

# **Linux Kommandolinjen**

Terje Berg-Hansen

[ITFakultetet.no](http://ITFakultetet.no)

# Linux Kommandolinjen

Av Terje Berg-Hansen.

Copyright © 2021 ITFakultetet.no – Alle rettigheter reservert

Publisert av ITFakultetet AS, Kåsabakken 28, 3804 Bø i Telemark, Norge

Denne E-boken brukes som dokumentasjon til disse kursene på ITFakultetet.no:

- Linux Workshop: Kommandolinjen
- Linux Sysadmin – trinn 1

Sjekk gjerne [www.itfakultetet.no](http://www.itfakultetet.no) for kursbeskrivelser og aktuelle kursdatoer.

# Forord

---

Denne E-boken er skrevet for den komplette nybegynner, men bør også fungere bra for de som har jobbet en del med kommandolinjen fra før, kanskje uten noen formell opplæring, men som har «Googlet» løsninger, klippet og limt litt, og gjerne vil ha litt større forståelse for hva som egentlig foregår når kommandoene gir forventede eller overraskende resultater – eller ingen resultater i det hele tatt.

Alle tilbakemeldinger mottas med takk, spesielt slike som kan forbedre boken og gjøre den mest mulig tilgjengelig og nyttig for leseren.

Oslo, 2021

Terje Berg-Hansen

Kursleder

ITFakultetet.no

Epost: [terje@itfakultetet.no](mailto:terje@itfakultetet.no)

# INNHOOLD

<b>Forord.....</b>	<b>4</b>
<b>Kapittel 1 Introduksjon og installering.....</b>	<b>10</b>
➔ Introduksjon til GNU/Linux.....	10
GNU/Linux blir til.....	10
Linux er et sikret flerbrukersystem.....	10
Noen grunner til å bruke Linux:.....	11
Frihet / Leverandøruavhengighet.....	11
Sikkerhet: tilnærmet virusfritt.....	11
Mengder av gratis programvare - enkelt installert og oppdatert gjennom internett.....	11
➔ Linux på Serveren.....	11
➔ Noen populære Server-distribusjoner.....	12
Debian.....	12
Ubuntu.....	12
Red Hat - RHEL / Centos / Fedora.....	12
SUSE - SLES / OpenSUSE Leap.....	12
➔ Installasjon av Ubuntu Desktop og Server.....	12
➔ Hva er kommandolinjen?.....	13
Grunnleggende bruk.....	13
Kommandoer versus museklikk.....	14
Tekstbaserte programmer.....	14
➔ history - gjenbruk av tidligere kommandoer.....	15
➔ .bashrc.....	16
➔ Tmux og Screen.....	16
tmux.....	16
screen.....	17
➔ Introduksjon til tekstbehandling med Vim.....	18
Behovet for en tekstbasert tekstbehandler.....	18
Vims særegenheter.....	18
Vims config-fil: .vimrc.....	22
Eksterne ressurser:.....	22
<b>Kapittel 2 Filsystemer, mapper og filer.....</b>	<b>23</b>
➔ Linux Filsystem og Systemfiler.....	23
➔ ls - list innholdet i en mappe.....	25
➔ stat - list status for filer og filsystem.....	25
➔ wc - tell antall linjer, ord og tegn i en tekst eller fil.....	26
➔ cd - change directory.....	27
➔ mkdir - Oppretter en ny mappe(make directory).....	27
➔ rmdir - Sletter en tom mappe.....	28
➔ rm (remove) - Sletter en eller flere mapper eller filer.....	28
➔ cp (copy) - Kopierer filer og mapper.....	28

➡ mv (move) - Flytter eller gir nytt navn til filer eller mapper.....	29
➡ ln - lag hard eller symbolsk lenke.....	30
ln - Lag en hard lenke (snarvei) til en fil eller mappe.....	30
ln -s - Lag en symbolsk eller soft lenke (snarvei) til en fil eller mappe.....	30
➡ df og du - vis størrelsen til partisjoner og mapper.....	30
df.....	30
du.....	31
➡ find - søk etter filer og mapper.....	31
Søke etter navn, type, filstørrelse og tid.....	32
Søke etter mapper/filer og endre de vi finner.....	32
Endre søkeresultatet med -exec.....	32
Endre søkeresultatet med xargs.....	32
➡ chown - endre eierskap til mapper og filer.....	32
➡ chmod - endre tilgangsrettigheter til mapper og filer.....	33
chmod med tall.....	34
chmod med bokstaver.....	34
➡ Komprimering og dekomprimering av filer og mapper.....	34
Komprimering med zip.....	35
Komprimering med gzip.....	35
Komprimering med bzip2.....	36
Pakking og komprimering med tar.....	36
➡ rsync - synkronisering av filer mellom maskiner.....	37
➡ ØVELSE Endre filnavn på mange filer samtidig med find og xargs.....	37
<b>Kapittel 3 Pakke- og brukerhåndtering.....</b>	<b>39</b>
➡ Pakkehåndtering fra kommandolinjen.....	39
➡ Installere og oppgradere DEB-pakker.....	39
DEB.....	39
APT.....	39
dpkg.....	41
➡ Installere og oppgradere RPM-pakker.....	42
➡ RPM - Pakkehåndtering med Red Hat Package Manager.....	42
RPM.....	42
YUM / DNF.....	42
rpm.....	44
➡ Brukerhåndtering fra kommandolinjen.....	45
Informasjon om en bruker.....	45
Legge til en ny bruker.....	45
Endre en eksisterende bruker.....	46
Slette en bruker fra systemet.....	47
Grupper.....	47
➡ /etc/passwd, /etc/shadow og /etc/group.....	48
<b>Kapittel 4 4: SSH / SCP / SFTP.....</b>	<b>51</b>
➡ Installasjon og konfigurering av OpenSSH - secure shell server.....	51
Installasjon.....	51
Konfigurering.....	51

➔ Bruk av aliaser via SSHs konfigurasjonsfil.....	52
➔ Passordløs innlogging.....	53
Innlogging med nøkler, uten passord.....	53
➔ Sikker kopiering av filer og mapper med scp.....	54
➔ SFTP - Sikker FTP.....	54
➔ SSH - tunneler.....	56
Eksempel 1:.....	56
Eksempel 2:.....	56
Eksempel 3:.....	57
<b>Kapittel 5 Data Wrangling.....</b>	<b>58</b>
➔ cat - skjøt sammen filer og mye mer.....	58
Eksempler:.....	59
➔ head og tail.....	60
head.....	60
tail.....	60
tail -f.....	60
➔ more og less.....	60
➔ date.....	61
➔ grep - fgrep - egrep - søk i tekstfiler.....	62
➔ sort - sorter tekstfiler.....	63
➔ uniq - Fjern duplikater.....	65
➔ tr (translate) - endre tegn i en tekst.....	66
➔ sed - søk og erstatt tekst.....	68
sed.....	68
➔ awk - et programmeringsspråk for behandling av tekst.....	69
gawks online manual:.....	70
➔ cut.....	70
➔ paste.....	73
➔ comm og diff.....	74
comm.....	74
diff.....	75
➔ split - del opp en fil i flere mindre filer.....	76
➔ Øvelse: Skriv direkte til en fil med echo og/eller cat.....	76
➔ Øvelse: Lese og endre en fil med while og read.....	77
➔ Øvelse: Finn de 20 mest brukte kommandoene dine.....	79
<b>Kapittel 6 Sikkerhet.....</b>	<b>81</b>
➔ Brannmur med UFW.....	81
➔ Port-scanning med nmap.....	82
Sjekk åpne porter med nmap.....	82
➔ Passord-cracking med ncrack.....	88
Moduler:.....	88
Eksempler:.....	88
➔ Kryptering av filer og epost med GnuPG.....	89
Installasjon av GnuPG.....	89
Lage offentlige og private nøkler.....	89

Opplasting av offentlig nøkkel til en nøkkel-server.....	91
Finne og importere andres offentlige nøkler.....	92
Kryptering og dekryptering av filer med GnuPG.....	92
Signering av filer og epost med GnuPG.....	93
➔ Passord-cracking med hashcat.....	95
<b>Kapittel 7 Jobber, tjenester og prosesser.....</b>	<b>99</b>
➔ Håndtering av jobber med bg, fg, jobs, nohup, & og ctrl+z.....	99
Forgrunn og bakgrunn.....	99
Kjøre jobber i bakgrunnen.....	100
Jobboversikt.....	100
Starte grafiske programmer.....	101
Starte programmer som forblir kjørende etter utlogging - med nohup.....	101
Avslutte programmer som ikke vil avslutte på vanlig måte med kill og killall.....	101
➔ Finn kjørende prosesser med ps.....	103
➔ Vis kjørende prosesser i en trestruktur med pstree.....	105
➔ systemctl - starte, stoppe og re-starte tjenester.....	107
➔ Cron og Crontab.....	108
Kommandoer for å sette opp crontab.....	108
Formatet til crontab-filen.....	108
Eksempler på crontab-oppføringer.....	108
En annen måte å gjøre det på.....	109
<b>Kapittel 8 Systemovervåking og loggsjekking.....</b>	<b>110</b>
➔ df - sjekk tilgjengelig diskplass.....	110
➔ free - sjekk tilgjengelig og brukt minne.....	111
➔ htop - top med mer grafisk oversikt.....	111
➔ sysctl - vis eller endre kjerne-parametere.....	112
➔ Nettverksovervåking med tcpdump.....	113
➔ Nettverksovervåking med iptraf.....	113
.....	114
➔ Sjekking av minnebruk og swapping med vmstat.....	115
➔ Overvåking av ressursbruken med top.....	116
➔ Sjekker MySQL-belastningen med mytop.....	117
➔ Sjekker Apache2-belastningen med apachetop.....	118
➔ Kommandoer for å håndtere kjerne-moduler.....	119
➔ uptime - vis oppetid og belastning.....	119
➔ lastlog - vis brukers siste login.....	120
➔ Oversikt over Linux loggsystem.....	121
➔ Sjekking av loggfiler.....	122
➔ Skrive til loggfiler.....	122
➔ journalctl.....	122
➔ Få en samlet logg-oversikt med logwatch.....	123
Installasjon.....	123
Bruk fra kommandolinjen.....	123
Konfigurerings.....	124
Dokumentasjon.....	124

<b>Kapittel 9 Nettverk.....</b>	<b>125</b>
➔ ip - vis og endre routing, network devices, interfaces og tunnels.....	125
➔ resolvectl - vis og endre navneservere.....	129
➔ netplan - vis og konfigurer nettverkskort.....	130
Konfigurasjon.....	130
Kommandoer.....	130
Eksempler:.....	130
➔ traceroute - spor rutingen til en maskin.....	131
➔ nmcli - håndter network manager fra kommandolinjen.....	133
➔ ss - socket utility program.....	135
Eksempler fra manualen (man ss).....	136
➔ iwlist - informasjon om trådløse nettverk.....	136
➔ tshark - wireshark fra kommandolinjen.....	139
Eksempler.....	140
➔ Øvelse: Finn tilkoblede maskiner i et nettverk med fping og arp-scan.....	141
arp-scan.....	142
➔ Øvelse: Hva er min eksterne ip-adresse?.....	142
<b>Kapittel 10 Skallskripting.....</b>	<b>144</b>
➔ Øvelse: Skript som teller antall forekomster av ordene i en tekstfil.....	144
Slik kan skriptet se ut:.....	145
➔ Øvelse: Skript for analyse av logger - som kan kjøres av cron.....	145
➔ Øvelse: Skript for oppretting eller konvertering av bilder.....	147
Bildebehandling med ImageMagick.....	147
Lagre tekst som bilde.....	148
.....	148
Endre størrelsen på alle bildene i en mappe.....	148
➔ Et par enkle triks.....	149
1. Start en webserver med en linje kode:.....	149
2. Sjekk hvilken web-server et nettsted kjører.....	150



# Kapittel 1

## Introduksjon og installering

### ➔ Introduksjon til GNU/Linux

#### GNU/Linux blir til

---

- Richard Stallman startet i 1983 prosjektet GNU for å lage et fritt operativsystem
- GNU = Gnu is Not Unix
- Linus Thorvalds lagde i 1991 et studentprosjekt han kalte Linux, som skulle være en Unix-lignende kjerne som kunne kjøres på vanlige PCer.
- GNU manglet en kjerne, og adopterte Linux-kjernen. Slik ble GNU/Linux et komplett operativsystem med en kjerne og et omkringliggende system av rutiner, verktøy og programmer.
- Idag kan Linux kjøres på PCer, Power PCer (Apple), Alpha-baserte maskiner, MIPS-baserte maskiner, IBMs S/390, ARM-maskiner og en rekke andre plattformer

#### Linux er et sikret flerbrukersystem

---

- Maskinvare var dyrt da Linux ble laget, og Linux er bygget for at mange brukere skal kunne bruke samme maskin. Brukerne er medlem av en eller flere grupper, og rettigheter tildeles på bruker- eller gruppenivå.
- Brukere kan være innlogget samtidig, kommunisere med hverandre og dele systemressurser på en intelligent måte.
- Linux er et operativsystem som håndterer protected mulittasking noe som innebærer at hver bruker kan kjøre mer enn en prosess samtidig. Prosessene kan kommunisere med hverandre, men er fullt beskyttet fra hverandre. Jobber kan kjøres i bakgrunnen, mens man fokuserer på den jobben som vises på skjermen.
- Filstrukturen er hierarkisk bygget opp gjennom en rot-mappe med undermapper. Lese- og skrivetillatelser gis til brukere eller grupper av brukere for hver mappe og hver fil. En vanlig bruker har ikke tilgang til f.eks. å slette viktige systemfiler, så hvis noen (en fremmed eller et virus) får tilgang til brukerens passord, kan ikke hele systemet ødelegges - kun denne brukerens egne mapper og filer.

## Noen grunner til å bruke Linux:

---

- **Frihet / Leverandøruavhengighet**

Linux og "Open Source" (åpen kildekode) programvare er gratis. Dette innebærer at lisensen er en "fri lisens", og den vanligste av disse er GPL (General Public License). Av denne lisensen framgår det at alle og enhver har rett til å bruke programvaren, distribuere programvaren, endre den, og distribuere endringene under forutsetning at den forblir lisensiert med GPL.

- **Sikkerhet: tilnærmet virusfritt**

Linux har så og si ingen virus. Det er nok ikke umulig å få det, men det er uhyre sjeldent at det opptrer fordi Linux er bygd på en måte som gjør det svært vanskelig for virus å trenge igjennom.

- **Mengder av gratis programvare - enkelt installert og oppdatert gjennom internett.**

Siden programvaren for det aller meste er fri og gratis, ligger den samlet i programvarekartoteker (brønner eller kilder) på internett. Det gjør at du kan installere og oppdatere ikke bare operativsystemet, men all programvare gjennom et par enkle klikk eller kommandoer.

## ➔ Linux på Serveren

En Linux-server er en system-administrators drøm. Linux tilbyr det beste og mest brukte innen web-servere, epost-servere, fil-servere, database-servere, media-streaming-servere, Hadoop-klynger mm. Linux-servere er stabile og sikre og blir stadig enklere å administrere.

Linux er mye brukt som web-server gjennom det såkalte LAMP-oppsettet. LAMP står for Linux, Apache, MySQL og Php. I praksis vil dette si at man setter opp en Linux-server med Apache web-server, MySQL database-server og Php skript-språk.

Det finnes en rekke verktøy for installasjon, administrasjon og overvåking av Linux-servere, og det er en stor community av Linux-entusiaster på diverse kanaler på internett som er behjelpelig hvis du står fast eller trenger løsning på et problem raskt. Et Google-søk er ofte nok til å vise deg en eller flere måter å løse problemet på.

Web-baserte grensesnitt, som f.eks. cockpit, gjør det enkelt å administrere de vanligste oppgavene, mens rot-tilgang via SSH (Secure SHell) gir en fantastisk detaljert kontroll over alle aspekter av serveren.

## ➔ Noen populære Server-distribusjoner

### Debian

---

Debian er en populær server-distro, som flere andre distroer bygger på, bl.a. Ubuntu. Debian er community-drevet, som innebærer at det ikke er ett selskap som har ansvar for utvikling, brukerstøtte osv.

### Ubuntu

---

**Ubuntu Server** har økt eksponensielt i popularitet de siste årene, i takt med Ubuntus generelle fremgang. Ubuntu støttes profesjonelt av firmaet bak Ubuntu- Canonical - og er en stabil og enkel installasjon. Den er også gratis (dersom du ikke ønsker support-avtale), og har en stor Community-støtte.

### Red Hat - RHEL / Centos / Fedora

---

**RHEL** (Red Hat Enterprise Linux) er en profesjonell, stabil og gjennomtestet server-installasjon, som støttes profesjonelt av Red Hat. For å ha et tilbud til de som ikke trenger Red Hats supportavtale, har man laget en Community-versjon av RHEL, som heter **Centos**, og som er identisk med den originale Red Hat serveren, minus support-avtale. Centos støttes nå også offisielt av Red Hat. **Fedora** er utviklerutgaven av RedHat, som inneholder nyere komponenter enn RHEL/Centos.

### SUSE - SLES / OpenSUSE Leap

---

Suse har en betydelig del av spesielt det europeiske servermarkedet med sin SLES (Suse Linux Enterprise Server). Etter at Suse ble kjøpt opp av Novell, har det blitt lagt inn mye av Novells Know-how i serveren, som bl.a støtter XEN-virtualisering og andre teknologier.

## ➔ Installasjon av Ubuntu Desktop og Server

**Desktop-utgaven** av Ubuntu kan lastes ned fra ubuntu nettsider:

<https://ubuntu.com/download/desktop>

**Server-utgaven** av Ubuntu kan lastes ned fra ubuntu nettsider:

<https://ubuntu.com/download/server>

### Testinstallasjon

Dersom du vil teste ut Ubuntu server, kan du installere den som en virtuell server i f.eks. VirtualBox.

Her er en lenke til en detaljert gjennomgang av installering til VirtualBox:

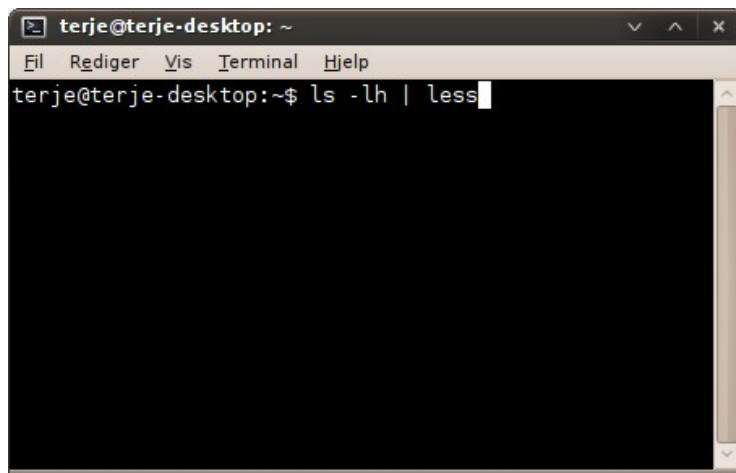
<https://www.wikihow.com/Install-Ubuntu-on-VirtualBox>

## ➔ Hva er kommandolinjen?

Kommandolinjen er et fleksibelt, allsidig verktøy som kan gjøre en rekke jobber raskt og effektivt. Den kan bli brukt interaktivt gjennom et *skall* eller *terminal-vindu* eller ved å skrive og kjøre såkalte *skallskript*, ofte kalt *Bash-skript* etter det populære Bash-skallet (**B**ourne **A**gain **S**hell). Resultatet en kommando produserer kan f.eks. sendes gjennom et "*rør*" (*pipe*), dvs. brukes som input til en annen kommando, det kan vises i et terminalvindu, printes eller lagres i en tekstfil. Resultatet av en kommando kan også lagres til en fil ved å omdirigere det fra standard output, som er skjerm, til et filnavn med tegnet `>` eller `>>` (det siste "appender" til fil) etterfulgt av banen/navnet til filen. For eksempel:

```
$ ls -lh > mappeinnhold.txt
```

Kommandoen i terminalvinduet nedenfor lister opp filene i en mappe (`ls`) med detaljert visning og i lettest format (`-lh`), og sender resultatet gjennom et rør (`|`) til programmet *less* som bl.a. lar deg bruke piltastene til å "scrolle" opp og ned i resultatet.



Kommandolinjen i et terminalvindu, -emulator eller skall

## Grunnleggende bruk

- Standard input = tastatur og standard output = skjerm
- Kommandoer skrives i et terminal-skall med standard input og resultatet sendes til standard input
  - hvis ikke input og/eller output er omdirigert med `<` eller `>`
- Omdirigering av output med `>` eller `>>` - omdirigerer fra skjerm til fil eller til ingenting (`/dev/null` - "the bit bucket")
  - `find -type f 2>/dev/null`

- Kjeding av kommandoer med `|` - output fra en kommando blir input til neste kommando
  - `sudo grep failed /var/log/secure | wc -l` (søker opp linjer som inneholder "failed" fra secure-loggen og sender resultatet til word count for å telle linjer, dvs. telle mislykkede innlogginger, passord-sjekker o.l.)
- Kjør to kommandoer etter hverandre med `&&` eller `||`
  - `mkdir mappe1 && cd mappe1`
  - `rm fil.txt || true`
- Initialiser variabler med `=` og referer til dem med `$`
  - `PATH = $PATH:/home/terje/bin`
- Bruk `(( ))` rundt matematiske beregninger og referer til dem med `$(( ))`
  - `$ echo $((4+2*3))`
  - `10`
- Bruk `{ }` til å erstatte noe med noe annet, og referer til det med `${ }`
  - `$ tekst="Dette er riktig"`
  - `$ echo ${tekst/er/var}`
  - Dette var riktig
- Kjør programmer i bakgrunnen med `&`
  - `gimp &`
- Bruk tab til å fylle ut det som mangler ("tab completion")
  - `cat fore + tab` fyller ut resten av filnavnet til : `cat forekomster_av_ord_i_war-and-peace.txt`
  - Gjelder også for programmer, kommandoer og noen steder også parametre
- Få hjelp via **man** og **info**
  - `man cut` (gir manualen til kommandoen [cut](#))

## Kommandoer versus museklikk

---

### Fordeler

- Raskere å bruke enn grafiske brukergrensesnitt (fingrene dine forlater aldri tastaturet)
- Konfigurerbare snarveier og taste-bindinger.
- Virker også når du ikke har tilgang til grafiske grensesnitt, f.eks. når du logger deg inn på en tjener gjennom et terminalvindu

### Ulemper

- Du må huske kommandoer og snarveier (selv om det finnes måter å forenkle dette på)
- Vanskelig å vise bilder og video (men ikke umulig)

## Tekstbaserte programmer

---

Kommandolinjen kan også brukes til å kjøre tekstbaserte programmer i terminalvinduet - også kalt **TUI-applikasjoner** (Text-based User Interface). TUI-applikasjoner kan være raskere og mer fleksible og

konfigurerbare enn sine grafiske motparter: GUI-applikasjoner (Graphical User Interface).

### Eksempler på tekstbaserte programmer

- Nettlesere
  - Lynx, Links, w3m
- Epost-programmer
  - Mutt, Pine
- Kalendere
  - Calcurse, cal
- Mediaspillere
  - Mop, Mp3blaster, play
- IRC
  - irssi
- Tekstbehandlere
  - Vim, Emacs, Nano, Joe etc

### ➔ history - gjenbruk av tidligere kommandoer

**history** er et program som lagrer et angitt antall kommandoer (som regel er default 1000) i en fil, og som inneholder kommandoer for å hente dem fram igjen.

#### Eksempler på bruk

##### 1) Finn foregående kommandoer:

a) Tast <Piltast opp> for forrige kommando

a) Tast <Piltast ned> for neste kommando

##### 2) Søk etter en tidligere kommando:

a) Tast <ctrl>+r og tast inn begynnelsen på søkeorde(ne)

b) Repeter <ctrl>+r til du finner riktig kommando

##### 3) Vis alle lagrede kommandoer:

```
$ history
```

##### 4) Vis n siste lagrede kommandoer:

```
$ history <n>
```

##### 5) Send alle lagrede kommandoer til egen fil:

```
$ history > history
```

## ➔ .bashrc

Den skjulte filen **.bashrc** ligger i brukerens hjemmemappe og inneholder default-innstillinger, path, systemvariabler, aliaser osv for den aktuelle brukeren.

I **.bashrc** kan du legge innstillinger som bare skal gjelde for deg. Dersom innstillingene skal gjelde for alle brukere, oppretter du i stedet en fil med et passende navn, og legger denne i mappen **/etc/profile.d/** (krever rot-tilgang).

Her er et par eksempler på hva du kan legge i din egen **.bashrc**

**alias upgrade='sudo apt update && sudo apt full-upgrade'** (for debian-baserte distroer)

**PATH=\$PATH:/home/terje/programmer** (legger til mappen programmer i søke-stien for kjørbare programmer)

**HISTSIZE=2000** (antall kommandoer som skal lagres i hist - filen - endret fra default 1000)

## ➔ Tmux og Screen

### tmux

Programmet tmux er glimrende hvis du trenger å ha flere terminalvinduer samtidig på en maskin uten grafisk grensesnitt. Det er også genialt hvis du f.eks. logger deg inn på en server med ssh, må avbryte og logge deg ut, men vil fortsette senere - uten å miste det du holdt på med.

