d
```

**/media/** -kansio on paikka kaikille ulkoisille laitteille, jotka yhdistetään tietokoneeseen. Esimerkiksi CD-levy, joka syötetään tietokoneen sisään, näkyy mediakansion alla.

## **/var/log/**

Var-hakemisto sisältää tiedostoja, joita järjestelmä kirjoittaa sen toiminnan aikana. Tiedostot tyypillisesti päivittyvät koko ajan järjestelmän ollessa päällä. /var/log-tiedosto sisältää lokitiedostoja, kaikesta toiminnasta mitä tietokoneella tapahtuu. Lokitiedostot voidaan yleisesti jakaa neljään eri kategoriaan, jotka ovat application logs, event logs, service logs ja system logs. Ongelma tilanteessa lokitiedoista voidaan selvittää mitä tietokoneelle on tapahtunut ja kuka sitä on käyttänyt.

**b)**

Komentokehote tehtävä

**Ongelma1:** Haluaisin katsoa kalenteria poistumatta komentokehotteesta

Ensiksi etsin sopivaa sovellusta komennolla apt-cache search calendar.

Komento apt-cache listaa paketit, jotka ovat saatavilla koneelleni.

Löysin ohjelman nimeltä calcurse.

Asensin ohjelman komennolla sudo apt-get install calcurse.

Sovelluksella näkee näppärästi päivämäärän.

		Calendar (#250)							
syyskuu 7, 2022		syyskuu 2022							
		ma	ti	ke	to	pe	la	su	
syyskuu 8, 2022	35	29	30	31	1	2	3	4	
	36	5	6	[ 7 ]	8	9	10	11	
	37	12	13	14	15	16	17	18	
	38	19	20	21	22	23	24	25	
	39	26	27	28	29	30	1	2	

**Ongelma2:** haluaisin lähettää kaverille viestin poistumatta komentokehotteesta.

Ensiksi etsin sopivaa sovellusta komennolla `apt-cache search mail cli`

Löytyisin ohjelman alpine: text based email client

Asensin alpine komennolla `sudo apt-get install alpine`

Alpinessa on täysin tekstipohjainen käyttöliittymä minkä käyttöön riittää pelkkä näppäimistö.

```
?      HELP          - Get help using Alpine
C      COMPOSE MESSAGE - Compose and send a message
I      MESSAGE INDEX  - View messages in current folder
L      FOLDER LIST    - Select a folder to view
A      ADDRESS BOOK   - Update address book
S      SETUP          - Configure Alpine Options
Q      QUIT           - Leave the Alpine program
```

**Ongelma 3:** Haluaisin kuunnella musiikkia poistumatta komentokehotteesta.

Ensiksi etsin hyvää sovellusta komennolla `apt-cache search music cli`. Löysin sovelluksen nimeltä draai- command line music player for MPD. Asensin sen komennolla `sudo apt-get install draai`.

```

walter@waldonboksi:/$ draai
/usr/bin/draai:shift:353: shift count must be <= $#
Usage: draai [option [option ...]] command [track [track ...]|tracknumber [tracknumber ...]]

Play audio tracks, using mpc(1).

-V, --version      show program's version number and exit
-h, --help         show this help message and exit
-l, --license       show license and exit

-d, --debug
    Be very verbose.
-S, --noshuffle
    Do not shuffle tracks and leave random mode untouched (default is: do
    shuffle and disable random mode). See also the script dr_unsort.
-p PLAYLIST, --playlist=PLAYLIST
    Playlist file; option can be supplied more than once. To be used
    with command "draai".
-r, --raw
    Print raw stuff, suitable for postprocessing (if combined with tail, peek
    or list).
-s, --sloppy
    Do not try hard to make everything sound smooth. If combined with skip:
    risk a squeak on old hardware.
-t TIME, --time=TIME
    If combined with commands quit or draai: time at which to quit or start.

commands:

add:
    Add file(s) (given either as args or on stdin) to playlist. You probably want
    to have 'draai add' read from a pipe fed by e.g. 'draai listall' or 'draai
    search'.

crescendo:
    Play louder.

```

c)

## Lokitapahtuma 1

Kokeilin kirjautua toisella käyttäjätunnuksella, jonka olin luonut jo aikaisemmin komennolla....

En muista enää komentoa ja kokeilen etsiä sitä lokeista...

Lähdin etsimään tietoa auth.log tiedostosta komennolla `sudo grep "kotirosvo" less auth.log`

Sain selville, että olin luonut kotirosvon 6.7.2022 kello 11:23 komennolla `sudo adduser kotirosvo`

Tämän jälkeen menin `var/log/auth.log` ja katsoin lokia komennolla `sudo less auth.log`.

Lokeista löytyy tieto, että käyttäjä kotirosvo on yrittänyt kirjautua kolme kertaa väärällä salasanalla.