Start tmux med denne kommandoen:

```
$ tmux
```

Etter en velkomstbeskjed (klikk enter for å bli kvitt den) er du klar til å lage flere vinduer. Screen bruker **<ctrl>+b** som kommandotast og her er de viktigste kommandoene:

```
$ <ctrl>+b+c = Lag nytt vindu (c = create)
$ <ctrl>+b+n = gå til neste vindu (n = next)
$ <ctrl>+b+x = slett vinduet du er i, når det siste er slettet, avsluttes
tmux
```

Men her er den beste:

```
$ <ctrl>+b+d = frigjør vinduene (d = detach)
```

Nå kan du logge ut fra serveren og komme tilbake dagen etter og logge deg inn, og så starter du tmux med denne kommandoen:

```
$ tmux a
```

(a for attach)

Og så kan du fortsette å jobbe der du slapp dagen før. Hvis du har flere gamle sesjoner kjørende, kan du taste:

```
$tmux a -t <nummer>
```

for å gjenopprette den sesjonen du vil gå inn i. Sesjonene nummereres med et løpenummer fra 0 og oppover.

**Dersom du ikke kan installere tmux, kan du antagelig installere screen, som er forløperen til, og fungerer som en enklere utgave av tmux**

## screen

---

Programmet screen er alternativet til tmux når du trenger flere terminalvinduer samtidig på en maskin uten grafisk grensesnitt.

Start screen med denne kommandoen:

```
$ screen
```

Etter en velkomstbeskjed (klikk enter for å bli kvitt den) er du klar til å lage flere vinduer. Screen bruker **<ctrl>+a** som kommandotast og her er de viktigste kommandoene:

**\$ <ctrl>+a+c** = Lag nytt vindu (c = create)

**\$ <ctrl>+a+n** = gå til neste vindu (n = next)

**\$ <ctrl>+a+a** = gå frem og tilbake mellom to vinduer (a = alternate)

**\$ <ctrl>+a+k** = slett vinduet du er i (k = kill)

**\$ <ctrl>+a+d** = frigjør vinduene (d = detach)



Nå kan du logge ut fra serveren og komme tilbake dagen etter og logge deg inn, og så starter du screen med denne kommandoen:

```
$ screen -r
```

(r = resume)

Og så kan du fortsette å jobbe der du slapp dagen før. Har du åpnet flere screen-sesjoner, får du en liste over dem, og må angi en id for å komme til den sesjonen du vil jobbe i.

Hvis du har flere gamle sesjoner kjørende, vil du få beskjed om det og blir bedt og å taste inn PID-nummeret (Prosess ID) til den sesjonen du ønsker å fortsette i (PID-nummerne til de aktuelle sesjonene vises på skjermen).

Hvis du starter screen uten -r, startes en ny sesjon som legges til evt. eksisterende sesjoner.

## ➔ Introduksjon til tekstbehandling med Vim

Vim står for VI Improved, og er som navnet antyder en forbedret utgave av den klassiske tekstbehandleren VI (uttales vi-ai). Det finnes flere tekstbehandlere som fungerer uten grafisk brukergrensesnitt - f.eks. Emacs, Nano og Joe - men Vim er mye brukt, ofte installert og ikke helt intuitiv i bruk, derfor kan det være på plass med en kort brukerveiledning til den.

### Behovet for en tekstbasert tekstbehandler

---

Det heter seg at "alt i Linux er tekstfiler", og f.eks. er de aller fleste konfigurasjonsfiler tekstbaserte. Når du skal redigere en tekstfil på en server, f.eks. via SSH, eller direkte på en server med en tekstbasert terminal, er Vim (eller en annen tekstbasert tekstbehandler) ofte svaret. Har man tilgang til et grafisk brukergrensesnitt vil nok mange velge f.eks. gedit, kate, geany, bluefish eller en annen grafisk editor, men det finnes også en gui-basert versjon av Vim -gVim, hvis man skulle ønske det.

### Vims særegenheter

---

Noe av det som forvirrer mest ved første møte med Vim er at programmet har to ulike modus - kommandomodus og redigeringsmodus. Når du starter Vim, starter programmet i kommandomodus. Slik åpner du en tekstfil for redigering med Vim:

```
$ vim tekstfil.txt
```

Dersom filen ikke finnes fra før vil Vim opprette en tom fil med filnavnet du tastet inn.

### Gå til redigeringsmodus

For å gå over i redigeringsmodus, slik at du kan begynne å skrive eller redigere, taster du bokstaven **i** (for *insert*) eller bokstaven **a** (for *append*). Flytt gjerne markøren med piltastene til linjen du vil redigere før du taster **i** eller **a**.

Du kan slette tegn på vanlig måte med tastene **<Del>** eller **<BackSpace>**.

### Gå til kommandomodus

Når du har redigert ferdig, må du gå over i kommandomodus igjen for å lagre og avslutte Vim. Dette gjøre du ved å taste **<escape>**.

### Lagre og avslutt

Når du er i kommandomodus, kan du gi Vim diverse kommandoer. Alle kommandoer begynner med tegnet kolon **:** etterfulgt av kommandoen, f.eks. slik:

**:w** (write) - lagrer filen, uten å lukke filen eller avslutte Vim

**:x** (exit) - lagrer filen, lukker den og avslutter Vim.

**:q** (quit) - avslutter Vim uten å lagre filen, dersom du ikke har gjort endringer)

**:q!** (quit anyway) - avslutter Vim uten å lagre filen, selv om du har gjort endringer.

### Andre nyttige kommandoer og funksjoner

#### Linjenummerering

Du kan slå av og på linjenummerering med disse kommandoene:

**:set number**

**:set nonumber**

Gå til en linje i et åpent dokument med kommandoen **:n** - hvor n er linjenummeret, f.eks vil **:234** flytte markøren til linje 234

Du kan åpne et dokument og gå direkte til en linje i dokumentet ved å skrive **+** og linjenummeret etter filnavnet når du åpner filen, f.eks slik:

```
vim main.cfg +367
```

#### Angre

**u** - angre siste endring (kan repeteres)

### ***Søke etter tekst***

**/** (søk) - skriv søkeord rett etter **/**, f.eks. slik:

**/test** - søker etter første forekomst av ordet test.

**n** (next) - søker etter neste forekomst av ordet test.

Vil du gjøre "case insensitive" søk, dvs. ikke skille mellom stor og små bokstaver, gjør du dette ved å sette vim til å være case insensitive før du søker, slik:

**:set ic** (ic står for: ignore case)

Etter søket kan du sette Vim tilbake til case sensitive modus slik:

**:set noic**

### ***Søk og erstatt***

**:%s/ord1/ord2** - erstatter første forekomst av ord1 med ord2 (søker i hele teksten)

**:%s/ord1/ord2/g** - erstatter alle forekomster av ord1 med ord2 ( i hele teksten)

**:%s/ord1/ord2/gc** - erstatter alle forekomster av ord1 med ord2 og ber om bekreftelse for hver erstatning (i hele teksten)

**:%s/ord1/ord2/i** - erstatter første forekomst av ord1 med ord2 uten å skille mellom store og små bokstaver (i hele teksten)

**:%s/ord1/ord2/I** - erstatter første forekomst av ord1 med ord2 og skiller mellom store og små bokstaver (i hele teksten) - dette er også default innstilling, men kan brukes etter å ha gjort om default til *case insensitive* med kommandoen **:set ignorecase**

### ***Slette tekst***

**dw** - sletter ett ord

**dd** - sletter en hel linje

### ***Kopiere og lime inn tekst***

**yy** - kopierer en linje til minnet

**yn** - kopierer n+1 linjer tekst til minnet

**p** - limer inn kopiert tekst

### ***Åpne flere filer i hvert sitt vindu (splittet skjerm)***

Du kan åpne flere filer samtidig, og la Vim plassere dem i hvert sitt vindu, enten horisontalt eller vertikalt, med disse kommandoene:

```
vim -o fil1.txt fil2.txt fil3.txt (splitter skjermen i tre horisontale vinduer)
vim -O fil1.txt fil2.txt fil3.txt (splitter skjermen i tre vertikale vinduer)
```

Du kan så redigere teksten i hvert vindu, f.eks. lagre og avslutte vinduet med **:x**, og bla til neste vindu med kommandoene: **<ctrl+w>+pil ned** eller **<ctrl+w>+pil opp** - eller ved vertikal deling, med **<ctrl+w>+pil venstre** eller **<ctrl+w>+pil høyre**. **<ctrl>+w+w** skifter frem og tilbake mellom to vinduer.

### Splitte et vindu i to deler

Du kan splitte et vindu horisontalt med kommandoen **:split**, og vertikalt med kommandoen **:vsplit**

Tast **<ctrl>+w+w** for å flytte markøren fra det ene vinduet til det andre.

Det nye vinduet vil inneholde det samme dokumentet som det gamle. Du kan redigere et nytt dokument i det nye (eller gamle) vinduet med kommandoen **:edit <filnavn>**

### Vise forskjellene mellom to filer med vimdiff

Programmet **vimdiff** lar deg sammenligne innholdet i to eller flere filer. Filene åpnes i vertikalt splitede vinduer, og ulikhetene markeres med fargekoder. Skriv filnavnene til filene du vil sammenligne som parametre til vimdiff, slik:

```
vimdiff <fil1> <fil2> <fil3>
```

Filene kan redigeres på vanlig måte

### Åpne flere filer i hver sin fane

Du kan åpne filer i faner i stedet for i egne vinduer. Dersom du redigerer en tekst og vil åpne en ny fil i en egen fane, kan du bruke denne kommandoen: **:tabe myfile.txt**. Du kan bla mellom fanene med kommandoene: **<ctrl>+pgup>** og **<ctrl>+pgdn>**

Du kan åpne flere filer direkte i faner ved å laste dem inn med flagget: **-p**, slik

```
vim -p first.txt second.txt
```

Her er noen flere kommandoer relatert til faner:

<b>:tabedit {filnavn}</b>	åpner en fil i en ny fane
<b>:tabfind {filnavn}</b>	søker etter filnavn (bruk tab) og åpner filen i ny fane
<b>:tabclose</b>	lukker gjeldende fane

```
:tabclose {i}      lukker fane nummer i  
:tabonly          lukker alle andre faner enn den gjeldende
```

### Vims config-fil: **.vimrc**

Du kan opprette en config-fil for vim i hjemmemappen din. Kall filen **.vimrc** (punktumet angir at det er en skjult fil). I denne filen kan du angi default-verdier for oppstart av vim, feks:

```
set number  
colorscheme darkblue
```

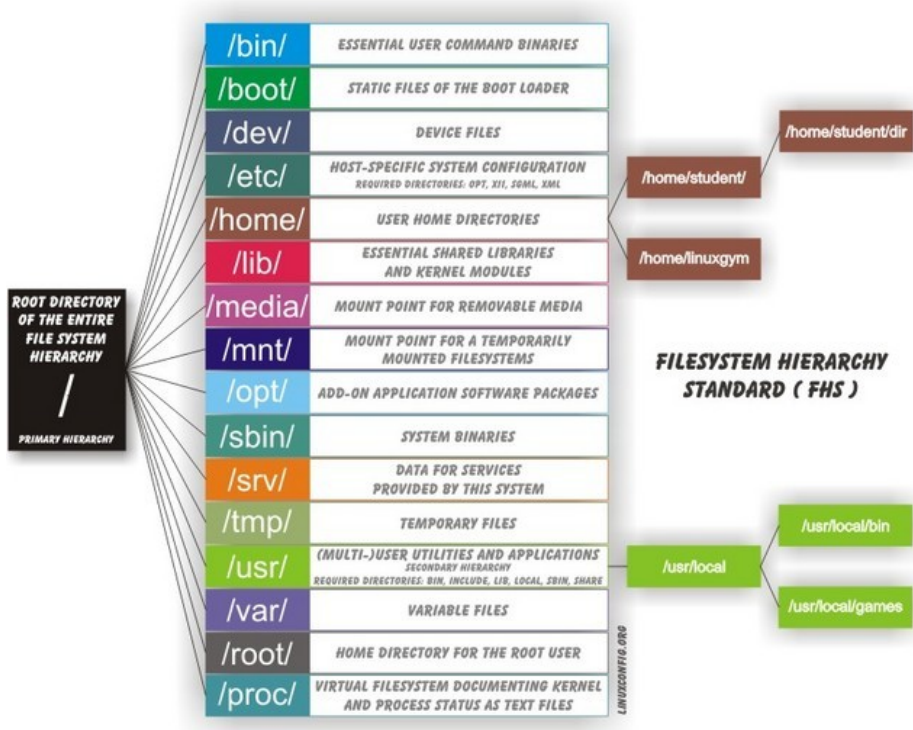
### Eksterne ressurser:

- <http://www.vim.org> - Vims offisielle hjemmeside, med dokumentasjon, nedlasting etc,
- <http://vim.wikia.com/> - Vim Tips og triks
- <http://vimdoc.sourceforge.net/> - Vim dokumentasjon

# Kapittel 2

## Filsystemer, mapper og filer

➔ Linux Filsystem og Systemfiler



Bildet over viser standard-mapper i en vanlig Linux-installasjon. Øverste nivå kalles gjerne **rot-nivå** og angis med:

/

**Brukernes hjemmemapper** lagres i mappen

**/home**

Feks: /home/petter (Denne mappen tilsvarer mer eller mindre "Mine Dokumenter" i Windows)

**Systemets konfigureringsfiler** ligger lagret i mappen:

**/etc**

**Systemets programmer** ligger lagret i mappen:

**/bin**

**Midlertidige filer** ligger lagret i mappen:

**/tmp**

**Filer som kan brukes av flere brukere** ligger i mappen:

**/usr**

Feks. /usr/share/wallpapers (mappe med bakgrunnsbilder til skrivebordet)

**Flyttbare media**, som CD-rom, DVD, USB, Ipod osv finner man i mappen:

**/media**

Når Linux-kjernen lastes ved oppstart, lages det et filsystem i mappen:

**/proc**

I denne mappen lagres innstillinger og parametre som brukes av kjernen. Man kan lese og endre disse parametrene ved å lese eller skrive til filer i undermappen:

**/proc/sys**

For eksempel ligger det en fil i mappen **/proc/sys/wm** som heter **swappiness**. Denne filen inneholder et parameter for hvor ofte kjernen skal skrive til swap-filen - mellom 0 (sjeldnest) og 100 (oftest). Du kan lese gjeldende innstilling ved å lese filen:

```
$ cat /proc/sys/vm/swappiness
$ 60
```

og du kan endre innstillingen ved å skrive til filen:

```
$ sudo echo "30" > /proc/sys/vm/swappiness
```

Dette setter parameteret til 30, som gjør at kjernen skriver sjeldnere til swap-området. Merk at endringen ikke beholdes ved restart av kjernen

## ➔ ls - list innholdet i en mappe

*ls* er antagelig den kommandoen du vil bruke mest. *ls* er en forkortelse for *list* og kommandoen lister opp filer og undermapper i den mappen du befinner deg i - dvs i din *working directory* (kommandoen ***pwd*** viser deg hvilken mappe dette er).

*ls* kan brukes med ett eller flere av følgende parametre. (Merk at man alltid skriver en bindestrek før parametrene):

```
$ ls -l   Lister filer og undermapper i detaljert (langt) format
$ ls -lh  Lister filer og undermapper i detaljert og "human readable format", som f.eks. å viser filstørrelser i
          Megabytes istedenfor bytes
$ ls -a   Lister alle filer, inkludert skjulte filer
$ ls -t   Lister filer sortert etter når de sist ble endret
$ ls -S   Lister filer sortert etter størrelse
$ ls -r   Lister filer sortert i omvendt (reversert) rekkefølge
```

## ➔ stat - list status for filer og filsystem

**stat** lister opp informasjon om en eller flere filer eller filsystemer.

### OPTIONS

**-L, --dereference**  
follow links

**-f, --file-system**  
display file system status instead of file status

**-c --format=FORMAT**  
use the specified FORMAT instead of the default; output a newline after each use of FORMAT

**--printf=FORMAT**



like `--format`, but interpret backslash escapes, and do not output a mandatory trailing newline; if you want a newline, include `\n` in `FORMAT`

**-t, --terse**

print the information in terse form

### Eksempler:

```
$ stat log.txt
File: log.txt
Size: 114          Blocks: 8          IO Block: 4096   regular file
Device: 902h/2306d Inode: 105124502   Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/   terje)   Gid: ( 1000/   terje)
Context: system_u:object_r:user_home_t:s0
Access: 2020-11-25 02:44:21.568729138 +0100
Modify: 2020-04-27 16:11:58.000000000 +0200
Change: 2020-10-03 13:16:17.657501333 +0200
Birth: -
$ stat -t log.txt
log.txt 114 8 81b4 1000 1000 902 105124502 1 0 0 1606268661 1587996718
1601723777 0 4096 system_u:object_r:user_home_t:s0
$ stat -f log.txt
File: "log.txt"
ID: 9f5d5b62d777948e Namelen: 255      Type: ext2/ext3
Block size: 4096      Fundamental block size: 4096
Blocks: Total: 476160368 Free: 318903772 Available: 294698690
Inodes: Total: 121012224 Free: 119242500
```

## ➔ **wc** - tell antall linjer, ord og tegn i en tekst eller fil

**wc (word count)** gir oss antall linjer, ord og tegn i en pipe eller en tekstfil.

### Parametere

**-l** kun antall linjer

**-w** kun antall ord

**-c** kun antall tegn

### Eksempler på bruk:

```
$ wc war-and-peace.txt
63846  562489 3266164 war-and-peace.txt
```

```
$ wc -l war-and-peace.txt
63846 war-and-peace.txt
$ wc -w war-and-peace.txt
562489 war-and-peace.txt
$ wc -c war-and-peace.txt
3266164 war-and-peace.txt
$ echo "Dette er en tekst" | wc -c
18
$ echo -n "Dette er en tekst" | wc -c
17
```

**MERK:** echo legger til et linjeskift (\n), som kan fjernes med flagget **-n**

## ➔ cd - change directory

cd (change directory) - Bytter til en annen mappe

### **Bruk:**

cd <sti til ny mappe>. Stien kan være absolutt eller relativ.

### **Eksempler:**

```
$ cd .. (bytter til mappen som ligger to nivåer opp).
$ cd (bytter til hjemmemappen din)
$ cd ~/Musikk (bytter til mappen Musikk i hjemmemappen din)
$ cd - (bytter til forrige mappe du var i)
$ cd / (bytter til rot-mappen i filsystemet)
```

## ➔ mkdir - Oppretter en ny mappe(make directory)

### **Bruk:**

\$ mkdir Bilder (Oppretter mappen *Bilder*)

\$ mkdir -p mappe1/mappe2/mappe3 (Oppretter mappe3 og også mappe2 og mappe2 hvis de ikke finnes fra før)

## ➔ rmdir - Sletter en tom mappe

### Bruk:

\$ rmdir Dokumenter (sletter mappen Dokumenter, men bare hvis mappen er tom)

\$ rmdir -p mappe1/mappe2/mappe3 (Sletter mappe1 og mappe2 og mappe3 hvis de er tomme)

## ➔ rm (remove) - Sletter en eller flere mapper eller filer

rm er kommandoen for å slette filer, men kan også slette hele mapper og undermapper.

### Eksempler:

```
$ rm fil.txt (sletter filen fil.txt)
```

```
$ rm -i fil.txt (spør om du virkelig vil slette filen fil.txt, sletter  
hvis du bekrefter. -i står for interaktiv)
```

```
$ rm -rf Dokumenter (sletter hele mappen Dokumenter, inkludert mappens  
filer og undermapper, uten flere spørsmål)
```

```
$ rm -I *.txt (sletter alle dokumenter som har navn som slutter med .txt,  
men ber om bekreftelse etter å ha slettet tre dokumenter. -I er en svakere  
beskyttelse enn -i, som ber om bekreftelse for hver fil som skal slettes.)
```

## ➔ cp (copy) - Kopierer filer og mapper

### Bruk:

```
cp <kilde> [<sti>/]<kopi>
```

### Eksempler:

```
$ cp fil.txt ..
```

- kopierer fil.txt til mappen ett nivå opp

```
$ cp -r Mp3/ Musikk/
```

- kopierer mappen Mp3 til mappen Musikk, inkludert alle undermapper og filer i mappen Mp3. -r står for *recursive*.

Merk at -r endrer fil-eierskap til den som utfører kopieringen. For å beholde originale filegenskaper, bruk:

```
$ cp -a          (som også kopierer rekursivt)
```

```
$ cp -u fil.doc /home/petter/dokumenter
```

- kopierer filen fil.doc til mappen /home/petter/dokumenter, men bare hvis filen ikke finnes der fra før, eller hvis filen er nyere enn den som finnes der fra før. -u står for *update*

## ➔ **mv** (move) - Flytter eller gir nytt navn til filer eller mapper

Merk: Linux har ingen egen kommando for å endre navn, men bruker mv til å gjøre denne operasjonen.

### Bruk:

```
$ mv filnavn ..
```

- flytter *filnavn* en mappe opp i filstrukturen

```
$ mv gammelnavn nyttnavn
```

- filen *gammelnavn* heter nå *nyttnavn*

```
$ mv /home/petter/gammelnavn /home/petter/video/nyttnavn
```

- flytter og gir nytt navn til filen *gammelnavn*

## ➔ ln - lag hard eller symbolsk lenke

Forskjellen mellom en hard og en symbolsk lenke er i korte trekk at en symbolsk lenke peker til en fil, mens en hard lenke peker til filens inode. Når man oppretter en fil, lages det 1 hard lenke til filen. Oppretter man en ny hard lenke er det 2 likeverdige harde lenker til filen. Når den siste harde lenken er slettet, slettes også filens inode (den blir *unlinked*). Sletter man en fil, vil den symbolske lenken ikke lenger virke, men en hard lenke vil fortsatt virke, siden den peker til filens inode.

En hard lenke er en mindre fleksibel løsning enn en symbolsk lenke (se nedenfor), og kan ikke brukes på tvers av filsystemer.

### ln - Lag en hard lenke (snarvei) til en fil eller mappe.

---

#### Bruk:

```
$ ln /home/petter/fil.txt /home/petter/Skrivebord/fil.txt
```

(lager en lenke til filen fil.txt. Lenken ligger i mappen Skrivebord)

### ln -s - Lag en symbolsk eller soft lenke (snarvei) til en fil eller mappe.

---

#### Bruk:

```
$ ln -s /home/petter/fil.txt /home/petter/Skrivebord/fil.txt
```

(lager en symbolsk lenke til filen fil.txt. Lenken ligger i mappen Skrivebord)

## ➔ df og du - vis størrelsen til partisjoner og mapper

### df

---

**df** - Viser partisjoner og hvor mye lagringsplass de har, samt hvor mye som er brukt og ledig.

#### Bruk:

```
$ df -h
```

(viser ledig plass "human readable format", dvs. Gigabytes, Megabytes etc.)

```
$ df -l
```

(viser kun ledig plass på lokale filsystemer)

## du

**du** - Viser hvor mye lagringsplass som blir brukt av den aktuelle mappen og dens undermapper

**Bruk:**

```
$ du -h
```

(lister i *"human readable format"*)

```
$ du -s
```

(summerer opp for hver mappe)

```
$ du -c
```

(viser en totalsum)

## ➔ find - søk etter filer og mapper

**find** er et kraftig verktøy for å søke etter mapper og filer. I motsetning til locate (mlocate eller slocate på noen systemer) bruker ikke find en indeksert database, men søker gjennom filsystemet i sanntid. Dette kan ta litt tid, men til gjengjeld har find flere muligheter til bl.a. å endre filene det søkes etter.

```
Syntaks:  find [-H] [-L] [-P] [-D] [-O]
           [bane]
           [ -type [-f] [-d] ]
           [ -name ]
           [ -amin, -cmin, -mmin [-] [+] <antall minutter>]
           [ -size [-] [+] <antall> [b] [k] [M] [G] ]
```

De tre første parametrene: -H, -L eller -P angir om søket skal følge symbolske lenker eller ikke, det vil si, hvis det dukker opp en symbolsk lenke i søkeresultatet, f.eks.:

## Eksempler på bruk:

### Søke etter navn, type, filstørrelse og tid

```
$ find -name "*.txt" (søker i den mappen du er i og dens undermapper -  
etter filer og mapper som ender med .txt)  
$ find / -type f -name "core" (søker i alle mapper i filsystemet etter  
filer som heter core)  
$ find -mmin -1 (søker etter filer og mapper i den mappen du står i, som  
er endret for mindre enn ett minutt siden).  
$ man find (lister opp alle valgene find har)
```

### Søke etter mapper/filer og endre de vi finner

med **find** kan vi også utføre operasjoner på søkeresultatet, som for eksempel endre eieskap eller tilgangsrettigheter, slette filer og mapper etc.

### Endre søkeresultatet med -exec

```
$ find /home/bruker/public_html -type d -exec chmod 755 {} \; (finner  
alle mapper i brukerens apache-hjemmemappe m/undermapper og gir dem  
tilgang 755)  
$ find /home/bruker/public_html -type f -exec chmod 644 {} \; (finner  
alle filer i brukerens apache-hjemmemappe m/undermapper og gir dem tilgang  
644)  
$ find /home/bruker/public_html -name .htaccess -exec rm {} \; (fjerner  
alle .htaccess-filer i brukerens apache-hjemmemappe og dens undermapper)
```

### Endre søkeresultatet med xargs

```
MERK: Istedenfor -exec kan vi også lage et rør (med | ) som sender  
resultatet til xargs etterfulgt av en kommando, f.eks. slik:  
$ find /home/bruker/public_html -type d | xargs chmod 755 (finner alle  
mapper i brukerens apache-hjemmemappe m/undermapper og gir dem tilgang  
755)  
$ find /home/bruker/public_html -type f | xargs chmod 644 (finner alle  
filer i brukerens apache-hjemmemappe m/undermapper og gir dem tilgang 644)
```

## ➡ chown - endre eierskap til mapper og filer

**chown** er kommandoen for å endre eierskap til mapper og filer.

Syntaksen for **chown** er denne:

```
$ sudo chown <brukernavn> [:<gruppenavn>] mappe[r] og/eller fil[er]
```

#### Eksempler:

**\$ sudo chown ole:apache test.html** (setter eier til ole og gruppe til apache for filen test.html)

**\$ sudo chown petter pettersmappe** (setter eier til petter for mappen pettersmappe, men ikke innholdet i mappen (endrer ikke gruppe))

**\$ sudo chown petter pettersmappe/\*** (setter eier til petter for innholdet i mappen pettersmappe, men ikke selve mappen, eller innholdet i undermapper (endrer ikke gruppe))

**\$ sudo chown -R :felles fellesmappe** (setter gruppe til felles for mappen fellesmappe og alt den inneholder)

## ➔ chmod - endre tilgangsrettigheter til mapper og filer

Mapper og filer blir opprettet med default tilgangsrettigheter. Disse kan man se (og evt. endre) med kommandoen **umask**, og de kan konfigureres ved å sette en umask-verdi i filen `/etc/pofile`, eller enda bedre i en egen fil i mappen `/etc/profile.d/` - eller eventuelt lokalt i brukerens `~/.bashrc` - fil.

**chmod** er kommandoen for å endre tilgangsrettighetene til mapper og filer **etter** at de er opprettet.

Først litt om rettighetene. Linux deler brukerne i tre hoveddeler:

1. Eier - den brukeren som står som eier av mappen eller filen (angitt med bokstaven **u** for user)
2. Gruppe - den gruppen som mappen eller filen tilhører (angitt med bokstaven **g** for group)
3. Alle andre - alle brukere som ikke hører inn under 1. eller 2. (angitt med bokstaven **o** for other)

Tilgangsrettighetene er også delt i tre deler:

1. Lese-tilgang - som angis ved tallet **4** eller bokstaven **r**
2. Skrive-tilgang - som angis ved tallet **2** eller bokstaven **w**
3. Kjøre-tilgang - som angis ved tallet **1** eller bokstaven **x**

**MERK:** For mapper er "kjøretilgangen" definert som tilgang til å åpne mappen. For filer er kjøretilgang definert som tilgang til å kjøre filen som et program

Tallene som definerer tilgangsnivåene er laget slik at de gir unike kombinasjoner:

- Kun kjøretilgang = 1,
- Kun skrivetilgang = 2
- Kjøre- og skrivetilgang = 3,



- Kun Lesetilgang = 4
- Lese- og kjøretilgang gir  $4+1=5$ ,
- Lese- og skrivetilgang gir  $4+2 = 6$ .
- Alle tilganger gir  $4+2+1= 7$

Det vil si at vi med ett siffer kan angi riktig kombinasjon av rettigheter. Vi kan sette tilgangsrettigheter for de tre brukergruppene, og dermed får vi en kombinasjon av tre siffer, en for eier, en for gruppe og en for alle andre. Rettighetene kan angis med tall eller bokstaver.

Her er noen eksempler på hvordan endring av tilgangsrettigheter ser ut i praksis:

## chmod med tall

---

**\$ chmod 755 mappe1** (Eier har alle rettigheter, gruppen og alle andre har tilgang til å åpne mappen og lese innholdet)

**\$ chmod 700 mappe2** (Eier har alle rettigheter, gruppen og alle andre har ingen tilgang)

**\$ chmod 775 mappe3** (Eier og gruppen har alle rettigheter, alle andre har tilgang til å åpne mappen og lese innholdet)

**\$ chmod 644 fil1.txt** (Eier har lese- og skrivetilgang, gruppen og alle andre har kun lesetilgang)

**\$ chmod 500 program1** (Eier har lese- og kjøretilgang, alle andre har ingen tilganger)

**\$ find fellesmappe/ -type f | xargs chmod 664** (Finner alle filer i mappen fellesmappe, og dens undermapper, og setter tilgangen til lese+skrive for eier og gruppe, og kun lese for andre)

## chmod med bokstaver

---

**\$ chmod +x program2** (legger til kjøretilgang for alle brukere)

**\$ chmod u+x program1** (legger til kjøretilgang for eieren av program1)

**\$ chmod o-w \*.txt** (fjerner skrivetilgang for andre enn eier og gruppe til alle filer i mappen med navn som slutter på **.txt**)

**OBS!** Sett aldri alle mapper og filer til 777 på en Linux-maskin (feks. med `sudo chmod -R 777 /`) - da vil den slutte å fungere. Det er viktige systemfiler som ikke vil kjøre med en så usikker tilgang.

## Komprimering og dekomprimering av filer og mapper

Linux har flere ypperlige kommandolinjeverktøy for pakking og komprimering / dekomprimering av filer og mapper med filer.

Her er en kort oversikt:

## Komprimering med zip

---

zip er en nyttig kommando siden den lager arkiver med komprimerte filer som er kompatible med bl.a. Microsoft Windows.

### **Eksempler på bruk av zip/unzip:**

\$ zip *filnavn.zip filnavn*

- oppretter arkivet *filnavn.zip* og kopierer en komprimert versjon av filen *filnavn* inn i arkivet.

\$ zip *arkivnavn.zip \**

- oppretter arkivet "arkivnavn.zip", komprimerer alle filer i gjeldende mappe og kopierer dem inn i arkivet.

\$ unzip *filnavn.zip*

- oppretter filen *filnavn* som en dekomprimert versjon av filen *filnavn.zip*.

## Komprimering med gzip

---

**gzip** er det mest brukte zip-formatet på Linux, og brukes gjerne sammen med arkiv-programmet *tar* (se nedenfor)

**gunzip** er kommandoen for å dekomprimere filer som er komprimert med gzip

### **Eksempler på bruk av gzip/gunzip:**

#### **Filer**

\$ gzip *filnavn*

- gzipper filen *filnavn* og gir den det nye navnet: *filnavn.gz*

\$ gzip -k *filnavn*

- gzipper filen *filnavn* og gir den det nye navnet: *filnavn.gz*, men beholder originalfilen (k = keep)

\$ gunzip *filnavn.gz*

- dekomprimerer filen *filnavn.gz* og gir den navnet *filnavn*

#### **Mapper**

\$ gzip -rv *mappenavn*

- gzipper alle filene i mappen *mappenavn* og gir dem nye navn med *.gz* endelse

\$ gunzip -rv *mappenavn*

- dekomprimerer alle filene i mappen *mappenavn* og fjerner endelsen *.gz*

## Komprimering med bzip2

---

**bzip2** gir en meget god komprimering, og blir mer og mer brukt. Dekomprimering gjøres med kommandoen **bunzip2**. **bzip2/bunzip2** brukes på tilsvarende måte som gzip/gunzip:

### **Eksempler på bruk av bzip2/bunzip2:**

#### **Filer**

```
$ bzip2 filnavn
- bzipper filen filnavn og gir den det nye navnet: filnavn.bz2
$ bunzip2 filnavn.bz2
- dekomprimerer filen filnavn.bz2 og gir den navnet filnavn
```

#### **Mapper**

```
$ bzip2 mappenavn/* (merk forskjellen fra gzip)
- bzipper alle filene i mappen mappenavn og gir dem nye navn med .bz2 endelse
$ bunzip2 mappenavn/* (merk forskjellen fra gzip)
- dekomprimerer alle filene i mappen mappenavn og fjerner endelsen .bz2
```

## Pakking og komprimering med tar

---

**tar** (Tape ARchive) er et kraftig verktøy som er mye brukt i Linux-verden, både til å samle filer i et arkiv, og til å komprimere/dekomprimere filer og mapper. Dette kan gjøres med samme kommando.

### **Eksempler på bruk av tar:**

```
$ tar -cf arkivnavn.tar filnavn1 filnavn2 filnavn3
- samler filene filnavn1 filnavn2 filnavn3 i arkivet arkivnavn.tar
```

```
$ tar -xf arkivnavn.tar
- trekker ut filene filnavn1 filnavn2 filnavn3 fra arkivet arkivnavn.tar
```

```
$ tar -czf arkivnavn.tar.gz filnavn1 filnavn2 filnavn3
- samler filene filnavn1 filnavn2 filnavn3 i det komprimerte arkivet arkivnavn.tar.gz
```

```
$ tar -xzf arkivnavn.tar.gz
- trekker ut og dekomprimerer filene filnavn1 filnavn2 filnavn3 fra det komprimerte arkivet arkivnavn.tar.gz
```

```
$ tar -tf arkiv.tar
- lister opp innholdet i arkivet arkiv.tar
```

```
$ tar -tzf arkiv.tar.gz
```

- lister opp innholdet i det komprimerte arkivet *arkiv.tar.gz*

```
$ tar -rf arkiv.tar filnavn4
```

- legger til filen *filnavn4* i slutten av arkivet *arkiv.tar*

Sjekk gjerne tar-manualen for flere valgmuligheter:

**\$ man tar**

## ➔ rsync - synkronisering av filer mellom maskiner

**rsync** ble lansert i 1996 som et terminal-program for å synkronisere mapper eller hele trestrukturer mellom ulike steder på en maskin, eller mellom to maskiner. **rsync** blir ofte brukt til f.eks. sikkerhetskopiering.

En av de viktigste egenskapene ved **rsync** er at den bruker *checksums* til å sjekke filene - om alle, ingen eller noen blokker er endret siden sist. Kun de blokkene som er endret blir overført. Det sparer tid og båndbredde. Hvis første gangs synkronisering tar timer, vil de påfølgende kunne ta minutter, avhengig av hvor mye som er endret.

### Eksempler:

```
$ rsync -a /home/terje/mappe1/ terje@itfakultetet.no:mappe1/
```

**-a** står for "**archive mode**", som bevarer symbolske lenker, eierskap og tilgangsrettigheter mm.

```
$ rsync -a /home/terje/utvikling2/synctest/ terje4:synctest/
```

Det siste eksemplet forutsetter en *.ssh/config* - fil hvor *terje4* er definert med *HostName*, *User* og *Port*

## ➔ ØVELSE

### *Endre filnavn på mange filer samtidig med find og xargs*

I denne lille øvelsen vil vi søke opp alle konfig-filene i en mappe, definert som at de har filendelsen **.cfg** og gi dem nytt navn ved å legge **.gammel** til filnavnet.

Her er syntaksen til *find* med *xargs* til å endre navnene

```
$ find </sti/til/mappe/> -name "*.cfg" --print0 | xargs --null -I{} mv {} {}.gammel
```

Gjennomføring:

```
1) La oss først lage en mappe og gå inn i den:
$ mkdir config
$ cd config
2) Så lager vi noen tomme config-filer og sjekker at de er laget:
$ touch 1.cfg 2.cfg 3.cfg 4.cfg
$ ls
1.cfg 2.cfg 3.cfg 4.cfg
3) så bruker vi find til å gi dem nytt navn, og sjekker at det gikk bra
$ find -name "*.cfg" -print0 | xargs --null -I{} mv {} {}.gammel
$ ls
1.cfg.gammel 2.cfg.gammel 3.cfg.gammel 4.cfg.gammel
```

**Forklaring:**

1. **find** søker opp alle filer med filendelse **.cfg**
2. **-print0** gir beskjed til find om å ikke printe linjeskift for hver fil den finner, men et null-tegn. Default for find er **-print**, som lager linjeskift etter hver funnet fil
3. Send filnavnene til xargs med **|**
4. Parameteret **--null** (evt **-0**) forteller xargs at hvert element er avsluttet med null-tegn og ikke whitespace
5. Parameteret **-I{}** sier at vi skal utføre en erstatning av tegn og **mv {}** sier flytt alle elementene til **{}.gammel**. (**{}** symboliserer alle elementene som xargs mottar)

# Kapittel 3

## Pakke- og brukerhåndtering

### ➔ Pakkehåndtering fra kommandolinjen

Ulike Linux distroer bruker ulike applikasjonspakker (installerbare programmer). En *pakke* i dette tilfelle er en måte å håndtere hvordan applikasjoner installeres i et system, hvordan håndtere dets avhengigheter av andre pakker osv. Pakken inneholder med andre ord programmet som skal installeres samt informasjon om hvilke andre programmer som må være installert for at programmet skal kunne kjøres og instruksjoner om å installere disse hvis de ikke er installert allerede.

### ➔ Installere og oppgradere DEB-pakker

#### DEB

DEB er Debians pakkesystem (Debian Packaging system). Deb fil-formatet blir brukt av Debian, Ubuntu, Mint og mange andre distroer.

#### APT

APT står for *Advanced Package Tool* og inneholder programmet **apt** (tidligere apt-get), en enkel måte og laste ned og installere pakker fra flere ulike kilder via kommandolinjen. I motsetning til dpkg, forstår ikke apt .deb filer, men installerer pakkene etter navn, og apt kan bare installere .deb-pakker fra kilder spesifisert på forhånd i filen **/etc/apt/sources.list**. apt bruker dpkg direkte etter at .deb-pakkene er lastet ned fra kildene.

Noen vanlige måter å bruke **apt** / **apt-get** på:

- Først lønner det seg å oppdatere pakkelistene - listene over tilgjengelig programvare - slik at systemet ditt vet hvilke nye versjoner som lagt til siden sist. Denne kommandoen gjør dette:

```
$ sudo apt update
```

(Dette bør gjøres før hver gang du oppdaterer)

- For å oppgradere alle installerte programmer på PCen din til siste tilgjengelige versjon, uten å slette noe eller legge til noe nytt kjør denne kommanden:

```
$ sudo apt upgrade
```

- For å oppgradere alle programmene på PCen og, hvis det er nødvendig for oppgraderingen, installere ekstra pakker eller fjerne eksisterende pakker, kjør denne kommandoen:

```
$ sudo apt full-upgrade (eller for eldre versjoner: dist-upgrade)
```

- (Med kommandoen `upgrade` beholdes den eksisterende versjonen av et program hvis oppgradering innebærer at en tilleggs pakke må installeres for å tilfredsstille nye avhengigheter. Med kommandoen `full-upgrade` eller `dist-upgrade` vil pakken bli oppgradert og tilleggs pakke(n)e installert og evt gamle pakker fjernet)
- For å installere programmet *foo* og alle tilleggsprogrammer den er avhengig av for å fungere, kjør denne kommandoen:

```
$ sudo apt install foo
```

- For å avinstallere programmet *foo* og fjerne det fra systemet, men la programmets konfigurasjonsfiler være igjen, kjør denne kommandoen:

```
$ sudo apt remove foo
```

- For å avinstallere programmet *foo* og slette programmets konfigurasjonsfiler, kjør kommandoen:

```
$ sudo apt --purge remove foo
```

merk at du må være innlogget som **root** - evt. tilføy **sudo** før kommandoene for å kunne installere, oppgradere eller avinstallere programpakker.

Apt inkluderer også verktøyet **apt-cache** som du kan bruke til å søke etter programpakker i pakkelistene. Du kan bruke det til å finne programmer som inneholder en viss funksjonalitet gjennom enkle tekstsøk eller mer avanserte søk med regulære uttrykk. I nyere versjoner av Ubuntu (14.04 og senere) kan du også bruke **apt search**.

Her er noen vanlige bruksområder for **apt** / **apt-cache**:

- For å finne pakker som inneholder ordet *word*:

```
$ sudo apt-cache search word
```

- For å vise detaljert informasjon om en pakke:

```
$ sudo apt-cache show package
```

- For å vise hvilke andre pakker en pakke avhenger av:

```
$ sudo apt-cache depends package
```

- For å vise detaljert informasjon om hvilke versjoner av en pakke som er tilgjengelig og informasjon om pakker som er avhengige av denne pakken:

```
$ sudo apt-cache showpkg package
```

For mer informasjon, installer apt og les `apt-get(8)`, `sources.list(5)`, og installer pakken `apt-doc` og les `/usr/share/doc/apt-doc/guide.html/index.html`.

## dpkg

---

Dette er den opprinnelige pakkehåndtereren for debian-pakker. `dpkg` kan kjøres med mange ulike opsjoner. Noen vanlige valg er:

- Finn ut hvilke mulige opsjoner programmet har:  
**dpkg --help.**
- Vis informasjonsfilen (og annen info) for en pakke :  
**dpkg --info foo\_VVV-RRR.deb**
- Installer en pakke (inkludert å pakke opp og konfigurere) på hardiskens filsystem:  
**dpkg --install foo\_VVV-RRR.deb.**
- Pakk opp (men ikke konfigurer) en Debian pakke til harddiskens filsystem:  
**dpkg --unpack foo\_VVV-RRR.deb.**  
Merk at dette ofte ikke er nok til å kunne kjøre programmet. Denne kommandoen fjerner tidligere installerte versjoner av programmet og kjører programmets pre-installasjons-skript.
- Konfigurer en pakke som allerede er pakket ut:  
**dpkg --configure foo.**  
Denne kommandoen kjører postinstallasjons-skriptet til pakken, og den oppdaterer også pakkens



fillister. Legg merke til at 'configure'-kommandoen etterfølges av et pakkenavn, (f.eks., foo), *ikke* navnet til Debian arkivfilen (f.eks., foo\_VVV-RRR.deb).

- Trekke ut en enkelt fil kalt "blurf" (eller en gruppe filer kalt "blurf\*") fra et Debian arkiv:  
**`dpkg --fsys-tarfile foo_VVV-RRR.deb | tar -xf - blurf*`**
- Fjerne/avinstallere en pakke (men ikke pakkens konfigurasjonsfiler):  
**`dpkg --remove foo.`**
- Fjerne/avinstallere en pakke (inkludert pakkens konfigurasjonsfiler):  
**`dpkg --purge foo.`**
- Liste opp installasjons-statusen til pakker som inneholder strengen (eller regulære uttrykket) "foo\*":  
**`dpkg --list 'foo*'`.**

## ➔ Installere og oppgradere RPM-pakker

Ulike Linux distroer bruker ulike applikasjonspakker (installerbare programmer). En *pakke* i dette tilfelle er en måte å håndtere hvordan applikasjoner innstalleres i et system, hvordan håndtere dets avhengigheter av andre pakker osv. Pakken inneholder med andre ord programmet som skal installeres samt informasjon om hvilke andre programmer som må være installert for at programmet skal kunne kjøres og instruksjoner om å installere disse hvis de ikke er installert allerede.

## ➔ RPM - Pakkehåndtering med Red Hat Package Manager

### RPM

---

RPM er RedHats pakkesystem (Redhat Package Manager). Fil-formatet **rpm** blir brukt av RHEL, Centos, Fedora, Suse og flere andre distroer.

### YUM / DNF

---

YUM står for *Yellowdog Updater, Modified* og inneholder programmet **yum**, en enkel måte og laste ned og installere pakker fra flere ulike kilder via kommandolinjen.

DNF står for "Dandified Yum", og ble introdusert i Fedora i 2013, som en arvtager etter yum. Fra og med RHEL/Centos 8 er **dnf** default pakkehåndterer for RedHat distroer.

I motsetning til rpm, forstår ikke yum eller dnf .rpm-filer, men installerer pakkene etter navn, og kan bare installere .rpm-pakker fra kilder spesifisert på forhånd i mappen **/etc/yum.repos.d** Yum og dnf bruker rpm direkte etter at .rpm-pakkene er lastet ned fra kildene.

Noen vanlige måter å bruke **yum** / **dnf** på:

- For å oppgradere alle installerte programmer på PCen din til siste tilgjengelige versjon, uten å slette noe eller legge til noe nytt kjør denne kommanden:

```
$ sudo yum/dnf upgrade
```

- For å installere programmet *foo* og alle tilleggsprogrammer den er avhengig av for å fungere, kjør denne kommandoen:

```
$ sudo yum/dnf install foo
```

- For å avinstallere programmet *foo* og fjerne det fra systemet, kjør denne kommandoen:

```
$ sudo yum/dnf remove foo
```

merk at du må være innlogget som **root** - evt. tilføy **sudo** før kommandoene for å kunne installere, oppgradere eller avinstallere programpakker.

- For å søke etter pakker som inneholder ordet *word*:

```
$ sudo yum/dnf search word
```

- For å liste opp alle pakke-brønner som er installert:

```
$ sudo yum/dnf repolist
```

**Tilgjengelige kommandoer for dnf:**

- alias
- autoremove
- check
- check-update
- clean
- deplist
- distro-sync
- downgrade
- group
- help
- history

- info
- install
- list
- makecache
- mark
- module
- provides
- reinstall
- remove
- repoinfo
- repolist
- repoquery
- repository-packages
- search
- shell
- swap
- updateinfo
- upgrade
- upgrade-minimal
- upgrade-to

## rpm

---

Dette er den opprinnelige pakkehåndtereren for rpm-pakker. programmet **rpm** kan kjøres med mange ulike parametere. Noen vanlige valg er:

- Finn ut hvilke mulige valg programmet har:  
**rpm --help.**

Her er et lite utdrag fra manualen til rpm som viser de vanligste kommandoene og parameterene:

### QUERYING AND VERIFYING PACKAGES:

```
rpm {-q|--query} [select-options] [query-options]
rpm --querytags
rpm {-V|--verify} [select-options] [verify-options]
```

### INSTALLING, UPGRADING, AND REMOVING PACKAGES:

```
rpm {-i|--install} [install-options] PACKAGE_FILE ...
rpm {-U|--upgrade} [install-options] PACKAGE_FILE ...
rpm {-F|--freshen} [install-options] PACKAGE_FILE ...
rpm [--reinstall] [install-options] PACKAGE_FILE ...
rpm {-e|--erase} [--allmatches] [--justdb] [--nodeps] [--noscripts]
  [--notriggers] [--test] PACKAGE_NAME ...
```

## ➔ Brukerhåndtering fra kommandolinjen

Det finnes gode grafiske verktøy for brukerbehandling, men det er ikke alltid man har tilgang til dem, f.eks. hvis man skal jobbe på en server med kun ssh-tilgang (ssh = secure shell). Heldigvis er det enkelt å administrere brukere, brukergrupper og tillatelser via kommandolinjen, som er det vi skal se på i denne teksten.

**Merk:** Du må være rot-bruker eller bruke sudo for å håndtere brukere og brukergrupper.

### Informasjon om en bruker

---

Du kan få grunnleggende informasjon om en bruker på flere måter. her er noen av dem:

Før du endrer gruppetilhørigheter o.l. kan du se hvilken id en bruker har og hvilke grupper en bruker er medlem av gjennom kommandoen **id**, slik:

```
$ id <username>
```

For eksempel:

```
$ id terje
uid=1000(terje) gid=1000(terje) groups=1000(terje),10(wheel),54335(felles)
```

Hvis du bare vil se gruppene en bruker er medlem av, kan du også bruke kommandoen groups, slik:

```
$ groups terje
terje : terje wheel felles
```

### Legge til en ny bruker

---

For å legge til en ny bruker fra kommandolinjen, kan man bruke verktøyet **adduser** slik:

```
$ sudo adduser petter
Oppretter bruker «petter» ...
Oppretter ny gruppe «petter» (1002) ...
Oppretter ny bruker «petter» (1002) med gruppe «petter» ...
Oppretter hjemmemappe «/home/petter» ...
Kopierer filer fra «/etc/skel» ...
Angi nytt UNIX-passord:
Bekreft nytt UNIX-passord:
passwd: passordet ble oppdatert
```

```
Changing the user information for petter
Enter the new value, or press ENTER for the default
Full Name []: Petter Testbruker
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
#
```

Som det fremgår av tilbakemeldingene fra adduser-programmet ovenfor, opprettes en hjemmemappe med brukerens navn i mappen «/home». Hit kopieres et sett med standardfiler fra mappen «/etc/skel» (skel står for "skeleton", og alle filer vi legger i denne mappen blir kopiert til hver ny bruker).

## Endre en eksisterende bruker

---

Endre en eksisterende bruker kan gjøres via kommandoen **usermod**:

### Her er parametrene for å endre en bruker:

- c, --comment NEW\_NAME setter ny verdi for brukerens fulle navn
- d, --home HOME\_DIR setter ny hjemmemappe for brukeren
- e, --expiredate EXPIRE\_DATE setter kontoens utløpsdato til EXPIRE\_DATE
- f, --inactive INACTIVE setter passordet etter kontoens utløp til INACTIVE
- g, --gid GROUP setter GROUP som ny primærgruppe
- G, --groups GROUPS setter ny liste av tilleggsgrupper brukeren er med i.
- a, --append legger brukeren til tilleggsgruppene GROUPS, spesifisert ved -G i tillegg til eksisterende gruppedlemskap
- h, --help Viser hjelpeteksten
- l, --login NEW\_LOGIN setter nytt login navn
- L, --lock låser brukerkontoen
- m, --move-home flytter hjemmemappen til ny mappe, brukes bare sammen med -d
- p, --password PASSWORD setter nytt passord til en kryptert versjon av PASSWORD
- s, --shell SHELL setter nytt login shell for brukeren
- u, --uid UID setter ny bruker-ID for brukeren
- U, --unlock låser opp brukerkontoen

### Eksempler på bruk av usermod:

```
$ sudo usermod -c "Nytt fullt navn" <username>
$ sudo usermod -l "Nytt brukernavn" <username>
```

**Merk:** Har du tilgang til et grafisk brukergrensesnitt, kan du også bruke det grafiske programmet **user-admin** til å endre bruker-data. Du kan starte det fra applikasjonsmenyen eller fra terminalvinduet ved å kjøre kommandoen:

```
$ user-admin
```

## Slette en bruker fra systemet

---

En bruker kan slettes fra systemet via kommandoen **userdel**, slik:

```
$ sudo userdel <username>
```

**Merk:** Dette sletter ikke brukerens hjemmemappe

For å slett brukerens hjemmemappe og lokal epost, bruk denne kommandoen:

```
$ sudo userdel -r <username>
```

## Grupper

---

En gruppe er en samling brukerkontoer som opptrer som en enkelt enhet. Hvis en gruppe får tilgang til å utføre en handling, har alle gruppens medlemmer samme tilgang.