```

Sep  6 15:23:53 waldonboksi systemd: pam_unix(systemd-user:session): session opened for user lightdm(uid=117) by (uid=0)
Sep  6 15:23:58 waldonboksi lightdm: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty2 ruser= rhost= user=kotirosvo
Sep  6 15:24:03 waldonboksi lightdm: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty2 ruser= rhost= user=kotirosvo
Sep  6 15:24:07 waldonboksi lightdm: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/tty2 ruser= rhost= user=kotirosvo

```

## Lokitapahtuma 2

Haluan selvittää kuka on asentanut koneelle uusia ohjelmia

Loki löytyi polusta `var/log/apt history.log`

Avasin lokitiedoston komennolla `sudo less history.log`

Lokitiedoista selviää, että käyttäjä walter on asentanut speedtest-cli ohjelman. Tiedoista selviää myös päivämäärä ja aika.

```
Start-Date: 2022-09-06 10:26:28
Commandline: apt-get install speedtest-cli
Requested-By: walter (1000)
Install: speedtest-cli:amd64 (2.1.3-2)
End-Date: 2022-09-06 10:26:30
```

d)

#### Grep-testi 1

Etsin Var/log/auth.log kansiota kaikki walter hakusanalla tapahtuneet kirjautumiset

Lähdin etsimään lokimerkintöjä komennolla `sudo grep "walter" auth.log`

Lokitiedoista selviää esimerkiksi, milloin käyttäjä walter on kirjautunut sisään, mitä komentoja hän on syöttänyt ja missä hakemistoissa hän on pyörinyt.

```
walter@waldonboksi:/var/log$ sudo grep 'walter' auth.log
[sudo] password for walter:
Sep 6 09:30:12 waldonboksi lightdm: pam_unix(lightdm:session): session opened for user walter(uid=1000) by (uid=
Sep 6 09:30:12 waldonboksi systemd-logind[479]: New session 2 of user walter.
Sep 6 09:30:12 waldonboksi systemd: pam_unix(systemd-user:session): session opened for user walter(uid=1000) by
Sep 6 09:32:46 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/home/walter ; USER=root ; COMMAND=/usr/bin/rm testi
Sep 6 09:34:06 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/home/walter ; USER=root ; COMMAND=/usr/bin/rm testi
Sep 6 09:37:32 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/home/walter/testi ; USER=root ; COMMAND=/usr/bin/cp
Sep 6 09:58:23 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/apt-get update
Sep 6 10:26:22 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/apt-get install spe
Sep 6 11:23:40 waldonboksi sudo: walter : TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/adduser kotirosvo
```

#### Grep-testi 2

Yritän etsiä missä tiedossa on kirjoittamani sana "kissa".

Etsin tiedostoa komennolla `sudo grep -r "kissa"`

-r tarkoittaa, että haku tehdään kaikkiin hakemistoihin.

Sana kissa löytyi polusta home/walter/tehtava/maanantai

```
walter@waldonboksi:~$ sudo grep -r 'kissa'
tehtävä/maanantai/haku:kissa
walter@waldonboksi:~$
```

#### e) Päivitä kaikki ohjelmat ja asenna tietoturvapäivitykset

Ohjelmat voi päivittää komennolla `sudo apt-get upgrade`

Minulla ei ollut mitään uusia päivityksiä tullut asennettavaksi.

Googletin pwnkit haavoittuvuutta ja löysin että se voidaan päivittää komennolla

`sudo apt-get install policykit-1`

Minun koneellani oli jo valmiina tämä uusin versio.

Lähde löytyi osoitteesta: <https://security-tracker.debian.org/tracker/CVE-2021-4034>