Her er noen nyttige kommandoer for å jobbe med Linuxgrupper:

- **groups** (lister opp hvilke grupper en bruker er medlem av)
- **groupadd** (opprettet en ny gruppe)
- **groupdel** (sletter en gruppe)
- **groupmod** (endrer en gruppe)
- **gpasswd -a <bruker> <gruppe>** (legg en bruker til en gruppe)
- **members <gruppenavn>** (list medlemmer i en gruppe - debian/ubuntu)
- **getent group <gruppenavn>** (list medlemmer i en gruppe - alle distroer)

**Slik kan de brukes:**

**\$ whoami** (vis brukernavnet til den som skriver kommandoen)  
petter (viser at brukernavnet er *petter*)

**\$ groups** (vis hvilke grupper petter er medlem av)

petter users (viser at petter med i gruppene *petter* og *users*)

**\$ groups per petter root** (vis hvilke grupper *per*, *petter* og *root* er medlem av)

per: per users (viser gruppene *per* er medlem av)

petter: petter users (viser gruppene *petter* er medlem av)

root: root bin daemon sys adm disk wheel src (viser gruppene *root* er medlem av)

**\$ sudo groupadd felles** Oppretter gruppen "felles"

**\$ sudo gpasswd -a petter felles**

Legger brukeren petter til gruppen felles

**\$ members felles**

petter

**\$ getent group felles**

felles:x:1034:petter

## /etc/passwd, /etc/shadow og /etc/group

**/etc/passwd** og **/etc/shadow** er to filer som inneholder informasjon om alle brukerne på en Linux-maskin. **/etc/shadow** krever rot-tilgang siden den inneholder brukernes krypterte passord.

**/etc/group** er en fil som inneholder informasjon om maskinens definerte grupper, inkludert hvilke brukere som er medlemmer i dem.

### Eksempler på format:

#### 1) **/etc/passwd**

**# cat /etc/passwd**

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

mssql:x:992:990::/var/opt/mssql:/bin/bash

terje:x:1000:1000::/home/terje:/bin/bash

backup:x:1001:1001::/home/backup:/bin/bash

postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash

mysql:x:991:989:MySQL server:/var/lib/mysql:/sbin/nologin

itfakultetet:x:1006:1006::/home/itfakultetet:/bin/bash

```

apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:990:988:Nginx web server:/var/lib/nginx:/sbin/nologin
mongodb:x:1010:1010::/home/mongodb:/bin/bash
jenkins:x:989:987:Jenkins Automation Server:/var/lib/jenkins:/bin/false
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin

```

## 2) /etc/shadow

\$ cat /etc/shadow

```

sshd:!!:18191::::
chrony:!!:18191::::
rngd:!!:18443:~:
saslauth:!!:18535:~:
mssql:!!:18535:~:
terje:$6$7hNOgw1zdWfDMsLJ$iz5.illxtzSsJdKJQuPoh1c2Joj6Q7DN.Z71MRZR6S5XQtJ/
cbc6fsc6rMzPAiHlwzQD2qnbaCkZuB8Z9Nj1j0:18535:0:99999:7:::
backup:$6$g0hhw1X/tL0oeHu9$cdGt9Zg5V1gZjVZO/.SnsPWL.vim2eSWPhgFjcKtQhtUksSJXC8xQ7o
vrrvWCSKyhEXnlHOr94HixBmEaKqxr0:18535:0:99999:7:::

```

Strukturen til /etc/shadow består av disse feltene, med kolon som skille tegn:

```

root:$6$.n:12236:0:66669:7:::
[--] [----] [--] - [---] ----
|      |      |      |      |      |||+-----> 9. Unused
|      |      |      |      |      ||+-----> 8. Expiration date
|      |      |      |      |      |+-----> 7. Inactivity period
|      |      |      |      |      +-----> 6. Warning period
|      |      |      |      +-----> 5. Maximum password age
|      |      |      +-----> 4. Minimum password age
|      |      +-----> 3. Last password change
|      +-----> 2. Encrypted Password
+-----> 1. Username

```

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to \$id\$salt\$hashed, The \$id is the algorithm used On GNU/Linux as follows:
  1. **\$1\$** is MD5
  2. **\$2a\$** is Blowfish
  3. **\$2y\$** is Blowfish
  4. **\$5\$** is SHA-256



5. **\$6\$** is SHA-512

3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute [date](#) specifying when the login may no longer be used.

3) **/etc/group**

mongod:x:981:

kurs1:x:54325:

kurs2:x:54326:

kurs3:x:54327:

kurs4:x:54328:

kurs5:x:54329:

kurs6:x:54330:

kurs7:x:54331:

kurs8:x:54332:

kurs9:x:54333:

kurs10:x:54334:

felles:x:54335:terje,kurs,kurs1,kurs2,kurs3,kurs4,kurs5,kurs6,kurs7,kurs8,kurs9,kurs10

# Kapittel 4

## 4: SSH / SCP / SFTP

### ➔ Installasjon og konfigurering av OpenSSH - secure shell server

Det viktigste administrasjonsgrensesnittet vårt mot serveren er gjennom SSH - Secure SHell. Så lenge vi kan logge oss inn på en SSH-konto med rot-tilgang til serveren har vi full kontroll over den. Noe av det første vi gjør er derfor å sørge for at denne tilgangen er tilstede, satt opp riktig og at den ikke kommer i hendene på uønskede inntrengere.

#### Installasjon

Dersom **Open SSH server** ikke ble valgt ved installasjon av Ubuntu-serveren, kan du installere OpenSSH - klient og server med følgende kommando:

```
$ sudo apt-get install openssh-client openssh-server
```

#### Konfigurering

SSH-serveren kan konfigureres ved å endre parametrene i konfigurasjonsfilen:

**/etc/ssh/sshd\_config**

Sjekk gjerne manualen for konfigurering gjennom kommandoen:

```
$ man sshd_config
```

**Merk:** Lag en kopi av den originale konfig-filen før du endrer noe. Dersom du gjør en feil som hindrer SSH-serveren fra å fungere, kan det bli vanskelig å nå serveren fra nettverket.

### Her er noen nyttige endringer du kan gjøre i konfig-filen:

- Endre portnummeret SSH-serveren lytter på. Dette er en effektiv måte å hindre "script kiddies" i å forsøke å hacke seg inn på serveren via SSH.  
port 22 er standard port for SSH, så du kan endre til noe over 1024, f.eks. slik:

port 2222

- For å tillate innlogging med offentlig nøkkel:

PubkeyAuthentication yes

- For å kunne kjøre programmer på serveren med grafisk brukergrensesnitt (GUI) fra en klient, kan du sette:

X11Forwarding yes

Dette fungerer dersom grafisk grensesnitt (X-server) er installert på serveren. Klienten logger seg på med flagget -X eller -Y og kan starte GUI-programmer som vises på klientens PC som om man satt ved serveren.

**Merk:** Hvis du endrer portnummeret til noe annet enn 22 må klienten logge seg inn med flagget -p etterfulgt av det oppsatte portnummeret. F.eks. slik:

**\$ ssh -p 2222 bruker@server.com**

eller

**\$ ssh -p -X 2222 bruker@server.com**

hvis man ønsker å kjøre GUI-baserte programmer fra serveren

## Bruk av aliaser via SSHs konfigurasjonsfil

Først rediger eller lag en fil som heter **config** i din egen **.ssh**-mappe, f.eks slik:

**\$ vim ~/.ssh/config** (eller bruk din favoritt-editor)

Filten skal inneholde dette oppsettet for hver alias du lager til en ssh-konto:

host aliasnavn

HostName server.domain.com

Port 5555

User username

F.eks. slik:

host hjemme

HostName server1.hjemme.no

Port 2222

User Petter

Når dette er lagret, kan du skrive:

```
$ ssh hjemme
```

istedenfor:

```
$ ssh -p 2222 petter@server1.hjemme.no
```

## ➔ Passordløs innlogging

### Innlogging med nøkler, uten passord

Først lager vi nøkler som vi kan bruke til innloggingen, slik:

```
$ ssh-keygen
```

La passordet stå blankt, slik at nøkkelen lages uten passord.

Så kopierer du den offentlige nøkkelen over til serveren, slik:

```
$ ssh-copy-id -p <port> bruker@server.com
```

eller slik (old school):

```
$ cat .ssh/id_rsa.pub | ssh bruker@server.com 'cat >>
.ssh/authorized_keys'
```

Dette kopierer nøkkelen fra id\_rsa.pub og legger den til filen **authorized\_keys** på serveren (bytt ut med ditt brukernavn og servernavn)

Og det er alt som trengs for en passordløs ssh-bruk. Og dette gjelder også for scp og sftp.

**Merk:** Det er nå viktig å ha et godt passord for innlogging på din egen pc, slik at du ikke åpner et sikkerhetshull av dimensjoner her.

## ➔ Sikker kopiering av filer og mapper med scp

Kommandoen **scp** er en del av SSH-serveren og brukes til kryptert kopiering til og fra servere.

### Eksempler:

```
$ scp filnavn.txt brukernavn@server.com:/mappe
```

- Kopierer *filnavn.txt* til mappen *mappe* på serveren *server.com* innlogget som *brukernavn*

```
$ scp -P 20300 filnavn.txt brukernavn@server.com:/mappe
```

- Samme som ovenfor, men bruker port 20300 istedenfor port 22 (default).

```
$ scp brukernavn@server.com:/mappe/filnavn.txt .
```

- Kopierer *filnavn.txt* fra mappen *mappe* på serveren *server.com* innlogget som *brukernavn*, til den mappen du er i lokal - angitt ved "."

```
$ scp -P 20300 -r mappe1 brukernavn@server.com:mappe1
```

- Samme som ovenfor, men kopierer rekursivt mappen *mappe1* til mappen *mappe1* i brukerens hjemmemappe på serveren

## ➔ SFTP - Sikker FTP

SFTP er en del av OpenSSH, og fungerer som en vanlig ftp-server eller klient med fordelen at all trafikk er kryptert.

**Her er noen enkle eksempler på bruk av SFTP**

```
$ sftp -P 2022 brukernavn@servernavn.com:/home/bruker/www/
```

- logger deg på *servernavn.com* som bruker *brukernavn* via port 2022, og går til mappen */home/bruker/www*

**Merk:** Dersom ssh-serveren kjøres på default-porten (port 22) trenger du ikke ha med port-parametret

```
$ pwd
```

- viser hvilken mappe du er i

```
$ lpwd
```

- viser hvilke mappe du er i lokalt (på din egen pc)

```
$ cd dokumenter
```

- går til mappen *dokumenter* på serveren

```
$ lcd dokumenter
```

- går til mappen *dokumenter* lokalt

```
$ put *.php
```

- laster opp alle php-filer fra den mappen du er i lokalt til den mappen du er i på serveren

```
$ get filnavn1 filnavn2
```

- laster ned dokumentene *filnavn1* og *filnavn2* fra serveren til mappen du er i lokalt

**Merk:** De fleste kommandoer du kan kjøre på serveren har en tilsvarende kommando for å kjøres lokalt - ved rett og slett å skrive "l" foran kommandoen, som i eksemplene ovenfor.

## ➔ SSH - tunneler

Et vanlig bruksområde for SSH er å lage såkalte tunneler fra en port på en maskin til en port på en annen. Slik kan man f.eks. kryptere trafikk som ellers ville gått i klartekst.

### Eksempel 1:

---

Du er på en server uten internet-tilgang (server1), men som er koblet i et lokalt nettverk til en annen maskin med internettilgang (server2). Serveren har problemer, og du trenger å Google frem en løsning. Slik gjør du:

```
$ ssh -L 12345:google.com:80 bruker@server2
```

Nå kan du åpne en forbindelse til port 12345 på server1 og få tilgang til Google fra server2 - f.eks. ved å peke Firefox til `http://localhost:12345`

For å unngå å utføre kommandoer på server2, er det vanlig å ta med paramteret `-N` (no command) slik:

```
$ ssh -L 12345:google.com:80 -N bruker@server2
```

Kjører server2 ssh-serveren på en annen port en port 22, må du også ta med portnummeret, f.eks slik (hvis den kjører på port 2222):

```
$ ssh -p 2222 -L 12345:google.com:80 bruker@server2
```

### Eksempel 2:

---

serverA er en server som kjører CUPS printerserver på standardport (631), men webgrensenettet til CUPS er bare tilgjengelig lokalt. Slik kan du få tilgang til det fra en annen maskin gjennom en ssh-tunnel:

```
$ ssh -L 12345:localhost:631 -N bruker@serverA
```

Port 12345 vil nå peke til port 631 på serverA, og CUPS er tilgjengelig fra:

`http://localhost:12345`

### Eksempel 3:

---

SSH kan gi deg full tilgang til internett fra en annen maskin gjennom den innebygde støtten for SOCKS 5. F.eks. slik:

```
$ ssh -D 1234 bruker@serverA
```

Når dette er gjort kan du sette opp f.eks. Firefox til å bruke localhost og port 1234 som Socks 5 Proxy, og så har du full tilgang til internett.



# Kapittel 5

## Data Wrangling

### ➔ cat - skjøt sammen filer og mye mer

**cat** har navnet sitt fra det engelske ordet *concatenate* som betyr å skjøte noe sammen, og det er ett av bruksområdene for **cat**.

**cat** tar disse parameterene:

- A, --show-all  
equivalent to -vET
- b, --number-nonblank  
number nonempty output lines, overrides -n
- e equivalent to -vE
- E, --show-ends  
display \$ at end of each line
- n, --number  
number all output lines
- s, --squeeze-blank  
suppress repeated empty output lines
- t equivalent to -vT
- T, --show-tabs  
display TAB characters as ^I
- u (ignored)
- v, --show-nonprinting  
use ^ and M- notation, except for LFD and TAB
- help display this help and exit
- version  
output version information and exit

**Eksempler:**

```
$ cat navn1
Ole Moen
Petter Jensen
$ cat navn2
Kari Diesen
Rolf Juster
$ cat navn1 navn2
Ole Moen
Petter Jensen
Kari Diesen
Rolf Juster
$ cat -n navn1 navn2
 1 Ole Moen
 2 Petter Jensen
 3 Kari Diesen
 4 Rolf Juster
```

**Skriv til fil fra tastaturet:**

```
$ cat frukt
eple
appelsin
$ cat >>frukt
papaya
ananas
$ cat frukt
eple
appelsin
papaya
ananas
```

**Skriv til en fil på en server:**

```
$ cat ~/.ssh/id_rsa.pub | ssh server4 'cat >> .ssh/authorized_keys'
```

Kommandoen over kopierer brukerens offentlige nøkkel over til server4 og legger den til i server-brukerens authorized\_keys

## ➔ head og tail

### head

**head** er et program som viser de første linjene i en tekstfil eller en tekststrøm. Default er 10 linjer, men du kan spesifisere antallet med en bindestrek etterfulgt av et tall, slik:

```
$ head -20 tekstfil.txt    (viser de 20 første linjene i tekstfil.txt)
$ history | head -5        (viser de 5 første linjene i kommando-historikken)
$ head -n -5000 enhetsregisteret (viser alle bortsett fra de siste 5000 linjene i filen enhetsregisteret)
```

### tail

**tail** viser de siste linjene i en tekstfil eller tekststrøm. Hvor mange kan du spesifisere med en bindestrek etterfulgt av et tall, slik:

```
$ tail -20 tekstfil.txt    (viser de 20 siste linjene i tekstfil.txt)
```

### tail -f

**tail** tar et parameter **-f** (follow) som lar deg se i sanntid hvordan en fil endres, dvs. hva som legges til (eller slettes) fra slutten av filen. **tail -f** brukes ofte til å følge med på loggfiler og andre filer som endres ofte. Eksempel:

```
# tail -f /var/log/maillog
```

Avslutt **tail -f** med **<ctrl>+c**

## ➔ more og less

Et potensielt problem med **cat** er at begynnelsen av teksten forsvinner hvis teksten rommer mer enn ett skjermbilde. **more** ble laget for å bøte på dette. Ved å bruke **more** istedenfor **cat** vil skjermen fylles av den første delen av teksten, og ved å taste mellomrom-tasten kommer vises neste skjermbilde, helt til hele teksten er vist. Du kan når som helst avslutte visningen ved å taste bokstaven "q" (for quit). Hvis teksten ikke fyller mer enn ett skjermbilde, fungerer **more** akkurat som **cat**.

**more** har en åpenbar begrensning i at man ikke kan bla seg bakover til forrige skjermbilde. Det ga inspirasjon til utviklingen av **less**, som fikk navnet sitt ut fra idéen om at **more is less**. Med **less** kan du "scrolle" frem og tilbake i teksten med piltastene, og avslutte med å taste bokstaven "q".

Moderne terminal-emulatorer, som **gnome terminal** eller kde sin **konsole** har innebygde scrollbars, som gjør more og less mer eller mindre overflødige, men de blir viktige når man er logget direkte inn på en server uten grafisk brukergrensesnitt, og det ikke er mulighet til scrolling.

**MERK:** Hvis vi sender resultatet av more eller less videre med en |, vil de fungere på samme måte som cat:

```
$ more war-and-peace.txt | wc
63846  562489 3266164
$ less war-and-peace.txt | wc
63846  562489 3266164
```

Kommandoer for å bevege seg rundt i tekst med **less**;

Key	Description
Arrow	Move by one line
Space	Move down one page
b	Move up one page
g	Go to the first line
G	Go to the last line
100g	Go to the 100th line
/string	Search for the string from current position
n/N	Go to the next or previous search match
q	Exit less

## ➔ date

**date** er en kommando som uten parametere gir oss dagens dato.

**Her er noen eksempler:**

```
$ date
ti. 08. des. 20:58:01 +0100 2020
$ date -I          (ISO-format)
2020-12-08
$ date --date='+2 weeks'
ti. 22. des. 20:59:53 +0100 2020
$ echo "filnavn_`date -I`.txt"
filnavn_2020-12-08.txt
$ echo "filnavn_`date --date='3 days ago' -I`.txt"
filnavn_2020-12-05.txt
```

## ➔ grep - fgrep - egrep - søk i tekstfiler

**grep** er et kraftig søkeverktøy for søk i tekstfiler. **grep** kan brukes direkte mot filer, eller på input fra en strøm, f.eks. via en | fra et annet program. **grep** kan søke etter fast tekst, men også etter regulære uttrykk (regex), men bare **basic** og ikke **extended** regex. ([forskjellen mellom basic og extended](#)).

**grep** har parameteret **-E** som lar deg bruke extended regex, og parameteret **-F** som lar deg søke i fast tekst uten regulære uttrykk (som er noe raskere).

**egrep** - er grep som også kan søke i **extended regex**. (**e** står for extended)

**fgrep** - er grep som ikke bruker regulære uttrykk i det hele tatt, og er demed litt raskere enn grep og egrep. (**f** står for fixed, som i "fixed string")

**MERK:** både fgrep og egrep er **deprecated**, som betyr at de vil bli fjernet på et senere tidspunkt - og det anbefales å erstatte dem med **grep -E** eller **grep -F**

### Eksempler:

#### 1) Tell hvor mange linjer som starter med ordet Prince i Tolstoys Krig og Fred:

```
$ grep -c '^Prince ' war-and-peace.txt
274
```

**MERK:** Tegnet ^ er en del av basic regex, og angir at det som følger må stå begynnelsen av teksten, som her blir i begynnelsen av en linje. Flagget **-c** ber grep om å telle antall forekomster.

#### 2) List alle linjer i /var/log/secure som inneholder ordene failed og mysql

```
$ sudo grep -i failed /var/log/secure | grep -i mysql
Aug  1 19:05:07 wp520 useradd[4429]: failed adding user 'mysql', exit
code: 9
Aug 19 15:41:13 wp520 useradd[5263]: failed adding user 'mysql', exit
code: 9
Nov  2 21:43:55 wp520 useradd[22115]: failed adding user 'mysql', exit
code: 9
Nov 11 01:55:40 wp520 useradd[44976]: failed adding user 'mysql', exit
code: 9
Dec 10 14:52:55 wp520 useradd[4596]: failed adding user 'mysql', exit
code: 9
Jan 19 15:04:17 wp520 useradd[14589]: failed adding user 'mysql', exit
code: 9
```

#### 3) Tell alle feilede loginforsøk på mailserveren

```
$ sudo grep -ic 'authentication failed' /var/log/maillog
74374
```

#### 4) søk etter navn som slutter på sen eller son

```
$ cat navn
Ole Olsen
Jan Janson
Per Petterson
Kari Svendsen
Olga Konkova
$ grep 'sen' navn
Ole Olsen
Kari Svendsen
$ grep 'son' navn
Jan Janson
Per Petterson
$ grep 's(o|e)n' navn
Ole Olsen
Jan Janson
Per Petterson
Kari Svendse
$ grep -E 's(o|e)n' navn
Ole Olsen
Jan Janson
Per Petterson
Kari Svendsen
```

## ➔ sort - sorter tekstfiler

**sort** er en nyttig kommando som sorterer linjer i en tekstfil eller i en strøm av tekst i en kommandokjede.

**sort** har disse parameterene;

- b, --ignore-leading-blanks  
ignore leading blanks
- d, --dictionary-order  
consider only blanks and alphanumeric characters
- f, --ignore-case  
fold lower case to upper case characters
- g, --general-numeric-sort  
compare according to general numerical value

- i, --ignore-nonprinting  
consider only printable characters
- M, --month-sort  
compare (unknown) < 'JAN' < ... < 'DEC'
- h, --human-numeric-sort  
compare human readable numbers (e.g., 2K 1G)
- n, --numeric-sort  
compare according to string numerical value
- R, --random-sort  
shuffle, but group identical keys. See shuf(1)
- random-source=FILE  
get random bytes from FILE
- r, --reverse  
reverse the result of comparisons
- sort=WORD  
sort according to WORD: general-numeric -g, human-numeric -h, month -M, numeric -n,  
random -R, version -V
- V, --version-sort  
natural sort of (version) numbers within text

### Eksempler:

```
$ cat >>tall
34
12
67
123
7
56
^C
$ sort tall
12
123
34
56
67
7
$ sort -nr tall
123
67
56
34
12
```

```

7
$ curl -s https://web.itfakultetet.no/navn
Ola
Petter
Kari
Anders
$ curl -s https://web.itfakultetet.no/navn | sort
Anders
Kari
Ola
Petter

```

## ➔ uniq - Fjern duplikater

Kommandoen **uniq** lar oss luke bort duplikate linjer i en tekstfil eller -strøm.

**MERK:** **uniq** sjekker en linje i forhold til foregående linje, så vi må sortere filen eller strømmen for å luke bort alle duplikater.

**uniq** tar disse parameterene:

- c, --count  
prefix lines by the number of occurrences
- d, --repeated  
only print duplicate lines, one for each group
- D print all duplicate lines
- all-repeated[=METHOD]  
like -D, but allow separating groups with an empty line;  
METHOD={none(default),prepend,separate}
- f, --skip-fields=N  
avoid comparing the first N fields
- group[=METHOD]  
show all items, separating groups with an empty line;  
METHOD={separate(default),prepend,append,both}
- i, --ignore-case  
ignore differences in case when comparing
- s, --skip-chars=N  
avoid comparing the first N characters
- u, --unique  
only print unique lines
- z, --zero-terminated  
line delimiter is NUL, not newline



- w, --check-chars=N  
compare no more than N characters in lines
- help display this help and exit
- version  
output version information and exit

### Eksempler:

```
$ cat frukt
eple
appelsin
eple
appelsin
eple
pære
pære
mango
$ uniq frukt
eple
appelsin
eple
appelsin
eple
pære
mango
$ sort frukt | uniq
appelsin
eple
mango
pære
$ sort frukt | uniq -c
  2 appelsin
  3 eple
  1 mango
  2 pære
```

### ➔ tr (translate) - endre tegn i en tekst

**tr** er en effektiv kommando for å endre (oversette) ett eller flere tegn i en tekst. **tr** kan brukes med eller uten regulære uttrykk.

### Eksempler på bruk:

```
$ cat navn
```

```
Ole Olson  
Jan Janson  
Per Petterson  
Kari Svendson
```

```
$ cat navn | tr '[:lower:]' '[:upper:]'
```

```
OLE OLSON  
JAN JANSON  
PER PETERSON  
KARI SVENDSON
```

```
$ cat navn | tr 'OJP' 'ojp'
```

```
ole olson  
jan janson  
per petterson  
kari svendson
```

```
$cat domener.txt
```

```
www. tecmint. com  
www. fossmint. com  
www. linuxsay. com
```

```
$ cat domener.txt | tr -d ' '
```

```
www.tecmint.com  
www.fossmint.com  
www.linuxsay.com
```

```
$ tr -d ' ' < domener.txt > domener_fixed.txt
```

```
$ cat domener_fixed.txt
```

```
www.tecmint.com  
www.fossmint.com  
www.linuxsay.com
```

## ➔ sed - søk og erstatt tekst

### sed

---

**sed (stream editor)** er en videreutvikling av den opprinnelige editoren **ed**, og brukes til å modifisere strømmer av tekst fra pipes eller filer.

**sed** kan ikke brukes interaktivt, i stedet spesifiserer man instruksjoner som **sed** utfører på devn valgte teksten. `mmand-line shells`.

Dette kan **sed** brukes til:

- Søke i tekst
- Erstatte tekst
- Legge linjer til tekst
- Slette linjer fra tekst
- Endre (eller bevare) en original fil

sed kan brukes med **regulære uttrykk**, som gjør det effektivt og fleksibelt å søke opp tekst.

### Eksempler

#### 1) Erstatte tekst fra en pipe

```
$ echo "Dette er en tekst som er uendret" | sed s/" er "/" var "/g
```

Dette var en tekst som var uendret

#### 2) Erstatte tekst fra en fil, uten å endre filen

```
$ cat navn
Ole Olsen
Jan Jansen
Per Pettersen
Kari Svendsen
$ sed 's/sen/son/g' navn
Ole Olson
Jan Janson
Per Petterson
Kari Svendson
```

Resultatet skrives til skjerm, men filen endres ikke

#### 3) Erstatte tekst i en fil, slik at filen endres, med flagget -i

```
$ sed -i 's/sen/son/g' navn
$ cat navn
Ole Olson
Jan Janson
Per Petterson
Kari Svendson
```

**MERK:** g står for "globally", dvs alle forekomster.

#### 4) Velg linjer fra en tekst

```
$ sed -n '3,4p' navn
Per Petterson
Kari Svendson
```

Velger linje 3 til og med linje 4. p står for print og n angir at resten av filen ikke skal printes samtidig.

#### 5) Erstatt mellomrum med linjeskift, slik at hvert ord kommer på en egen linje

```
$ sed 's/\s/\n/g' navn
Ole
Olson
Jan
Janson
Per
Petterson
Kari
Svendson
```

**MERK:** \s står for "space" og \n står for "new line".

## ➡ awk - et programmeringsspråk for behandling av tekst

**awk** er et eget programmeringsspråk utviklet ved AT&T Bell i 1977 og har navnet sitt fra utviklerne: Aho, Weinberger og Kernighan.

**awk** har brukerdefinerte funksjoner, kan håndtere multiple input-strømmer, TCP/IP networking og et rikt sett med regulære uttrykk. Det brukes ofte til å prosessere rene tekstfiler, hvor awk kan tolke data som rader og felt som brukeren kan behandle.

**awk** søker i filer etter tekst-enheter (som regel linjer avsluttet med en *end-of-line character*) som inneholder bruker-definerte mønstre.

### Eksempler:

**\$ awk '/foo/ { print toupper(\$0); }'**

Dette er en tekst

Dette er en tekst som inneholder ordet foo

DETTE ER EN TEKST SOM INNEHOLDER ORDET FOO

**\$ cat navn**

Ole Olsen

Jan Janson

Per Pettersen

Kari Svendsen

Olga Konkova

**\$ awk '/Kari/ { print \$2 }' navn**

Svendsen

**GNU-versjonen av awk kalles gawk, men programmet er linket til awk, og kan startes med kommandoen: awk.**

**gawks online manual:**

<https://www.gnu.org/software/gawk/manual/>

## ➔ cut

**cut** lar deg klippe ut kolonner fra en kolonne-inndelt tekst og enten lagre dem til en ny fil eller sende dem videre med en | til en ny kommando.

**cut** tar disse parametrene:

```
-b, --bytes=LIST
    select only these bytes
-c, --characters=LIST
    select only these characters
-d, --delimiter=DELIM
    use DELIM instead of TAB for field delimiter
-f, --fields=LIST
    select only these fields; also print any line that contains
no delimiter character, unless the -s option is specified
-n      with -b: don't split multibyte characters
--complement
    complement the set of selected bytes, characters or fields
```

```

-s, --only-delimited
    do not print lines not containing delimiters
--output-delimiter=STRING
    use STRING as the output delimiter the default is to use the
input delimiter
-z, --zero-terminated
    line delimiter is NUL, not newline
--help display this help and exit
--version
    output version information and exit

```

### Eksempler:

1) Hent ut navn, orgnummer og antall ansatte fra Brønnøysunds enhetsregister, og erstatt semikolon med komma som skille tegn:

Hent filen fra difi:

```
$ wget https://hotell.difi.no/download/brreg/enhetsregisteret
```

(vi kan bruke **head** for å se strukturen på filen):

```

$ head enhetsregisteret
orgnr;navn;organisasjonsform;forretningsadr;forradrpostnr;forradrpoststed;
forradrkommnr;forradrkommnavn;forradrland;postadresse;ppostnr;ppoststed;pp
ostland;regifr;regimva;nkode1;nkode2;nkode3;sektorkode;konkurs;avvikling;t
vangsavvikling;regiaa;regifriv;regdato;stiftelsesdato;tlf;tlf_mobil:url;re
gnskap;hovedenhet;ansatte_antall;ansatte_dato
"974766507";"VOSS HERAD KOMMUNALAVDELING
OPPVEKST";"ORGL";"";"5700";"VOSS";"4621";"VOSS";"Norge";"";"5701";"VOSS";"
Norge";"N";"N";"84.120";"";"6500";"N";"N";"N";"J";"N";"01.09.1996";"01.
02.1969";"";"60510542";"1072";"15.04.2020"
"974774356";"VOSS HERAD KOMMUNALAVDELING
TEKNISK";"ORGL";"";"5700";"VOSS";"4621";"VOSS";"Norge";"";"5701";"VOSS";"N
orge";"N";"N";"84.130";"";"6500";"N";"N";"N";"J";"N";"01.09.1996";"01.0
4.1988";"";"60510542";"184";"12.03.2020"
"974781468";"VOSS HERAD RÅDMANNEN SIN
STAB";"ORGL";"";"5700";"VOSS";"4621";"VOSS";"Norge";"";"5701";"VOSS";"Norg
e";"N";"N";"84.110";"";"6500";"N";"N";"N";"J";"N";"01.09.1996";"01.01.1
995";"56 51 94 00";"";"60510542";"72";"15.04.2020"
"974770962";"VOSS
KINO";"ORGL";"";"5704";"VOSS";"4621";"VOSS";"Norge";"";"5701";"VOSS";"Norg
e";"N";"N";"59.140";"";"6500";"N";"N";"N";"J";"N";"01.09.1996";"01.12.1
973";"";"60510542";"4";"11.03.2020"

```

```

"922201722";"& DALE";"ENK";"H0101 Bjerkelundgata
6A";"0553";"OSLO";"0301";"OSLO";"Norge";"";"";"";"";"";"N";"N";"70.210";"";""
;"8200";"N";"N";"N";"N";"N";"11.02.2019";"";"";"";"";"";"";"";"";""
"917887721";"&ACTION";"FLI";"c/o Håvard Sørli Helgesmark
29";"7716";"STEINKJER";"5006";"STEINKJER";"Norge";"";"";"";"";"";"N";"N";"94.
991";"";"";"";"7000";"N";"N";"N";"N";"J";"17.10.2016";"12.10.2016";"";"";"";""
",""";"";"";""
"999015611";"&M HOLDING AS";"AS";"Bygg D12 Sandakerveien
24C";"0473";"OSLO";"0301";"OSLO";"Norge";"";"";"";"";"";"J";"N";"74.102";"";""
;"2100";"N";"N";"N";"N";"N";"16.10.2012";"04.10.2012";"";"";"900 54
237";"";"";"2019";"";"";"";""
"812467182";"&MORE AS";"AS";"Sofies gate
72";"0454";"OSLO";"0301";"OSLO";"Norge";"";"";"";"";"";"J";"J";"71.129";"";""
;"2100";"N";"N";"N";"N";"J";"N";"19.09.2013";"15.09.2013";"";"";"926 33
798";"";"";"2018";"";"";"1";"11.07.2017"
"920352928";"&TRADITION NORWAY AS";"AS";"Parkveien
41B";"0258";"OSLO";"0301";"OSLO";"Norge";"";"";"";"";"";"J";"J";"46.150";"";""
;"2100";"N";"N";"N";"N";"J";"N";"31.01.2018";"05.01.2018";"";"";"";"";"2018";"";
"2";"12.02.2020"

$ cut -d ';' -f 1,2,32 --output-delimiter=', ' enhetsregisteret
orgnr,navn,ansatte_antall
"974766507","VOSS HERAD KOMMUNALAVDELING OPPVEKST","1072"
"974774356","VOSS HERAD KOMMUNALAVDELING TEKNISK","184"
"974781468","VOSS HERAD RÅDMANNEN SIN STAB","72"
"974770962","VOSS KINO","4"
"922201722","& DALE",""
"917887721","&ACTION",""
"999015611","&M HOLDING AS",""
"812467182","&MORE AS","1"
"920352928","&TRADITION NORWAY AS","2"
... etc

```

## 2) Hent brukernavn og bruker-ID fra /etc/passwd og sorter etter navn

```

$ cut -d: -f1,3 /etc/passwd | sort
abrt:173
adm:3
akmods:974
apache:48
avahi:70
bin:1
chrony:994
colord:981
daemon:2

```

```
dbus:81
dnsmasq:986
flatpak:978
ftp:14
```

## ➔ paste

**paste** er motsvarigheten til [cut](#), og lar deg "lime inn" kolonner fra en fil i en annen fil, evt. til skjerm eller en | til et annet program.

**paste** tar disse parametrene:

-d, --delimiters=LIST  
reuse characters from LIST instead of TABs

-s, --serial  
paste one file at a time instead of in parallel

-z, --zero-terminated  
line delimiter is NUL, not newline

--help display this help and exit

--version  
output version information and exit

### Eksempler:

```
$ cat fornavn
Ole
Jan
Per
Kari
```

```
$ cat etternavn
Olsen
Jansen
Pettersen
Svendsen
```

```
$ paste fornavn etternavn
```



```
Ole    Olsen
Jan    Jansen
Per    Pettersen
Kari    Svendsen
```

```
$ paste -d ',' etternavn fornavn
Olsen,Ole
Jansen,Jan
Pettersen,Per
Svendsen,Kari
```

## ➔ comm og diff

**comm** og **diff** er to kommandoer som alr deg sammenlikne to tekstfiler og se hva som er likt og hva som er forskjellig mellom de to filene.

### **comm**

Her er et enkelt eksempel på bruk av **comm**:

```
$ cat frukt
appelsin
eple
mango
papaya
$ cat frukt2
ananas
banan
eple
mango
pære
$ comm frukt frukt2
      ananas
appelsin
      banan
          eple
          mango
papaya
      pære
```

**Forklaring:** comm produserer tre kolonner:

1. Det som finnes i fil a men ikke i fil b

2. Det som finnes i fil b men ikke i fil a
3. Det som er likt i de to filene

Vi kan velge å fjerne en eller flere av kolonnene, f.eks. kolonne 1 og 2, slik at vi bare står igjen med det som er felles:

```
$ comm frukt frukt2 -1 -2
eple
mango
```

## diff

**diff** gir oss en oversikt over forskjellen mellom to filer.

Her er et eksempel basert på lignende, men mer like frukt-filer enn ovenfor:

```
$ cat frukt1
ananas
banan
papaya
mango
pære
$ cat frukt2
ananas
banan
eple
mango
pære
$ diff frukt1 frukt2
3c3
< papaya
---
> eple
```

## Forklaring:

Utgangspunktet for **diff** er at den første filen skal redigeres med den andre filen som referanse-fil. Konkret:

**3c3** betyr at linje 3 i fil a skal byttes ut (c = change) med linje 3 i fil b, så ut med papaya og inn med eple, så er filene like.

## ➔ split - del opp en fil i flere mindre filer

Med kommandoen **split** kan vi dele opp en stor fil i mindre filer. Default-innstillingen er 1000 linjer per ny fil, men vi kan også dele filer opp etter størrelse.

### Eksempler:

#### 1) Hent teksten til boken Krig og Fred:

```
$ curl https://web.itfakultetet.no/war-and-peace.txt > kof.txt
$ ls -lh kof.txt
-rw-r--r-- 1 Lenovo 197609 3,2M des  7 00:46 kof.tx
```

#### 2) Del filen i filer på 1Mb størrelse hver, med prefiks krig\_og fred\_

```
$ split -b 1M kof.txt krig_og_fred_
$ ls -lh krig*
-rw-r--r-- 1 Lenovo 197609 1,0M des  7 00:59 krig_og_fred_ab
-rw-r--r-- 1 Lenovo 197609 1,0M des  7 00:59 krig_og_fred_ac
-rw-r--r-- 1 Lenovo 197609 118K des  7 00:59 krig_og_fred_ad
-rw-r--r-- 1 Lenovo 197609 1,0M des  7 00:59 krig_og_fred_aa
```

#### 3) Slå sammen delene til 1 fil igjen

```
$ cat krig_og_fred_aa krig_og_fred_ab krig_og_fred_ac krig_og_fred_ad >
krig_og_fred.txt
```

## ➔ Øvelse: Skriv direkte til en fil med echo og/eller cat

**echo** <tekst eller variabel> skriver til standard output, hvis ikke annet angis

**cat** <filnavn> - leser inn en fil og skriver til skjerm eller ny fil

Du kan skrive rett til en fil med **echo** og/eller **cat** på flere måter. Her er et par eksempler

1) med **echo "tekst" > (eller >>) filnavn (> overskriver filen, >> legger til en linje på slutten av filen)**

```
$echo "Dette er noe som skal logges" >> loggfil.txt
$echo "Dette er også noe som skal logges" >> loggfil.txt
```

```
$cat loggfil.txt
```

```
Dette er noe som skal logges
```

```
Dette er også noe som skal logges
```

## 2) med cat << avslutningstegn > filnavn

Skriv tekst over flere linjer og avslutt med avslutningstegnet (f.eks. EOF) på en egen linje tilslutt.

```
$ cat <<EOF>test.txt
```

```
> DETTE ER TITTELEN
```

```
> og her kommer resten av teksten
```

```
> som slutter på neste linje
```

```
> EOF
```

```
$ cat test.txt
```

```
DETTE ER TITTELEN
```

```
og her kommer resten av teksten
```

```
som slutter på neste linje
```

```
$cat<<slutt>>loggfil.txt
```

```
> og her er en linje til
```

```
> og enda en linje
```

```
> slutt
```

```
$ cat loggfil.txt
```

```
Dette er noe som skal logges
```

```
Dette er også noe som skal logges
```

```
og her er en linje til
```

```
og enda en linje
```

## ➡ Øvelse: Lese og endre en fil med while og read

I denne enkle øvelsen skal vi lese inn en fil med navn, hvor hver linje består av et fornavn og et etternavn, og endre den slik at etternavn kommer før fornavn, med et komma mellom de to.

La oss først lage filen, som vi kan kalle *navn*:

```
$ cat >>navn
```

```
Ole Moen
```

```
Petter Jensen
```

```
Kari Diesen  
Rolf Juster  
(avslutt med <ctrl> + c )
```

Slik kan vi skrive filen ut til skjermen med etternavn først:

```
$ while read fornavn etternavn  
> do  
> echo $etternavn, $fornavn  
> done < navn  
Moen, Ole  
Jensen, Petter  
Diesen, Kari  
Juster, Rolf
```

Vil vi lagre resultatet i en ny fil, f.eks. *navn2*, kan vi gjøre det slik

```
while read fornavn etternavn; do echo $etternavn, $fornavn; done < navn >  
navn2
```

(her står alt på 1 linje, og da bruker vi semikolon der vi ellers ville brukt linjeskift)

Vi ser at innholdet i *navn2* er riktig:

```
$ cat navn2  
Moen, Ole  
Jensen, Petter  
Diesen, Kari  
Juster, Rolf
```

Vi kan også endre teksten underveis, for eksempel ved å bruke *bash* sin innebygde endringsfunksjon:

```
${<tekst>/<gammel verdi>/<ny verdi>}
```

Vil vi endre alle forekomster av *<gammel verdi>*, setter vi to *//* etter teksten vi vil endre, slik:

```
${<tekst>//<gammel verdi>/<ny verdi>}
```

Her endre vi alle forekomster av *jensen* til *Jansson* og lagrer resultatet i filen: *navn3*:

```
$ while read fornavn etternavn; do echo ${etternavn//Jensen/Jansson},
$fornavn; done < navn > navn3
```

Vi kan sjekke resultatet ved å se på navn3:

```
$ cat navn3
Moen, Ole
Jansson, Petter
Diesen, Kari
Juster, Rolf
```

## ➔ Øvelse: Finn de 20 mest brukte kommandoene dine

I denne øvelsen skal vi se hvordan vi enkelt (relativt sett) kan hente ut en oversikt over de mest brukte kommandoene fra skallets **history**.

Vi kan dele operasjonen inn i trinn:

1. Hent alle lagrede kommandoer med kommandoen **history**
2. Set felt 1 til et mellomrom med kommandoen **awk '\$1=" "'**
3. Klipp ut felt 3 med kommandoen **cut -d ' ' -f3**
4. Sorter alfabetisk med kommandoen **sort**
5. Tell unike forekomster med kommandoen **uniq -c**
6. Sorter etter antall i synkende rekkefølge med kommandoen **sort -n -r**
7. Velg de 20 øverste på listen med kommandoen **head 20**

Slik vil hele kjeden av kommandoer se ut:

```
$ history | awk '$1=" "' | cut -d ' ' -f3 | sort | uniq -c | sort -n -r |
head -20
135 sudo
77 ls
59 grep
49 cat
48 man
42 echo
34 sed
33 egrep
23 getent
23 find
```

```
21 nmcli
18 chmod
17 resolvectl
17 history
16 hashcat
15 cut
14 ssh
14 head
13 iwlist
11 systemctl
```

Dersom du vil ha med parameterene også, kan du sette et minus-tegn etter 4 tallet i [cut](#)-kommandoen, som betyr hent fra felt 4 og ut linjen

```
$ history | awk '$1=" "| cut -d ' ' -f3- | sort | uniq -c | sort -n -r |
head -20
51 ls
46 systemctl restart httpd
25 ls -lh
22 vim pgadmin4.conf
20 htop
19 su terje
16 dnf upgrade
14 ls -lrt
14 cd ..
13 vim pgadmin4-v1-le-ssl.conf
9 cd /home/backup/server4/
8 vim /etc/httpd/conf.d/pgadmin4-le-ssl.conf
7 ls -lrth
7 journalctl -xe
7 du -sh
6 ls -l
5 systemctl restart jenkins
4 vim config_local.py
4 vim /etc/sysconfig/jenkins
4 vim /etc/httpd/conf.d/pgadmin4.conf
```

# Kapittel 6

## Sikkerhet

### ➔ Brannmur med UFW

UFW - Uncomplicated Fire Wall - er default brannmur for Ubuntu servere, og kan også enkelt installeres for Red Hat / Centos - servere med kommandoene:

```
# dnf install ufw
# systemctl enable ufw
# systemctl start ufw
```

#### Eksempler:

Når UFW kjører, kan du bl.a. bruke disse kommandoene

```
# ufw status (lister opp alle etablerte regler
# ufw status numbered (lister opp alle etablerte regler i nummerert
rekefølge)
# ufw delete <nummer> - sletter regel <nummer>
# ufw allow <portnummer>
# ufw allow <tjeneste> - f.eks. imap eller smtp
# ufw allow from <ip-adresse>
# ufw deny from <ip-adresse>
# ufw deny <portnummer>
Eksempler:
# ufw allow from 10.0.0.0/8
# ufw allow from 172.16.0.0/12
# ufw allow from 192.168.0.0/16
# ufw allow in on eth0 from 192.168.0.0/16
# ufw allow out on eth1 to 10.0.0.0/8
# ufw route allow in on eth0 out on eth1 to 10.0.0.0/8 from 192.168.0.0/16
# ufw limit 2222/tcp comment 'SSH port'
```

Bruk **man ufw** til å se flere valg og eksempler



## ➔ Port-scanning med nmap

### Sjekk åpne porter med nmap

Verktøyet **nmap** er en såkalt portskanner, som sjekker hvilke porter på en maskin som er åpne, og hvilke tjenester som bruker portene. Dette gir en indikasjon på hvilke tjenester en server har kjørende. **nmap** installeres med kommandoen:

```
$ sudo apt-get install nmap
```

**Merk:** Portskanning med nmap ansees som en invaderende handling, og bør kun brukes på egne servere eller i samråd med serverens eier. Det er litt som å sjekke hvilke dører i et hus som er låst.

Slik skanner du enkelt din egen maskin med nmap:

```
$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-26 16:36 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

Scan et enkelt domene:

```
# nmap scanme.org
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-29 19:43 CET
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
```

Du kan også scanne hele eller deler av et nettverk

```
$ nmap 10.0.0.*
Nmap scan report for 10.0.0.16
Host is up (0.0032s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp  open  iphone-sync
Nmap scan report for 10.0.0.20
Host is up (0.0058s latency).
All 1000 scanned ports on 10.0.0.20 are closed
Nmap scan report for wp530 (10.0.0.89)
Host is up (0.00023s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
5900/tcp  open  vnc
Nmap scan report for _gateway (10.0.0.138)
Host is up (0.0030s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
23/tcp    filtered telnet
53/tcp    open    domain
80/tcp    open    http
443/tcp   filtered https
5431/tcp  open    park-agent
7676/tcp  open    imqbrokerd
Nmap done: 256 IP addresses (4 hosts up) scanned in 45.19 seconds
$ nmap -A noderia.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 15:20 CET
Nmap scan report for noderia.com (136.243.23.69)
Host is up (0.069s latency).
rDNS record for 136.243.23.69: server4.noderia.com
Not shown: 987 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    closed ssh
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: server4.noderia.com, PIPELINING, SIZE, VRFY, ETRN,
STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=server4.noderia.com
```

```

| Subject Alternative Name: DNS:server4.noderia.com
| Not valid before: 2020-09-27T14:09:51
|_Not valid after: 2020-12-26T14:09:51
|_ssl-date: TLS randomness does not represent time
80/tcp open http Apache httpd 2.4.37 ((centos)
OpenSSL/1.1.1c mod_wsgi/4.6.4 Python/3.6)
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c mod_wsgi/4.6.4
Python/3.6
|_http-title: Did not follow redirect to https://noderia.com/
143/tcp open imap Dovecot imapd
|_imap-capabilities: IDLE STARTTLS capabilities OK more ID AUTH=LOGINA0001
have ENABLE SASL-IR Pre-login LOGIN-REFERRALS IMAP4rev1 LITERAL+
AUTH=PLAIN post-login listed
| ssl-cert: Subject: commonName=server4.noderia.com
| Subject Alternative Name: DNS:server4.noderia.com
| Not valid before: 2020-09-27T14:09:51
|_Not valid after: 2020-12-26T14:09:51
443/tcp open ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c mod_wsgi/4.6.4
Python/3.6
|_http-title: coming soon
| ssl-cert: Subject: commonName=noderia.com
| Subject Alternative Name: DNS:noderia.com
| Not valid before: 2020-11-29T22:56:48
|_Not valid after: 2021-02-27T22:56:48
1433/tcp open ms-sql-s Microsoft SQL Server 15.00.4073.00
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2020-12-07T14:20:29
|_Not valid after: 2050-12-07T14:20:29
|_ssl-date: TLS randomness does not represent time
1521/tcp open oracle-tns Oracle TNS listener 1.2.0.0.0
(unauthorized)
3306/tcp open mysql MySQL 5.5.5-10.5.8-MariaDB
| mysql-info:
| Protocol: 10
| Version: 5.5.5-10.5.8-MariaDB
| Thread ID: 100253
| Capabilities flags: 63486
| Some Capabilities: SupportsCompression, SupportsLoadDataLocal,
Support41Auth, IgnoreSigpipes, Speaks41ProtocolOld, Speaks41ProtocolNew,
InteractiveClient, ODBCClient, FoundRows, ConnectWithDatabase,
SupportsTransactions, IgnoreSpaceBeforeParenthesis,
DontAllowDatabaseTableName, LongColumnFlag, SupportsMultipleResults,
SupportsAuthPlugins, SupportsMultipleStatments
| Status: Autocommit
| Salt: 'lpmQ.20v'ZpEGu:\@m&

```

```

|_ Auth Plugin Name: mysql_native_password
5432/tcp open  postgresql      PostgreSQL DB 9.6.0 or later
| fingerprint-strings:
|   SMBProgNeg:
|     SFATAL
|     VFATAL
|     C0A000
|     Munsupported frontend protocol 65363.19778: server supports 2.0 to
3.0
|     Fpostmaster.c
|     L2108
|_ RProcessStartupPacket
8000/tcp open  http      CherryPy wsgiserver
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: itfakultetet.no
|_http-title: OmniDB
8080/tcp open  http      Jetty 9.4.33.v20201020
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.33.v20201020)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
8081/tcp closed blackice-icecap
9090/tcp open  ssl/zeus-admin?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad request
|     Content-Type: text/html; charset=utf8
|     Transfer-Encoding: chunked
|     X-DNS-Prefetch-Control: off
|     Referrer-Policy: no-referrer
|     X-Content-Type-Options: nosniff
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>
|     request
|     </title>
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|     <meta name="viewport" content="width=device-width, initial-
scale=1.0">
|     <style>
|     body {
|     margin: 0;
|     font-family: "RedHatDisplay", "Open Sans", Helvetica, Arial, sans-
serif;
|     font-size: 12px;

```

```

|     line-height: 1.66666667;
|     color: #333333;
|     background-color: #f5f5f5;
|     border: 0;
|     vertical-align: middle;
|     font-weight: 300;
|     margin: 0 0 10px;
|_   @font-face {
| ssl-cert: Subject:
commonName=server4.noderia.com/organizationName=53ee87f33e3a4c1b9edeaa2083
de06e5/countryName=US
| Subject Alternative Name: DNS:server4.noderia.com, DNS:localhost, IP
Address:127.0.0.1
| Not valid before: 2020-10-08T19:48:47
|_Not valid after:  2030-11-26T12:28:47
|_ssl-date: TLS randomness does not represent time
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port5432-TCP:V=7.80%I=7%D=12/7%Time=5FCE3A28%P=x86_64-redhat-linux-gnu%
SF:r(SMBProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fro
SF:ntend\x20protocol\x2065363\19778:\x20server\x20supports\x202\0\x20to\
SF:x203\0\0Fpostmaster.c\0L2108\0RProcessStartupPacket\0\0");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port9090-TCP:V=7.80%T=SSL%I=7%D=12/7%Time=5FCE3A63%P=x86_64-redhat-linu
SF:x-gnu%r(GetRequest,E45,"HTTP/1\1\x20400\x20Bad\x20request\r\nContent-T
SF:ype:\x20text/html;\x20charset=utf8\r\nTransfer-Encoding:\x20chunked\r\n
SF:X-DNS-Prefetch-Control:\x20off\r\nReferrer-Policy:\x20no-referrer\r\nX-
SF:Content-Type-Options:\x20nosniff\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html
SF:>\n<head>\n\x20\x20\x20\x20<title>\r\nb\r\nBad\x20request\r\n08\r\n</t
SF:itle>\n\x20\x20\x20\x20<meta\x20http-equiv=\x20Content-Type\x20content=
SF:\x20text/html;\x20charset=utf-8\x20>\n\x20\x20\x20\x20<meta\x20name=\x20viewp
SF:ort\x20content=\x20width=device-width,\x20initial-scale=1\0\x20>\n\x20\x
SF:20\x20\x20<style>\n\tbody\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0font-family:\x20"RedHatDisplay",\x20"Open\x20Sans",\x20Helvetica,\
SF:\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:\x20font-size:\x2012px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0line-height:\x201\66666667;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20color:\x20#333333;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20background-color:\x20#f5f5f5;\n\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20border:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:\x20\x20vertical-align:\x20middle;\n\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20font-family:\x20"RedHatDisplay",\x20"Open\x20Sans",\x20Helvetica,\
SF:\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

```

```

SF:0\x20\x20\x20\x20\x20font-weight:\x20300;\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20@font-face\x20{\n\x20\x2
SF:20\x20\x20\x20\x20\x20\x20\x20)%r(HTTPOptions,E45,"HTTP/1.1\x20400\x2
SF:0Bad\x20request\r\nContent-Type:\x20text/html;\x20charset=utf8\r\nTrans
SF:fer-Encoding:\x20chunked\r\nX-DNS-Prefetch-Control:\x20off\r\nReferrer-
SF:Policy:\x20no-referrer\r\nX-Content-Type-Options:\x20nosniff\r\n\r\n29\
SF:r\n<!DOCTYPE\x20html>\n<html>\n<head>\n\x20\x20\x20\x20<title>\r\nnb\r\n
SF:Bad\x20request\r\nnd08\r\n</title>\n\x20\x20\x20\x20<meta\x20http-equiv=
SF:"Content-Type"\x20content="\text/html;\x20charset=utf-8">\n\x20\x20\x20
SF:x20\x20<meta\x20name="\viewport"\x20content="\width=device-width,\x20i
SF:nitial-scale=1.0">\n\x20\x20\x20\x20<style>\n\tbody\x20{\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20"RedHatDisplay",\x20"Op
SF:en\x20Sans",\x20Helvetica,\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2012px;\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201.66666667;\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333333;\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#f5f5f5;\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20img\x20{\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20border:\x200;\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20vertical-align:\x20middle;\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20h1\x20{\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20300;\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20p\x20{\
SF:0{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x
SF:2010px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20@font-face\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20");
Service Info: Host: server4.noderia.com

```

#### Host script results:

```

| ms-sql-info:
|   136.243.23.69:1433:
|     Version:
|       name: Microsoft SQL Server
|       number: 15.00.4073.00
|       Product: Microsoft SQL Server
|_   TCP port: 1433

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
 Nmap done: 1 IP address (1 host up) scanned in 197.74 seconds

**nmap** har mange flere valg, sjekk **man nmap** for en oversikt

## ➔ Passord-cracking med ncrack

**ncrack** er et program som har en rekke moduler egnet for å gjette passord til ulike tjenester.

### Fra manualen:

```
"Ncrack is an open source tool for network authentication cracking.
It was designed for high-speed parallel
cracking using a dynamic engine that can adapt to different network
situations. Ncrack can also be extensively
fine-tuned for special cases, though the default parameters are
generic enough to cover almost every situation.
It is built on a modular architecture that allows for easy
extension to support additional protocols. Ncrack is
designed for companies and security professionals to audit large
networks for default or weak passwords in a
rapid and reliable way. It can also be used to conduct fairly
sophisticated and intensive brute force attacks
against individual services."
```

### Moduler:

SSH, RDP, FTP, Telnet, HTTP(S), Wordpress, POP3(S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSSQL, MongoDB, Cassandra, WinRM, OWA, DICOM

### Eksempler:

```
EEST $ ncrack 10.0.0.130:21 192.168.1.2:22
Starting Ncrack 0.6 ( http://ncrack.org ) at 2016-01-03 22:10

Discovered credentials for ftp on 10.0.0.130 21/tcp:
10.0.0.130 21/tcp ftp: admin hello1
Discovered credentials for ssh on 192.168.1.2 22/tcp:
192.168.1.2 22/tcp ssh: guest 12345
192.168.1.2 22/tcp ssh: admin money$
Ncrack done: 2 services scanned in 156.03 seconds.
Ncrack finished.
$ ncrack -v --user root localhost:22
$ ncrack -v -T5 https://192.168.0.1
```

### Forklaring til parameterene:

- -v = verbose
- -T5 = "insane mode" - bruker max båndbredde

Flere eksempler og valg på manualsidene til **ncrack**: <http://nmap.org/ncrack/man.html>

## ➔ Kryptering av filer og epost med GnuPG

GnuPG står for GNU Privacy Guard og forkortes gjerne til gpg. GnuPg brukes til å kryptere og dekryptere filer og eposter, og til å signere filer og eposter med en digital signatur. Vi skal her introdusere de vanligste funksjonene og kommandoene i pakken gpg, som kjøres fra kommandolinjen. Vi skal også se på integrasjon av gpg i enkelte epostlesere (MUAs).

### Installasjon av GnuPG

---

GnuPG er som regel installert på de fleste Linux-servere. Du kan enkelt sjekke dette med kommandoen:

```
$ which gpg  
/usr/bin/gpg
```

Dersom GnuPG ikke er installert, kan du installere pakken gnupg slik:

```
$ sudo apt/yum/dnf install gnupg
```

### Lage offentlige og private nøkler

---

Det første man gjerne vil gjøre er å lage en offentlig og en privat nøkkel. Den offentlige nøkkelen gjøres tilgjengelig for de som ønsker å sende deg en kryptert fil eller epost, og brukes også av deg når du krypterer en fil. Den private (hemmelige) nøkkelen brukes når du dekrypterer en fil eller en epost, og inneholder en passord-setning som kun du kjenner til.

Slik genererer du et nøkkelpar:

```
$ gpg --full-gen-key
```

Vennligst velg hvilken type nøkkel du vil ha:

- (1) RSA and RSA (default)
- (2) DSA and Elgamal
- (3) DSA (bare signering)
- (4) RSA (bare signering)

Tast inn *1* eller *<enter>* for å generere RSA-nøkler. Du blir så bedt om å angi størrelsen på nøkkelen:



### Hvilken nøkkelstørrelse vil du ha? (2048)

Nøkkelstørrelser varierer mellom 1024 og 4096 bits. 4096 bits er godt nok for de fleste formål. Tast inn 4096 og <enter> for å lage 4096-bits nøkler. Du må nå angi hvor lenge nøklene skal være gyldige:

**Vennligst angi hvor lenge nøkkelen skal være gyldig.**

**0 = nøkkelen utgår ikke**

**<n> = nøkkelen utgår om n dager**

**<n>w = nøkkelen utgår om n uker**

**<n>m = nøkkelen utgår om n måneder**

**<n>y = nøkkelen utgår om n år**

Tast inn 0 eller <enter> for en nøkkel som ikke er tidsbegrenset, eller f.eks. 1y for en nøkkel som varer ett år. Neste skritt er å fylle inn informasjonen nøkkelen skal inneholde. Dette er Fullt navn (minst 5 tegn), Epostadresse og en valgfri kommentar. Formen på informasjonen blir til slutt en slik linje:

«Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>»

Tast til slutt inn R (riktig) for å verifisere informasjonen du har tastet inn, og så genereres nøkkelen. Underveis kan du få meldinger som dette:

Ikke nok tilfeldige byter tilgjengelig. Vennligst gjør noe annet arbeid for å gi operativsystemet en sjanse til å samle mer entropi! (Trenger 155 flere byter)

Alt du gjøre på maskinen, som å bruke tastaturet eller musen genererer tilfeldige bytes som brukes til nøkkelgenereringen. Når nøkkelen er generert, får du en melding som ligner på denne:

gpg: nøkkel 17DAE5604F84B6FC markert som endelig betrodd.

gpg: opphevelsessertifikat lagret som «/home/terje/.gnupg/openpgp-revocs.d/A893AE75AD9E6313D1EE3CC917DAE5604F84B6FC.rev»

offentlig og hemmelig nøkkel opprettet og signert.

pub rsa3072 2020-12-08 [SC] [utgår: 2022-12-08]

A893AE75AD9E6313D1EE3CC917DAE5604F84B6FC

uid Terje Berg-Hansen (Use this key for cooped.org)

<terje@cooped.org>

sub rsa3072 2020-12-08 [E] [utgår: 2022-12-08]

Du har nå generert både offentlig og privat nøkkel for navnet/epostadressen du tastet inn, og kan begynne å bruke disse.

Dersom det ikke opprettes et opphevingssertifikat etter at man har laget en nøkkel, anbefales det å gjøre dette. Sertifikatet (revoke certificate) trenger du hvis den private nøkkelen din blir kompromittert, eller hvis du av andre grunner trenger å slette (oppheve) den offentlige nøkkelen fra en offentlig nøkkel-server (se neste avsnitt). Slik lager du et opphevingssertifikat manuelt:

```
$ gpg --output revoke.asc --gen-revoke <brukernavn>
```

Du blir bedt om å angi en grunn til opphevelsen, og en evt. kommentar:

```
Please select the reason for the revocation:
0 = Ingen grunn er angitt
1 = Nøkkelen har blitt kompromittert
2 = Nøkkelen er overgått
3 = Nøkkelen er ikke lengre i bruk
Q = Cancel
```

Sertifikatet er nå tilgjengelig i filen *revoke.asc*, som du bør ta godt vare på, siden denne filen kan brukes av alle til å oppheve din offentlige nøkkel

## Opplasting av offentlig nøkkel til en nøkkel-server

For at andre skal kunne sende deg krypterte filer eller eposter, laster du opp din offentlige nøkkel til en nøkkel-server. Det finnes en rekke nøkkel-servere, og siden disse er synkroniserte med hverandre, er det greit å bruke den som ligger som default hos GnuPG. Dersom det ikke er lagt inn en default nøkkelserver, legger du den inn ved å legge til denne linjen i filen *~/.gnupg/gpg.conf*

**keyserver hkp://keys.gnupg.net** (evt en annen server du vil bruke som default)

Slik laster du opp din nylig genererte offentlige nøkkel:

```
$ gpg --send-keys <nøkkel-ID>
```

For å liste opp dine offentlige nøkkel-IDer kan du bruke denne kommandoen:

```
$ gpg -k (samme som $ gpg --list-keys)

pub 2048R/42AADD51 2011-08-29
uid Terje Berg-Hansen (Axenna) <terje@axenna.no>
```

Nøkkel-ID i eksemplet ovenfor er 42AADD51.

Du kan evt. velge hvilken nøkkel-server du vil laste nøkkelen opp til, f.eks. Ubuntus nøkkelserver, slik:

```
$ gpg --send-keys --keyserver keyserver.ubuntu.com <nøkkel-ID>
```

Du kan også lagre en ascii-versjon av den offentlige nøkkelen. Denne kan sendes eller limes inn på enkelte nettsteder, og kan være nyttig hvis for eksempel nøkkel-servere er utilgjengelig. Slik eksporterer du nøkkelen til filen *mykey.asc*:

```
$ gpg --output mykey.asc --export -a <nøkkel-ID>
```

## Finne og importere andres offentlige nøkler

For å kunne sende noen en kryptert fil, må du ha tilgang til vedkommendes offentlige nøkkel. Du kan søke i nøkkel-servernes database etter andres offentlige nøkler slik:

```
$ gpg --search-keys <navn, firmanavn eller epostadresse>
```

Søkeresultatet inneholder et nummer til hver nøkkel som blir funnet. Tast inn nummeret + <enter>, så importeres nøkkelen til din nøkkelring, og du kan bruke den til å kryptere filer/eposter som skal dekrypteres av vedkommende.

## Kryptering og dekryptering av filer med GnuPG

Hvis du vil kryptere en fil for eget bruk, kan du bruke din egen offentlige nøkkel. Skal du kryptere en fil du vil sende til andre, krypterer du filen med vedkommendes offentlige nøkkel. Slik krypterer du filen *file.txt* med nøkkelen til petter@itfakultetet.no:

```
$ gpg -r petter@itfakultetet.no -e file.txt
```

GnuPG lagrer en ny, kryptert fil med navnet: *file.txt.gpg*, som du kan sende til Petter

Når du mottar en fil som er kryptert ned din offentlige nøkkel, dekrypterer du den slik:

```
$ gpg file.txt.gpg
```

GnuPG sjekker om du har den private (hemmelige) nøkkelen som tilsvarer den offentlige nøkkelen filen er kryptert med, og ber deg om passord-frasen for å låse den opp. De dekrypterte dataene lagres i en ny fil: *file.txt*

## Signering av filer og epost med GnuPG

### Oversikt over pgp-programmer for LINUX epost

#### [Claws Mail](#)

Is a very nice GTK+ based MUA with full support for GnuPG. The Windows version is part of [Gpg4win](#) .

#### [Enigmail](#)

Is a plug-in for Mozilla's mailer.

#### [Evolution](#)

Is a catch all MUA application for the GNOME desktop.

#### [exmh](#)

Is a Tcl/Tk based MUA.

#### [ez-pine-gpg](#)

ez-pine-gpg is a set of scripts that allows beginners and experts to use gpg with Pine. There are plenty of other applications that allow gpg to be used with Pine: this one is intended to be the best, since it merges intuitive use with powerful features. The result is an application that's not only fast and secure, but also perfect for novices and power-users alike.

#### [Gabber](#)

Gabber is a Free and Open Source GNOME client for an instant messaging system called Jabber. Jabber is a Free and Open Source distributed instant messaging system. It does not rely on a single server, and the protocol is well documented. Jabber allows communication with many different instant messaging systems, including ICQ and AIM.

#### [GnuPG Shell](#)

GnuPG Shell is a cross-platform graphical frontend for GnuPG.

#### [GPA](#)

Aims to be the standard GnuPG graphical frontend. [GPA](#) is hosted on this site.

#### [gpg\\_mail](#)

This script is able to encode/sign emails in an automatic fashion. There is also a [mirror site](#) available.

### KGpg

Is a KDE frontend for GnuPG.

### KMail

From the KDE desktop, it does also support GnuPG.

### kuvert

This frontend is for GnuPG and old-style pgp2. It works slightly similar to Raph Levien's premail: it sits between MUA and MTA and decides based on the keyring contents whether to sign, sign/encrypt or leave an email as it is.

kuvert is unix-only and designed to work for outbound emails only. It's a daemon tool and requires some form of passphrase cache.

kuvert has been around (under earlier names) since about 1996.

### MagicPGP

Is yet another set of scripts to use GnuPG with Pine.

### Mailcrypt

For Emacs. You may need the latest [patches](#) until there is a new release of Mailcrypt.

### Mew

Has support for GnuPG.

### Mutt

Is an advanced MUA with complete MIME and GnuPG/PGP support. It is also available an [internationalized version](#) .

### PGG

PGG is a complete PGP signing/encrypting solution provided from scratch by the Gnus development team. It deserves the same than [mailcrypt](#) but it has also native MIME support whereas mailcrypt does not. There is no PGG homepage at the moment, sorry.

### pgpenvelope

Is a Pine and procmail filter which allows one to process messages with GnuPG.

### pgpgpg

Is a comandline wrapper tool to allow the use of scripts written for PGP with GnuPG.

### PSI

Psi is a free and crossplatform client for connecting to the Jabber network. It supports multiple accounts, group chat, Unicode, and strong security (TLS and GnuPG).

### [Scribe](#)

Scribe is a small and fast email client that lets you send, receive and manage email without fuss. Scribe comes with a [plugin](#) that calls GnuPG.

### [Seahorse](#)

Is a GNOME frontend for GnuPG.

### [Sylpheed](#)

Is a very nice GTK+ based MUA with full support for GnuPG.

### [Tkabber](#)

Tkabber is a free client for an instant messaging system called Jabber. It is written in Tcl/Tk and supports many features like support of unicode, ssl support, http proxy, file transfers and support of multi-user conference protocol.

### [Topal](#)

Is another program to use GnuPG with Pine.

### [wija](#)

wija is a free and cross-platform Jabber/XMPP client written in Java, with built-in GnuPG key rings management GUI. Its extended protocols allow users to encrypt chat and multi-user chat as well as encrypting/signing messages and signing presence of the user. It is multilingual and runs on GNU/Linux, Mac OS X and Windows.

### [XAP](#)

Is the X application panel and filemanager

## ➡ Passord-cracking med hashcat

Dersom man har tilgang til krypterte passord, f.eks. ved å få tilgang til filen **/etc/shadow** eller en database-tabell med krypterte passord, er **hashcat** antagelig det mest effektive verktøyet for å cracke passordene. **hashcat** markedsfører seg som et verktøy for å gjenvinne tapte passord, men brukes ekstensivt av hackere til å få ulovlig tilgang til servere, epostkontoer osv.

Den enkleste måten å bruke hashcat på er fra en sikkerhets-orientert distro, som f.eks. **Kali Linux**. Da får man med nyttige ordlister også.

I denne øvelsen skal vi bruke hashcat med ordlisten "**rockyou**" for å se hvor enkelt det er å cracke vanlige, enkle passord, selv om de er kryptert med en sterk algoritme.

## Forberedelse

### 1) Installere Kali Linux, f.eks. i en lokal VirtualBox

### 2) unzip rockyou-ordlisten, som ligger i mappen **/usr/share/wordlists**

```
$ wc /usr/share/wordlists/rockyou.txt
14344392 14442062 139921507 /usr/share/wordlists/rockyou.txt
```

### 3) Lag noen enkle, krypterte passord:

```
$ echo -n "password" | sha512sum | tr -d " -" > passwords_sha512
$ echo -n "12345678" | sha512sum | tr -d " -" >> passwords_sha512
$ echo -n "admin123" | sha512sum | tr -d " -" >> passwords_sha512

$ cat passwords_sha512
a9d50700baec3d1e40c238bcb37847d3a9633e174dfabeedddcac68d661d02937f71c0edba8
b41602e8993015c465ec330f40843849c163d9235d00542a96e3a1
fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c65
2826e0fc5c706695a03cddce372f139eff4d13959da6f1f5d3eabe
7fcf4ba391c48784edde599889d6e3f1e47a27db36ecc050cc92f259bfac38afad2c68a1ae
804d77075e8fb722503f3eca2b2c1006ee6f6c7b7628cb45ffffd1d
```

## Crack passordene med hashcat

```
$ hashcat -m 1700 passwords_sha512 /usr/share/wordlists/rockyou.txt -O
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP,
DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
=====
* Device #1: pthread-Intel(R) Core(TM) i7-3740QM CPU @ 2.70GHz, 4397/4461
MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13
rotates
```

Rules: 1

Applicable optimizers applied:

- \* Optimized-Kernel
- \* Zero-Byte
- \* Precompute-Init
- \* Early-Skip
- \* Not-Salted
- \* Not-Iterated
- \* Single-Salt
- \* Raw-Hash
- \* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.

Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:

- \* Filename.: /usr/share/wordlists/rockyou.txt
- \* Passwords.: 14344385
- \* Bytes.....: 139921507
- \* Keyspace.: 14344385

```
fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c65
2826e0fc5c706695a03cddce372f139eff4d13959da6f1f5d3eabe:12345678
a9d50700baec3d1e40c238bcb37847d3a9633e174dfabeeddcac68d661d02937f71c0edba8
b41602e8993015c465ec330f40843849c163d9235d00542a96e3a1:password
7fcf4ba391c48784edde599889d6e3f1e47a27db36ecc050cc92f259bfac38afad2c68a1ae
804d77075e8fb722503f3eca2b2c1006ee6f6c7b7628cb45fffd1d:admin123
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: SHA2-512
Hash.Target.....: passwords_sha512
Time.Started....: Mon Dec  7 17:34:12 2020 (0 secs)
Time.Estimated...: Mon Dec  7 17:34:12 2020 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 368.2 kH/s (6.46ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered.....: 3/3 (100.00%) Digests
Progress.....: 90113/14344385 (0.63%)
Rejected.....: 1/90113 (0.00%)
Restore.Point....: 86017/14344385 (0.60%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: bunny10 -> KAROLINA
```



```
Started: Mon Dec 7 17:34:08 2020  
Stopped: Mon Dec 7 17:34:14 2020
```

# Kapittel 7

## Jobber, tjenester og prosesser

### ➔ Håndtering av jobber med bg, fg, jobs, nohup, & og ctrl+z

Hver gang du skriver en kommando i et terminalvindu startes en *prosess* og en *jobb*. Hver jobb tildeles et jobbnummer og en prosess-ID (PID). Her skal vi vise noen nyttige kommandoer for å håndtere jobber før og etter at de er startet.

### Forgrunn og bakgrunn

Starter du en tidkrevende jobb, eller f.eks. et gui-basert program fra kommandolinjen, opptas terminalvinduet så lenge jobben kjøres, og du blokkeres fra å gjøre andre ting i vinduet. Du kan frigjøre kommandolinjen for bruk ved å kjøre jobben i bakgrunnen. Dette kan du gjøre når du starter jobben, f.eks. slik:

```
$ gimp &  
[1] 6527
```

Dette starter Gimp i bakgrunnen og frigjør kommandolinjen for videre bruk. Som respons på kommandoen gis et jobbnummer og en PID - i dette tilfellet kjøres Gimp i bakgrunnen som jobb 1 med PID 6527.

eller slik:

```
$ find / -name *.conf | grep -i failed > /tmp/failed.txt &  
[2] 6531
```

Denne tidkrevende kommandoen finner alle filer som slutter med `.conf`, søker etter ordet *failed* - med store eller små bokstaver - lagrer resultatet i filen *failed.txt*, og frigjør kommandolinjen for videre bruk. Jobben kjøres i bakgrunnen som jobb 2 med PID 6531

## Kjøre jobber i bakgrunnen

---

Dersom du allerede kjører en jobb i forgrunnen, men vil sende den til bakgrunnen for å frigjøre terminalvinduet, må du gjøre dette i to operasjoner. Først *suspenderer* du jobben, dvs. stopper den midlertidig med kommandoen:

```
$ <ctrl>+z
```

Så starter du den igjen i bakgrunnen med kommandoen:

```
$ bg
```

Programmet vil kjøres i bakgrunnen, men vil fortsatt sende meldinger til terminalvinduet.

Du kan bringe jobben til forgrunnen igjen med denne kommandoen:

```
$ fg
```

**Merk:** Har du flere jobber kjørende i bakgrunnen, bringer du en av dem til forgrunnen ved å taste **fg** + **jobbnummer**, f.eks. slik:

```
$ fg 1
```

(bringer Gimp til forgrunnen i dette eksemplet)

## Jobboversikt

---

Oversikt over hvilke jobber som kjører i bakgrunnen får du enkelt ved å taste kommandoen:

```
$ jobs  
[1]+  Running gimp &
```

Terminalvinduet svarer med jobbnummer, status og hvilken kommando som ble gitt for å starte jobben.

## Starte grafiske programmer

---

Du kan også starte GUI-applikasjoner, dvs. vanlige programmer med grafisk brukergrensesnitt fra kommandolinjen ved å skrive inn programmets navn eller en variasjon av dette (f.eks. *oowriter* for å starte Open Office Tekstbehandling), men programmet vil starte i sitt eget vindu. Skriver du en `&` etter programnavnet, f.eks.

```
$ gimp &
```

vil Gimp åpnes i et eget vindu og kjøre som en prosess i bakgrunnen i terminalvinduet - slik at kontrollen går tilbake til kommandolinjen og du kan fortsette å skrive programmer. Uten `&` vil du ikke kunne bruke terminalvinduet før gimp lukkes igjen. En annen fordel med å starte programmer fra kommandolinjen er at feilmeldinger og annen informasjon vil vises i terminalvinduet så lenge programmet kjøres. Denne informasjonen går ellers tapt eller lagres i spesielle log-filer.

## Starte programmer som forblir kjørende etter utlogging - med `nohup`

---

Programmer du starter vi kommandolinjen, vil avsluttes når du lukker terminavinduet programmet startes fra, eller når du logger deg ut. For å unngå dette kan du starte kommandoen med nøkkelordet: **`nohup`**. Det står for **no hangup**, og daterer seg fra tiden man brukte oppringte forbindelser. Kommandoen nedenfor vil starte programmet "mittprogram" i bakgrunnen, og la det fortsette å kjøre etter at du har logget deg ut.

```
$ nohup mittprogram &
```

## Avslutte programmer som ikke vil avslutte på vanlig måte med `kill` og `killall`

---

Med kommandolinjen kan du enkelt avslutte et program som "henger". Det er to kommandoer som kan gjøre dette: **`kill`** etterfulgt av et PID-nummer (Prosess-ID nummer) og **`killall`** etterfulgt av programmets navn.

Du kan enkelt finne PID-nummeret med kommandoen **`pidof`** etterfulgt av programets navn. For eksempel slik:

```
$ pidof tmux
28790
$ kill 28790
[terminated]
```

Kommandoen **`kill`** uten noen parametere utfører det samme som **`kill -15`**, som avslutter programmet på en ryddig måte, slik at f.eks. programmets midlertidige filer blir slettet osv. Dersom dette ikke avslutter programmet, kan man bruke parameteret `-9`, som avslutter direkte og brutalt, slik:

```
$ kill -9 28798
```

Hvis programmet kjører mange prosesser, kan det være enklere å avslutte dem alle samtidig, med kommandoen **killall** etterfulgt av navnet til programmet, dvs kommandoen det ble startet med, f.eks. so i eksemplet nedenfor.

Vi kan bruke kommandoen **ps** til å se at apache webserver (som startes med kommandoen: **httpd** på en RedHat-basert server) kjører flere prosesser:

```
$ ps -ef | grep httpd
root      3217      1  0 nov.23 ?        00:00:05 /usr/sbin/httpd -
DFOREGROUND
apache    3483      3217  0 nov.23 ?        00:00:00 /usr/sbin/httpd -
DFOREGROUND
apache    3485      3217  0 nov.23 ?        00:00:32 /usr/sbin/httpd -
DFOREGROUND
apache    3486      3217  0 nov.23 ?        00:00:24 /usr/sbin/httpd -
DFOREGROUND
apache    3488      3217  0 nov.23 ?        00:00:24 /usr/sbin/httpd -
DFOREGROUND
apache    138406     3217  0 nov.23 ?        00:00:20 /usr/sbin/httpd -
DFOREGROUND
terje     415560     6469  0 16:48 ?        00:00:00 /usr/sbin/httpd -f
/usr/share/gnome-user-share/dav_user_2.4.conf -C Listen 33421
terje     415561     415560  0 16:48 ?        00:00:00 /usr/sbin/httpd -f
/usr/share/gnome-user-share/dav_user_2.4.conf -C Listen 33421
terje     415562     415560  0 16:48 ?        00:00:00 /usr/sbin/httpd -f
/usr/share/gnome-user-share/dav_user_2.4.conf -C Listen 33421
terje     421766     8928  0 19:08 pts/1    00:00:00 grep --color=auto
httpd
terje@wp530:~/utvikling2/bash$ sudo killall httpd
terje@wp530:~/utvikling2/bash$ ps -ef | grep httpd
terje     421792     8928  0 19:09 pts/1    00:00:00 grep --color=auto
httpd
```

Vi kan avslutte dem alle med på en gang (hvis vi ikke kan avslutte på vanlig måte med systemctl), slik

```
$ sudo killall httpd
```

Som vi ser er alle prosessene avsluttet:

```
$ ps -ef | grep httpd
```

```
terje      421792      8928  0 19:09 pts/1      00:00:00 grep --color=auto
httpd
```

## ➔ Finn kjørende prosesser med **ps**

Kommandoen **ps** gir en oversikt over alle eller utvalgte deler av de prosessene maskinen kjører på et gitt tidspunkt. For å få en løpende oppdatering av prosesser kan du for eksempel bruke **top** eller **htop**.

### Eksempler:

#### List alle prosesser på systemet med standard syntaks:

```
ps -e
ps -ef
ps -eF
ps -ely
```

#### Print et prosess-tre:

```
ps -ejH
ps axjf
```

#### List info om tråder:

```
ps -eLf
ps axms
```

#### List sikkerhetsrelatert info:

```
ps -eo euser,ruser,suser,fuser,f,comm,label
ps axZ
ps -eM
```

#### List alle prosesser som kjøres som root:

```
ps -U root -u root u
```

#### List alle prosesser i et brukerdefinert format:

```
ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm
ps axo stat,euid,ruid,tt,tpgid,sess,pgrp,ppid,pid,pcpu,comm
ps -Ao pid,tt,user,fname,tmout,f,wchan
```

#### Print bare prosess-IDen til syslogd:

```
ps -C syslogd -o pid=
```

**Forskjell i output mellom ps -ef og ps -aux****\$ ps -ef | grep postgres**

```

terje      337012  336411  0 17:35 pts/0    00:00:00 grep --color=auto
postgres
postgres 2698198          1  0 Nov12 ?           00:02:40
/usr/pgsql-13/bin/postmaster -D /var/lib/pgsql/13/data/
postgres 2698199 2698198  0 Nov12 ?           00:00:01 postgres: logger
postgres 2698201 2698198  0 Nov12 ?           00:00:00 postgres: checkpointer
postgres 2698202 2698198  0 Nov12 ?           00:00:03 postgres: background
writer
postgres 2698203 2698198  0 Nov12 ?           00:00:03 postgres: walwriter
postgres 2698204 2698198  0 Nov12 ?           00:01:53 postgres: autovacuum
launcher
postgres 2698205 2698198  0 Nov12 ?           00:05:17 postgres: stats
collector
postgres 2698206 2698198  0 Nov12 ?           00:00:00 postgres: logical
replication launcher
postgres 4087483 2698198  0 Nov22 ?           00:00:00 postgres: kurs3
postgres 136.243.23.69(60562) idle
postgres 4087489 2698198  0 Nov22 ?           00:00:00 postgres: kurs3 hr
136.243.23.69(60566) idle

```

**\$ ps -aux | grep postgres**

```

terje      337023  0.0  0.0 12108 1088 pts/0    S+   17:35   0:00 grep --
color=auto postgres
postgres 2698198  0.0  0.0 287064 22240 ?      Ss   Nov12    2:40
/usr/pgsql-13/bin/postmaster -D /var/lib/pgsql/13/data/
postgres 2698199  0.0  0.0 139308  3376 ?      Ss   Nov12    0:01
postgres: logger
postgres 2698201  0.0  0.0 287180  9716 ?      Ss   Nov12    0:00
postgres: checkpointer
postgres 2698202  0.0  0.0 287064  7104 ?      Ss   Nov12    0:03
postgres: background writer
postgres 2698203  0.0  0.0 287064  8436 ?      Ss   Nov12    0:03
postgres: walwriter
postgres 2698204  0.0  0.0 288024  6716 ?      Ss   Nov12    1:53
postgres: autovacuum launcher
postgres 2698205  0.0  0.0 143556  5504 ?      Ss   Nov12    5:17
postgres: stats collector
postgres 2698206  0.0  0.0 287500  6684 ?      Ss   Nov12    0:00
postgres: logical replication launcher
postgres 4087483  0.0  0.0 298620 26568 ?      Ss   Nov22    0:00
postgres: kurs3 postgres 136.243.23.69(60562) idle

```

```
postgres 4087489  0.0  0.1 301556 33448 ?          Ss   Nov22   0:00
postgres: kurs3 hr 136.243.23.69(60566) idle
```

## ➔ Vis kjørende prosesser i en trestruktur med **pstree**

**pstree** viser kjørende prosesser som et tre. Hvis ikke en **pid** er spesifisert, regnes treets rot som **init**. Hvis et brukernavn er spesifisert vises alle prosesser som eies av brukeren.

### Eksempler:

Vis terjes prosesser, sammenslått

```
$ pstree terje
bash—pstree
tmux: server—2*[bash]
```

Vis terjes prosesser fullt ut

```
$ pstree -c terje
bash—pstree
tmux: server—┬─bash
               └─bash
```

### OPTIONS

-a Show command line arguments. If the command line of a process is swapped out, that process is shown in parentheses. -a implicitly disables compaction for processes but not threads.

-A Use ASCII characters to draw the tree.

-c Disable compaction of identical subtrees. By default, subtrees are compacted whenever possible.

-G Use VT100 line drawing characters.

-h Highlight the current process and its ancestors. This is a no-op if the terminal doesn't support highlighting or if neither the current process nor any of its ancestors are in the subtree being shown.

-H Like -h, but highlight the specified process instead. Unlike with -h, pstree fails when using -H if highlighting is not



available.

-g Show PGIDs. Process Group IDs are shown as decimal numbers in parentheses after each process name. -g implicitly disables compaction. If both PIDs and PGIDs are displayed then PIDs are shown first.

-l Display long lines. By default, lines are truncated to either the COLUMNS environment variable or the display width. If neither of these methods work, the default of 132 columns is used.

-n Sort processes with the same ancestor by PID instead of by name. (Numeric sort.)

-N Show individual trees for each namespace of the type specified. The available types are: ipc, mnt, net, pid, user, uts.

Regular users don't have access to other users' processes information, so the output will be limited.

-p Show PIDs. PIDs are shown as decimal numbers in parentheses after each process name. -p implicitly disables compaction.

-s Show parent processes of the specified process.

-S Show namespaces transitions. Like -N, the output is limited when running as a regular user.

-t Show full names for threads when available.

-T Hide threads and only show processes.

-u Show uid transitions. Whenever the uid of a process differs from the uid of its parent, the new uid is shown in parentheses after the process name.

-U Use UTF-8 (Unicode) line drawing characters. Under Linux 1.1-54 and above, UTF-8 mode is entered on the console with echo -e ' 33%8' and left with echo -e ' 33%@'

-V Display version information.

-Z (SELinux) Show security context for each process. This flag will only work if pstree is compiled with SELinux support.

## ➔ systemctl - starte, stoppe og re-starte tjenester

**systemctl** (System Control) er et relativt nytt verktøy (implementert rundt 2016) for å kontrollere tjenester som kjører på en Linux-maskin. Syntaksen er enkel:

```
$ sudo systemctl [OPTION] [SERVICE]
```

**OPTION** kan være en av

1. start - starter en tjeneste
2. stop - stopper en tjeneste
3. restart - restarter en tjeneste
4. reload - laster inn konfigurasjoner osv på nytt uten å restarte tjenesten
5. reload-or-restart - restarter dersom det ikke er mulig med en reload.
6. enable - gjør at tjenesten restarteres også ved restart av maskinen
7. disable - gjør at tjenesten ikke restarteres ved restart av maskinen
8. status - viser om tjenesten kjører eller ikke, og om den er enabled eller disabled
9. is-active - returnerer **active** hvis en tjeneste kjører
10. is-enabled - returnerer **enabled** hvis en tjeneste er enabled.
11. list-units --type=service - lister opp alle tjenester på maskinen, og om de kjører eller ikke
12. list-unit-files --state=enabled - lister opp alle tjenester som er enabled
13. list-unit-files --state=disabled - lister opp alle tjenester som er disabled

### Eksempler

```
$ sudo systemctl restart httpd
```

Restarter Apache webserver på en RedHat-basert server

```
$ sudo systemctl start mariadb
```

Starter mariadb-serveren

```
$ sudo systemctl enable mariadb
```

Setter mariadb-serveren til *enabled*, slik at den vil kunne starte automatisk ved restart av maskinen

```
$ sudo systemctl reload postfix
```

Reloader konfigurasjonen til postfix mailserver

## ➔ Cron og Crontab

**Cron** er et program som utfører oppgaver til oppsatte tider etter en plan som settes opp i tabellen **crontab**. Hver bruker kan lage sin personlige crontab, og systemet setter også gjerne opp en crontab som kjører system-oppgaver som rot-bruker.

### Kommandoer for å sette opp crontab

---

#### **\$ crontab -l**

- lister opp oppføringene i evt. eksisterende crontab-filer.

#### **\$ crontab -e**

- åpner brukerens crontab for redigering (med valg av editor), eller oppretter en ny crontab hvis det ikke finnes noen og åpner denne for redigering

#### **\$ crontab -su chris**

- åpner en annen bruker (chris) sin crontab for redigering. Du må ha rot-rettigheter for å gjøre dette

#### **\$ crontab -r**

- sletter din personlige crontab-fil

### Formatet til crontab-filen

---

Crontab-filen er formattert med følgende kolonneoverskrifter:

#### **m h dom mon dow command**

m = minutt (0-60)

h = time (1-24)

dom = dag i måneden (1-31)

mon = måned (1-12)

dow = ukedag (1-7)

command = kommando eller skript som skal kjøres på denne tiden

### Eksempler på crontab-oppføringer

---

#### **0 5 \* \* 2 tar -zcf /var/backups/home.tgz /home/**

- Kommandoen lager et gzippet tar-arkiv av alle filene i /home/-mappen og lagrer arkivet i /var/backups/home.tgz

- Kommandoen kjøres 0 minutter over 5 om morgenen, en gang i uken (hver tirsdag, etter norsk

tidsregning, hvor uken starter på mandag) - uansett hvilken dag i måneden eller hvilken måned det er (\* \*).

**15 8 1 1,4,7,10 \* mail manager@server.com < /var/salg/kvartalsrapport.txt**

- Kommandoen sender innholdet i filen kvartalsrapport.txt som epost til manager@server.com
- Kommandoen kjøres 15 minutter over 8 om morgenen den første dagen i månedene januar, april, juli og oktober (1,4,7,10) uansett hvilken ukedag dette er.

## En annen måte å gjøre det på

---

Det finnes en annen måte å organisere cron-kjøringer på ved at man lager et skript med kommandoene som skal kjøres og lagrer skriptet i en av disse mappene:

**/etc/cron.hourly**  
**/etc/cron.daily**  
**/etc/cron.weekly**  
**/etc/cron.monthly**

Skriptet blir så kjørt hver time, daglig, ukentlig, eller månedlig.

# Kapittel 8

## Systemovervåking og loggsjekking

### ➔ df - sjekk tilgjengelig diskplass

**df** er kommandoen for å vise hvor mye plass det er på hver partisjon av mountede harddisker.

**Eksempel:**

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        16G   0    16G   0% /dev
tmpfs           16G  16K   16G   1% /dev/shm
tmpfs           16G  700K   16G   1% /run
tmpfs           16G   0    16G   0% /sys/fs/cgroup
/dev/md2        1.8T 604G  1.1T  36% /
/dev/md1        487M 298M  164M  65% /boot
tmpfs           3.2G   0   3.2G   0% /run/user/54321
tmpfs           3.2G   0   3.2G   0% /run/user/0

$ df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  16G   0    16G   0% /dev
tmpfs           tmpfs     16G  16K   16G   1% /dev/shm
tmpfs           tmpfs     16G 692K   16G   1% /run
tmpfs           tmpfs     16G   0    16G   0% /sys/fs/cgroup
/dev/md2        ext4      1.8T 604G  1.1T  36% /
/dev/md1        ext3      487M 298M  164M  65% /boot
tmpfs           tmpfs     3.2G   0   3.2G   0% /run/user/54321
tmpfs           tmpfs     3.2G   0   3.2G   0% /run/user/0
```

Flagget **-h** angir at tallene skal vises i "human readable format", dvs i M, G og T istedenfor i bytes. Flagget **-T** angir at typen filsystem også skal vises.

## ➔ free - sjekk tilgjengelig og brukt minne

**free** er kommandoen for å sjekke minnebruken på en Linux-maskin.

### Eksempel:

```
$ free -ht
              total        used        free      shared  buff/cache
available
Mem:          31Gi        7.9Gi        3.2Gi        1.2Gi        20Gi
21Gi
Swap:         15Gi        1.5Gi         14Gi
Total:         47Gi        9.4Gi        17Gi
```

**MERK:** **available** angir ledig minne til å starte nye applikasjoner uten swapping

Flagget **-h** angir "human readable format".

Flagget **-t** angir at det skal legges til en linje med total-summer

## ➔ htop - top med mer grafisk oversikt

htop kan være mer oversiktlig enn top hvis du vil få et raskt blick på ressursbruken på en maskin, spesielt minne-bruken.

htop er som regel ikke installert "by default", men kan lett installeres slik:

```
$ sudo apt/dnf/yum/zypper install htop
```

Slik kan et skjermbilde fra htop se ut:

The screenshot shows a Linux terminal window. At the top, there's a status bar with 'Aktiviteter', 'Programmer', and 'Steder'. Below that, a system status line shows 'to, 3. des. 19:22' and '0,6 °C'. A progress bar for memory usage is shown, followed by system statistics: 'Tasks: 172, 757 thr; 1 running', 'Load average: 0.75 0.69 0.64', and 'Uptime: 49 days, 09:43:20'. The main part of the terminal displays a table of running processes with columns: PID, USER, PRI, NI, VIRT, RES, SHR, S, CPU%, MEM%, TIME+, and Command. The table lists various system services and user processes, including httpd, XE, mongod, mssql, and jenkins. At the bottom, there's a navigation bar with keys like F2Setup, F3Search, F4Filter, F5Tree, F6SortBy, F7Nice, F8Nice, F9Kill, and F10Quit.

## → sysctl - vis eller endre kjerne-parametere

**sysctl** (ikke å forveksle med **systemctl**) er et program som lar deg se eller endre innstillingene i Linux-kjernen. Disse opptrer som "filer" i mappen **/proc/sys**, og som alternativ til **sysctl** kan man også lese eller skrive til disse "filene".

Eksempler på bruk av **sysctl**:

### 1) Vis innstillingen for **overcommit\_memory**.

```
$ sysctl vm.overcommit_memory
vm.overcommit_memory = 0
```

### 2) Endre innstillingen for **overcommit\_memory**

```
$ sudo sysctl vm.overcommit_memory=1
vm.overcommit_memory = 1
```

### 3) Vis alle innstillingene for **/proc/sys/vm**

```
$ sysctl vm.      (+ tast tab to ganger)
vm.admin_reserve_kbytes      vm.dirty_writeback_centisecs
vm.min_slab_ratio            vm.oom_dump_tasks
vm.stat_refresh
vm.block_dump                vm.extfrag_threshold
vm.min_unmapped_ratio        vm.oom_kill_allocating_task
vm.swappiness
vm.compaction_proactiveness  vm.hugetlb_shm_group
vm.mmap_min_addr             vm.overcommit_kbytes
vm.unprivileged_userfaultfd
vm.compact_unevictable_allowed vm.laptop_mode
vm.mmap_rnd_bits             vm.overcommit_memory
vm.user_reserve_kbytes
vm.dirty_background_bytes    vm.legacy_va_layout
vm.mmap_rnd_compat_bits      vm.overcommit_ratio
vm.vfs_cache_pressure
vm.dirty_background_ratio    vm.lowmem_reserve_ratio
vm.nr_hugepages              vm.page-cluster
vm.watermark_boost_factor
vm.dirty_bytes               vm.max_map_count
vm.nr_hugepages_mempolicy    vm.page_lock_unfairness
vm.watermark_scale_factor
vm.dirty_expire_centisecs    vm.memory_failure_early_kill
vm.nr_overcommit_hugepages   vm.panic_on_oom
vm.zone_reclaim_mode
vm.dirty_ratio               vm.memory_failure_recovery
vm.numa_stat                 vm.percpu_pagelist_fraction
vm.dirtytime_expire_seconds  vm.min_free_kbytes
vm.numa_zonelist_order       vm.stat_interval
```

## ➔ Nettverksovervåking med tcpdump

tcpdump skriver ut en beskrivelse av innholdet av pakker som sendes inn og ut over et angitt nettverkskort. Hvis ikke annet er angitt, skrives dette ut til stdout, dvs. terminalvinduet. Teksten kan f.eks. "pipes" til grep for å sile ut informasjon man er interessert i, og resultatet kan lagres i en fil. Feks. slik:

```
$ sudo tcpdump -i wlan0 | grep minmaskin >> tcp_logg.txt
```

## ➔ Nettverksovervåking med iptraf

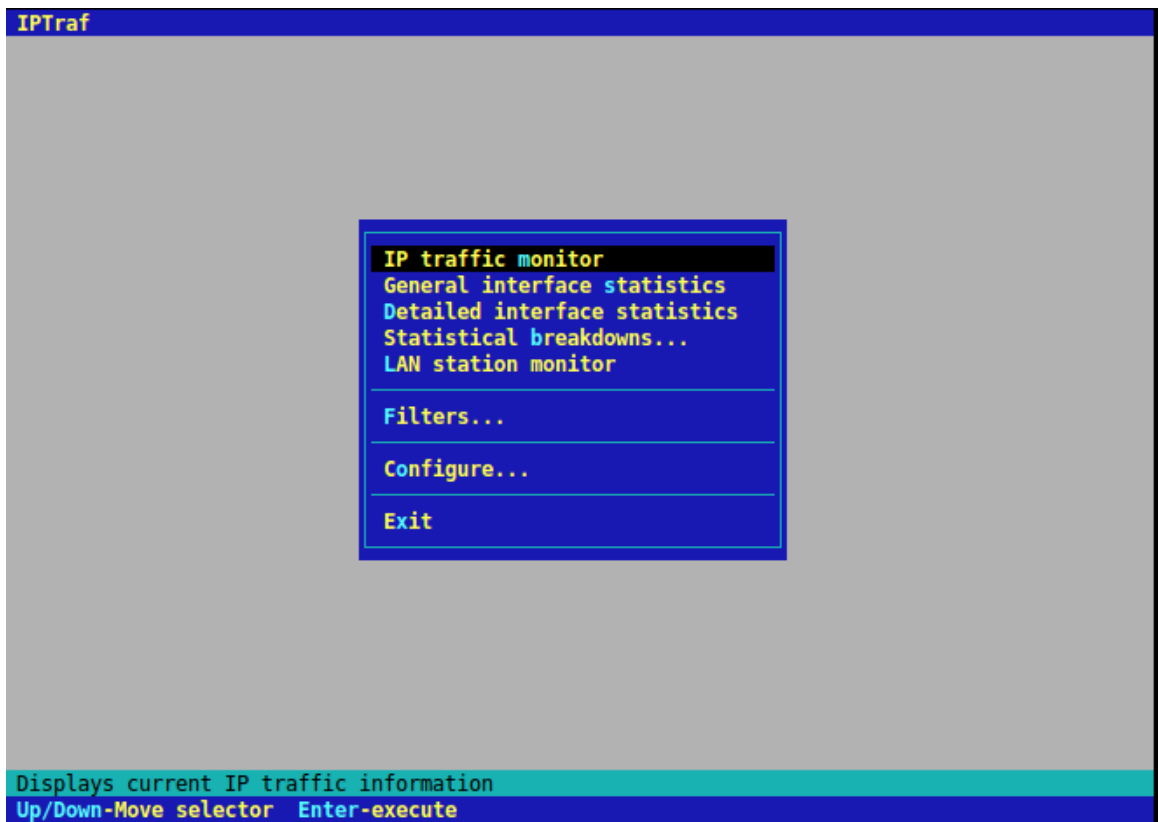
iptraf er et kraftig verktøy med et enkelt TUI-grensesnitt. Programmet installeres enkelt med kommandoen:



```
$ sudo apt-get install iptraf
```

Start programmet med kommandoen:

```
$ sudo iptraf
```



Taster du <enter>, kan du velge hvilket nettverkskort som skal overvåkes. Selve overvåkningsbildet ser slik ut:

```

IPTraf
TCP Connections (Source Host:Port) ----- Packets ----- Bytes ----- Flags ----- Iface -----
[terjeubuntu.lan:57986] = 115 11826 --A- wlan0
[axenna.com:80] = 258 368907 -PA- wlan0
[terjeubuntu.lan:57987] = 39 11691 --A- wlan0
[axenna.com:80] = 53 60581 -PA- wlan0
[terjeubuntu.lan:57988] = 73 14458 --A- wlan0
[axenna.com:80] = 153 206311 -PA- wlan0
[terjeubuntu.lan:57993] = 23 4862 --A- wlan0
[axenna.com:80] = 23 24365 -PA- wlan0
[terjeubuntu.lan:57990] = 111 14080 --A- wlan0
[axenna.com:80] = 270 380633 -PA- wlan0
[terjeubuntu.lan:57992] = 107 7777 --A- wlan0
[axenna.com:80] = 212 311232 -PA- wlan0
[axenna.com:80] > 1 52 --A- wlan0
[terjeubuntu.lan:57989] = 0 0 ---- wlan0

TCP: 7 entries ----- Active -----

UDP (68 bytes) from 10.0.0.138:53 to terjeubuntu.lan:32339 on wlan0
UDP (74 bytes) from terjeubuntu.lan:63175 to 10.0.0.138:53 on wlan0
UDP (69 bytes) from terjeubuntu.lan:49576 to 10.0.0.138:53 on wlan0
UDP (74 bytes) from 10.0.0.138:53 to terjeubuntu.lan:63175 on wlan0
UDP (69 bytes) from 10.0.0.138:53 to terjeubuntu.lan:49576 on wlan0
UDP (100 bytes) from terjeubuntu.lan:5353 to 224.0.0.251:5353 on wlan0
UDP (131 bytes) from 10.0.0.78:5353 to 224.0.0.251:5353 on wlan0
UDP (91 bytes) from terjeubuntu.lan:5353 to 224.0.0.251:5353 on wlan0

Bottom ----- Elapsed time: 0:00 -----
Pkts captured (all interfaces): 1693 | TCP flow rate: 18.80 kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg activ win S-sort TCP X-exit

```

Brukerhåndboken til iptraf finner du her: <http://iptraf.seul.org/2.7/manual.html>

## ➔ Sjekking av minnebruk og swapping med vmstat

Dersom systemet går tregt, så kan det skyldes flere ting, men du vil trolig sjekke med kommandoen `vmstat` for å se om det er mye "swapping", altså om det fysiske minnet stort sett er fullt, slik at systemet må bruke virtuelt minne på disken.

Swapping til disk er som kjent ikke veldig raskt. Dersom du med `vmstat` ser at det ofte er mye swapping, og du har sjekka at det ikke er store minnelekkasjer som går igjen hele tiden, så bør du definitivt kjøpe mer minne.

For å sjekke minnebruken med 2 sekunders mellomrum og skrive resultatet til skjermen:

```
$ sudo vmstat 2
```

Resultatet skrives i en tabell:

procs		-----memory-----				---swap--		-----io----		-system--		----cpu----			
r	b	swpd	free	buff	cache	si	so	bi	bo	in	cs	us	sy	id	wa
4	0	16512	179720	38996	448072	0	1	96	70	564	1499	20	4	75	2
0	0	16512	179712	39004	448064	0	0	0	6	360	953	6	2	91	2
0	0	16512	179712	39012	448072	0	0	0	6	356	931	6	2	91	2
1	0	16512	179712	39020	448072	0	0	0	20	377	970	5	3	91	2
0	0	16512	179720	39020	448072	0	0	0	0	385	1062	13	2	85	0
0	0	16512	179720	39020	448072	0	0	0	0	368	985	7	2	92	0
0	0	16512	179720	39036	448072	0	0	0	28	382	942	6	3	89	3
0	0	16512	179588	39036	448072	0	0	0	2	375	988	10	3	88	0

## ➔ Overvåking av ressursbruken med top

Top er et mye brukt og ekstremt nyttig program hvis du vil vite hva som spiser mest minne eller cpu-kapasitet på en maskin. Top kan endre oppførsel etter ønske, og det lønner seg å sjekke manualen for alle mulighetene med: **\$ man top**

```
$ top
```

Resultatet listes i en tabell, slik:

```
%Cpu(s):  7,6 us,  3,3 sy,  0,0 ni, 86,8 id,  2,3 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem:  1800880 total, 1649316 used,  151564 free,  16900 buffers
KiB Swap: 1535996 total,  67936 used, 1468060 free,  336804 cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3249	terjebh	20	0	297m	66m	25m	S	4,6	3,8	14:47.91	chromium-browse
1216	root	20	0	132m	81m	8372	S	1,3	4,6	8:47.80	Xorg
2967	terjebh	20	0	89496	28m	15m	S	0,7	1,6	0:10.06	python
1197	mongodb	20	0	90608	1852	1620	S	0,3	0,1	1:28.02	mongod
1342	postgres	20	0	52256	1676	988	S	0,3	0,1	0:00.58	postgres
2950	terjebh	20	0	97,8m	15m	10m	S	0,3	0,9	0:14.66	yakuake
4229	terjebh	20	0	176m	43m	18m	S	0,3	2,5	0:31.38	chromium-browse
7199	terjebh	20	0	752m	122m	49m	S	0,3	7,0	0:46.08	soffice.bin
8168	terjebh	20	0	6524	1400	996	R	0,3	0,1	0:00.05	top
1	root	20	0	3724	1848	1208	S	0,0	0,1	0:00.92	init
2	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:12.42	ksoftirqd/0
6	root	rt	0	0	0	0	S	0,0	0,0	0:00.00	migration/0
7	root	rt	0	0	0	0	S	0,0	0,0	0:00.10	watchdog/0
8	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	cpuset
9	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	khelper
10	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kdevtmpfs
11	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	netns
12	root	20	0	0	0	0	S	0,0	0,0	0:00.04	sync supers
13	root	20	0	0	0	0	S	0,0	0,0	0:00.00	bdi-default
14	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kintegrityd
15	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kblockd
16	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	ata_sff
17	root	20	0	0	0	0	S	0,0	0,0	0:00.09	khubd
18	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	md
21	root	20	0	0	0	0	S	0,0	0,0	0:00.00	khungtaskd
22	root	20	0	0	0	0	S	0,0	0,0	0:00.72	kswapd0

## ➔ Sjekk MySQL-belastningen med mytop

**mytop** kan installeres med denne kommandoen:

```
$ sudo apt-get install mytop
```

Du logger deg så på en MySQL (evt. MariaDB)-server med denne kommandoen:

```
$ mytop <databasenavn> -h <servernavn> -u <brukernavn> --prompt
```

Det siste flagget (--prompt) prompter deg for et passord, men passordet kan også settes inn i filen ~/.mytop eller skrives inn på kommandolinjen med flagget -p<passord> (anbefales ikke).

```

File Edit View Search Terminal Tabs Help
MySQL on localhost (5.1.61)
Queries: 11.0 qps: 0 Slow: 0.0 Se/In/Up/De(%): 00/00/00/00 up 0+00:21:23 [23:08:32]
qps now: 0 Slow qps: 0.0 Threads: 3 ( 1/ 0) 00/00/00/00
Key Efficiency: 100.0% Bps in/out: 0.2/ 30.3 Now in/out: 8.4/ 1.5k

  Id  User      Host/IP      DB      Time  Cmd Query or State
  --  -
  9   root      localhost    test     0   Query show full processlist
  3   icinga    localhost    icinga   4   Sleep
  4   icinga    localhost    icinga  976   Sleep

```

Sjekk manualen til mytop (\$ man mytop) for beskrivelse av output og kommandoer tilgjengelige i mytop

## ➔ Sjekk Apache2-belastningen med **apachetop**

**apachetop** kan installeres med kommandoen:

```
$ sudo apt-get install apachetop
```

I motsetning til **mytop** (se ovenfor) kjøres apachetop fra serveren hvor Apache2 kjører, så du må logge deg inn med f.eks. ssh først. Du kan spesifisere hvilken logfil apachetop skal kjøres mot med denne kommandoen:

```
$ apachetop -f /var/log/apache2/access.log
```

```

last hit: 16:32:10      atop runtime: 0 days, 00:01:11      16
All:      10 reqs (    0.5/sec)      839.8K (   38.2K/sec)      84.
2xx:      8 (80.0%) 3xx:      1 (10.0%) 4xx:      1 (10.0%) 5xx:      0 (
R ( 60s):  10 reqs (    0.2/sec)      839.8K (   14.0K/sec)      84.
2xx:      8 (80.0%) 3xx:      1 (10.0%) 4xx:      1 (10.0%) 5xx:      0 (
0.0%)
REQS REQ/S    KB KB/S URL
  1  0.05    0.4  0.0 */kurs/course/modedit.php
  1  0.05   78.7  3.7 /kurs/mod/page/view.php
  1  0.05    0.0  0.0 /kurs/theme/image.php/elegance/theme/1407965264/
  1  0.05   16.3  0.8 /kurs/pluginfile.php/1266/mod_page/content/15/ip
  1  0.05   99.4  5.0 /kurs/pluginfile.php/1266/mod_page/content/15/vm
  1  0.05   53.0  2.7 /kurs/pluginfile.php/1266/mod_page/content/15/ip
  1  0.05   44.8  2.2 /kurs/pluginfile.php/1266/mod_page/content/15/my
  1  0.05   21.2  1.1 /kurs/pluginfile.php/1266/mod_page/content/15/nm
  1  0.05  292.2 15.4 /kurs/pluginfile.php/1266/mod_page/content/15/to
  1  0.05  233.7 12.3 /kurs/pluginfile.php/1266/mod_page/content/15/ps

```

## ➔ Kommandoer for å håndtere kjerne-moduler.

**lsmod** viser lastede moduler

**insmod** laster inn moduler

**rmmod** fjerner (unloads) kjernemoduler

**modprobe** Mer intelligent/høytnivå program for bl.a. å laste og fjerne moduler

**depmod** Håndterer avhengigheter, sjekker hvilke moduler som er tilgjengelige m.m.

**ksyms** Viser eksporterte kjernesymboler (kernel symbols)

## ➔ uptime - vis oppetid og belastning

**uptime** er en enkel kommando som viser hvor lenge maskinen har vært oppe, samt belastningen på maskinens cpu.

### Parametere:

**-p** (pretty) formateret output enklere (men fjerner informasjon om belastning)

### Eksempler:

```
$ uptime
20:00:47 up 55 days, 10:21,  2 users,  load average: 0.18, 0.17, 0.36

$ uptime -p
up 7 weeks, 6 days, 10 hours, 22 minutes

$ ssh server4 uptime
20:03:40 up 55 days, 10:24,  1 user,  load average: 0.18, 0.20, 0.34
```

## ➔ lastlog - vis brukeres siste login

**lastlog** er et nyttig program som viser siste login for alle eller valgte brukere.

### Parametere:

The options which apply to the lastlog command are:

-b, --before DAYS

Print only lastlog records older than DAYS.

-C, --clear

Clear lastlog record of a user. This option can be used only together with -u (--user)).

-h, --help

Display help message and exit.

-R, --root CHROOT\_DIR

Apply changes in the CHROOT\_DIR directory and use the configuration files from the CHROOT\_DIR directory.

-S, --set

Set lastlog record of a user to the current time. This option can be used only together with -u (--user)).

-t, --time DAYS

Print the lastlog records more recent than DAYS.

-u, --user LOGIN|RANGE

Print the lastlog record of the specified user(s).

The users can be specified by a login name, a numerical user ID, or a RANGE of users. This RANGE of users can be

specified with a min and max values (UID\_MIN-UID\_MAX), a max value (-UID\_MAX), or a min value (UID\_MIN-).

### Eksempler:

```
$ lastlog -u terje
```

```

Username      Port      From      Latest
terje         pts/1
$ lastlog -t 1
Username      Port      From      Latest
root          pts/1      85.165.21.92   Wed Dec  9 19:08:14 +0100 2020
terje         pts/1      Wed Dec  9 19:33:53 +0100 2020
kurs2         pts/1      85.165.21.92   Wed Dec  9 09:32:00 +0100 2020
kurs4         pts/0      88.90.185.214   Wed Dec  9 10:18:40 +0100 2020
kurs5         pts/0      85.165.21.92   Wed Dec  9 10:16:41 +0100 2020
kurs6         pts/5      89.162.66.100   Wed Dec  9 10:25:53 +0100 2020
kurs7         pts/1      158.36.232.247   Wed Dec  9 10:18:47 +0100 2020
kurs8         pts/2      85.167.72.45    Wed Dec  9 10:20:36 +0100 2020
kurs9         pts/3      84.212.12.153   Wed Dec  9 10:19:15 +0100 2020
kurs10        pts/0      Tue Dec  8 22:47:23 +0100 2020
kurs15        pts/0      Tue Dec  8 22:47:07 +0100 2020

```

## ➔ Oversikt over Linux loggsystem

De fleste Linux-tjenester er satt opp til å logge aktivitetene fortløpende, og disse loggene lagres i mappen:

```
/var/log
```

Ubuntu og flere andre distroer bruker **syslogd** (system log daemon) og **klogd** (kernel log daemon) til å administrere system-logging. Disse startes automatisk fra syslog init-skriptet. (*/etc/init.d/sysklogd*). Informasjon fra disse systemene lagres i filer i */var/log*-mappen - slik som *messages*, *secure*, *cron* og *boot.log*.

Automatisk log-rotering håndteres av **logrotate**, basert på innstillingene i */etc/logrotate.conf*-filen og */etc/logrotate.d* -mappen. Cron-jobben */etc/cron.daily/logrotate* gjør jobben med å rotere loggene daglig.

Her er noen vanlige logg-filer slik de lagres i en Ubuntu-server:

=> **/var/log/faillog** : Feilede brukerlogin

=> **/var/log/kern.log** : Kjernens loggfil

=> **/var/log/lpr.log** : Printer loggfil

=> **/var/log/mail.\*** : Alle loggfilene fra mail-serveren

=> **/var/log/mysql.\*** : MySQL server loggfil

=> **/var/log/user.log** : Logger for alle userlevel



=> **/var/log/xorg.0.log** : X.org loggfil

=> **/var/log/apache2/\*** : Loggfiler for Apache web server

=> **/var/log/lighttpd/\*** : Loggfiler for Lighttpd web server

=> **/var/log/fsck/\*** : fsck command logger

=> **/var/log/apport.log** : Application crash report / loggfil

## ➔ Sjekking av loggfiler

Loggfiler kan undersøkes manuelt (med f.eks. **less**), og man kan søke ut interessante hendelser med **grep**.

Kommandoen **\$ dmesg** - skriver meldingene fra oppstartsloggen til skjermen

*Eks:*

```
$ dmesg | tail 30 > bootmesg.txt
```

(skriver de siste 30 meldingene til filen bootmesg.txt)

Pakken **logwatch** gjør jobben enklere ved at den kan hente utdrag av mange loggfiler samtidig og f.eks. sende dem som epost med jevne mellomrom til sysadmin. Både avsender og mottaker av denne mailen kan endres ved å redigere */etc/cron.daily/0logwatch* -filen. Du kan også logge inn som root og lese mailene lokalt på serveren (se egen artikkel om logwatch).

## ➔ Skrive til loggfiler

Du kan sende dine egne beskjeder til loggfiler som styres av *syslogd* ved å bruke **logger**-kommandoen, f.eks. slik:

```
$ logger La til nytt nettverkskort
```

(skriver beskjeden *La til nytt nettverkskort* til *syslog*-filen)

```
$ logger -p info -t CARD -f /tmp/min_tekstfil.txt
```

(setter prioriteten i beskjeden til *info* og legger til en *tag (CARD)* til hver linje i beskjeden som hentes fra filen */tmp/min\_tekstfil.txt* - resultatet lagres i *syslog*-filen)

## ➔ journalctl

**journalctl** er som navnet antyder et kontrollprogram for journaler, eller logger.

De fleste moderne Linux-distroer bruker nå **systemd** til å håndtere logger. Det inkluderer **journald**, en daemon som samler logger fra ulike systemer, slik som **syslog** gjorde tidligere, for distroer som brukte **SysVinit** istedet for **systemd**. **syslog** var rene tekstfiler, som man måtte søke i, mens med **journald** kan vi bruke programme **journalctl** til å vise oss innholdet loggene, som nå lagres i binærformat.

Med **journalctl**, kan vi *lese* logger, *monitorere* logger i sanntid og *filtrere* logger basert på tid, tjeneste, alvorlighetsgrad og andre parametere.

**Journalctl** bruker **less** til å vise loggene, så vi kan bevege oss rundt med samme kommandoer som med **less**.

#### Eksempel:

```
$ journalctl -r
```

(Viser de siste logglinjene først)

## ➔ Få en samlet logg-oversikt med logwatch

### Installasjon

**Logwatch** installeres med en av disse kommandoene:

**\$ sudo apt install logwatch** (**sudo apt-get install logwatch** for eldre debianbaserte systemer)

**\$ sudo yum install logwatch** (for eldre RedHat-baserte systemer)

**\$ sudo dnf install logwatch** (for nyere RedHat-baserte systemer - f.o.m RHEL/CENTOS 8.0)

**\$ sudo zypper install logwatch** (for SuSE-baserte systemer)

### Bruk fra kommandolinjen

```
$ sudo logwatch
```

- sender output til skjermen.

```
$ sudo logwatch > loggger.txt
```

- lagrer output i en fil

```
$ sudo logwatch --mailto bruker@server.com
```

- sender output via epost til [bruker@server.com](mailto:bruker@server.com)

```
$ sudo logwatch --service pam_pwdb --range yesterday --detail high --  
output=stdout
```

- sender login-informasjon fra igår til skjermen

## Konfigurering

---

En god idé kan være å kopiere en standard konfig-fil til /etc/logwatch/conf/ - mappen, slik:

```
# cp /usr/share/logwatch/default.conf/logwatch.conf  
/etc/logwatch/conf/logwatch.conf
```

I denne filen kan du for eksempel endre disse to parameterene slik:

**Output = mail**

**MailTo = epost@dittdomene**

Så vil logwatch sende en mail hver gang den kjøres. Det ligger et oppsett for kjøring i mappen

```
/etc/cron.daily
```

## Dokumentasjon

---

```
$ man logwatch  
  
$ info logwatch
```

gir oversikt over parametre og eksempler på bruk

# Kapittel 9

## Nettverk

### ➔ ip - vis og endre routing, network devices, interfaces og tunnels

**ip** er en nyttig og kraftig kommando som både kan gi informasjon om og endre innstillinger for nettverksrelaterte funksjoner.

#### Eksempler

Her er noen eksempler på bruk av **ip**:

#### 1) Vis informasjon om konfigurasjonen for maskinens nettverkskort

```
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 44:8a:5b:d4:49:73 brd ff:ff:ff:ff:ff:ff
    inet 136.243.23.69/32 scope global noprefixroute enp2s0
        valid_lft forever preferred_lft forever
    inet6 2a01:4f8:211:1444::2/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::468a:5bff:fed4:4973/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

**ip a** - viser her for eksempel at nettverkskortet **enp2s0** er knyttet til ip-adressen 136.243.23.69

#### 2) Vis kun ip 4 adresser:

```
$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    inet 136.243.23.69/32 scope global noprefixroute enp2s0
        valid_lft forever preferred_lft forever
```

### 3) Legg en IP-adresse til et nettverkskort

```
$ sudo ip addr add 192.168.4.44/24 dev enp0s3
```

### 4) Fjern en IP-adresse fra et nettverkskort

```
$ sudo ip addr del 192.168.4.44/24 dev enp0s3
```

### 5) Ta ned eller opp et nettverkskort

```
$ sudo ip link set enp0s3 down
$ sudo ip link set enp0s3 up
```

### 6) Vis ruting

```
$ ip route ( eller bare ip r)
default via 136.243.23.65 dev enp2s0 proto static metric 100
136.243.23.65 dev enp2s0 proto static scope link metric 10
```

Her er de ulike objektene **ip** kan operere på:

```
link | address | addrlabel | route | rule | neigh | ntable
| tunnel | tuntap |
    maddress | mroute | mrule | monitor | xfrm | netns | l2tp |
tcp_metrics | token |
    macsec | vrf | mptcp
```

Og her er en oversikt over parameterene

```

-V, -Version
    Print the version of the ip utility and exit.
-h, -human, -human-readable
    output statistics with human readable values followed by
suffix.
-b, -batch <FILENAME>
    Read commands from provided file or standard input and
invoke them. First failure
    will cause termination of ip.
-force Don't terminate ip on errors in batch mode. If there were
any errors during execu-
    tion of the commands, the application return code will be
non zero.
-s, -stats, -statistics
    Output more information. If the option appears twice or
more, the amount of informa-
    tion increases. As a rule, the information is statistics or
some time values.
-d, -details
    Output more detailed information.
-l, -loops <COUNT>
    Specify maximum number of loops the 'ip address flush' logic
will attempt before giv-
    ing up. The default is 10. Zero (0) means loop until all
addresses are removed.
-f, -family <FAMILY>
    Specifies the protocol family to use. The protocol family
identifier can be one of
    inet, inet6, bridge, mpls or link. If this option is not
present, the protocol fam-
    ily is guessed from other arguments. If the rest of the
command line does not give
    enough information to guess the family, ip falls back to the
default one, usually
    inet or any. link is a special family identifier meaning
that no networking protocol
    is involved.
-4    shortcut for -family inet.
-6    shortcut for -family inet6.
-B    shortcut for -family bridge.
-M    shortcut for -family mpls.
-o, -oneline
    output each record on a single line, replacing line feeds
with the '\n' character.
    This is convenient when you want to count records with wc(1)
or to grep(1) the out-

```

```

        put.
    -r, -resolve
        use the system's name resolver to print DNS names instead of
host addresses.
    -n, -netns <NETNS>
        switches ip to the specified network namespace NETNS.
Actually it just simplifies
        executing of:
        ip netns exec NETNS ip [ OPTIONS ] OBJECT { COMMAND | help }
        to
        ip -n[etns] NETNS [ OPTIONS ] OBJECT { COMMAND | help }
    -N, -Numeric
        Print the number of protocol, scope, dsfield, etc directly
instead of converting it
        to human readable name.
    -a, -all
        executes specified command over all objects, it depends if
command supports this
        option.
    -c[color][={always|auto|never}
        Configure color output. If parameter is omitted or always,
color output is enabled
        regardless of stdout state. If parameter is auto, stdout is
checked to be a terminal
        before enabling color output. If parameter is never, color
output is disabled. If
        specified multiple times, the last one takes precedence.
This flag is ignored if
        -json is also given.
        Used color palette can be influenced by COLORFGBG
environment variable (see ENVIRON-
        MENT).
    -t, -timestamp
        display current time when using monitor option.
    -ts, -tshort
        Like -timestamp, but use shorter format.
    -rc, -rcvbuf<SIZE>
        Set the netlink socket receive buffer size, defaults to 1MB.
    -iec
        print human readable rates in IEC units (e.g. 1Ki = 1024).
    -br, -brief
        Print only basic information in a tabular format for better
readability. This option
        is currently only supported by ip addr show and ip link show
commands.
    -j, -json
        Output results in JavaScript Object Notation (JSON).

```

```
-p, -pretty
    The default JSON format is compact and more efficient to
    parse but hard for most
    users to read. This flag adds indentation for readability.
```

## ➔ resolvectl - vis og endre navneservere

**resolvectl** er et program som lar deg gjøre diverse oppgaver knyttet til DNS og navneservere

**Eksempler:**

### 1) Vis navneservere for maskin tilkoblet nettverk via trådløst nettverkskort wlp3s0

```
$ resolvectl status wlp3s0
Link 4 (wlp3s0)
    Current Scopes: DNS LLMNR/IPv4 LLMNR/IPv6
DefaultRoute setting: yes
    LLMNR setting: yes
MulticastDNS setting: no
    DNSOverTLS setting: no
    DNSSEC setting: no
    DNSSEC supported: no
    Current DNS Server: 2001:4600:4:fff::253
    DNS Servers: 148.122.164.253
                  148.122.16.253
                  2001:4600:4:1fff::253
                  2001:4600:4:fff::253
    DNS Domain: ~.
```

### 2) Finn IP-adressen til domenet: itfakultet.no

```
$ resolvectl query itfakultet.no
itfakultet.no: 136.243.23.69          -- link: wlp3s0
-- Information acquired via protocol DNS in 47.3ms.
-- Data is authenticated: no
```

### 3) Finn domenenavnet til IP-adressen: 136.243.23.69

```
$ resolvectl query 136.243.23.69
136.243.23.69: server4.noderia.com    -- link: wlp3s0
```



```
-- Information acquired via protocol DNS in 108.7ms.  
-- Data is authenticated: no
```

## ➔ netplan - vis og konfigurer nettverkskort

**netplan** er standard nettverks-konfigurerings-system for bl.a Ubuntu etter versjon ?

### Konfigurasjon

Konfigurasjonsfil fra en Ubuntu 20.10 - server:

**/etc/netplan/00-installer-config.yaml** (eller lignende fil i /etc/netplan-mappen)

```
# This is the network config written by 'subiquity'
```

```
network:
```

```
  ethernets:
```

```
    enp0s3:
```

```
      dhcp4: true
```

```
  version: 2
```

### Kommandoer

- **netplan generate:** Bruker **/etc/netplan** til å generere konfigurasjon.
- **netplan apply:** Bruker konfigurasjonen, og restarter tjenester hvis nødvendig.
- **netplan try:** Bruker konfigurasjonen, og venter på bruker-konfirmering - ruller tilbake hvis nettverket er ødelagt eller ingen konfigurasjon er gitt.

### Eksempler:

**Vis informasjon om nettverkskonfigurasjonen til nettverksenheten *enp0s3*:**

```
$ netplan ip leases enp0s3
```

```
# This is private data. Do not parse.
```

```
ADDRESS=10.0.0.27
```

```
NETMASK=255.255.255.0
```

```
ROUTER=10.0.0.138
```

```
SERVER_ADDRESS=10.0.0.138
```

```
T1=43200
```

```
T2=75600
```

```
LIFETIME=86400
```

```
DNS=148.122.164.253 148.122.16.253
```

```
NTP=193.212.1.10
CLIENTID=ffe2343f3e00020000ab119aa82fd7deffc0d0
```

## ➔ traceroute - spor rutingen til en maskin

**traceroute** er programmet vi bruker for å se hvilke nettverkskomponenter en pakke må gjennom for å nå en destinasjon.

### Parametere:

```
traceroute [-46dFITUnreAV] [-f first_ttl] [-g gate,...]
            [-i device] [-m max_ttl] [-p port] [-s src_addr]
            [-q nqueries] [-N squeries] [-t tos]
            [-l flow_label] [-w waittimes] [-z sendwait] [-UL] [-D]
            [-P proto] [--sport=port] [-M method] [-O mod_options]
            [--mtu] [--back]
            host [packet_len]
```

### Eksempler:

```
$ traceroute itfakultetet.no
```

```
traceroute to itfakultetet.no (136.243.23.69), 30 hops max, 60 byte
packets
 1 _gateway (10.0.0.138)  1.560 ms  1.744 ms  1.999 ms
 2 ti0030a400-gw.ti.telenor.net (88.91.62.1)  26.003 ms  26.538 ms
26.823 ms
 3 ti0023c400-ae7-0.ti.telenor.net (146.172.101.9)  60.247 ms  60.455 ms
60.760 ms
 4 ti0016c360-ae2-0.ti.telenor.net (146.172.20.233)  55.170 ms  55.776
ms  56.037 ms
 5 ti3003c400-ae0-0.ti.telenor.net (146.172.23.90)  56.482 ms  56.809 ms
57.088 ms
 6 ti9006b400-ae2-0.ti.telenor.net (146.172.105.81)  62.752 ms  59.449
ms  59.579 ms
 7 decix-gw.hetzner.com (80.81.192.164)  54.257 ms  52.629 ms  53.058 ms
 8 * core23.fsn1.hetzner.com (213.239.252.38)  63.483 ms *
 9 ex9k1.dc12.fsn1.hetzner.com (213.239.203.186)  58.263 ms
ex9k1.dc12.fsn1.hetzner.com (213.239.203.174)  64.322 ms
ex9k1.dc12.fsn1.hetzner.com (213.239.203.186)  58.496 ms
10 server4.noderia.com (136.243.23.69)  64.973 ms  65.225 ms  65.298 ms
```

**-I** Bruk ICMP ECHO istedenfor [UDP datagrammer](#).

```
$ traceroute -I itfakultetet.no
```

```
traceroute to itfakultetet.no (136.243.23.69), 30 hops max, 60 byte packets
 1 _gateway (10.0.0.138)  1.518 ms  1.843 ms  2.113 ms
 2 ti0030a400-gw.ti.telenor.net (88.91.62.1)  26.206 ms  26.450 ms  27.250 ms
 3 ti0030c400-ae2-0.ti.telenor.net (146.172.101.33)  65.342 ms  65.861 ms  66.174 ms
 4 ti0001c360-ae1-0.ti.telenor.net (146.172.14.129)  60.922 ms  61.960 ms  61.952 ms
 5 ti3004c400-ae38-0.ti.telenor.net (146.172.23.45)  62.020 ms  62.229 ms  62.284 ms
 6 ti9006b400-ae1-0.ti.telenor.net (146.172.105.25)  66.479 ms  62.758 ms  63.014 ms
 7 decix2-gw.hetzner.com (80.81.193.164)  64.299 ms  63.606 ms  63.801 ms
 8 core24.fsn1.hetzner.com (213.239.203.150)  63.445 ms  62.848 ms  62.759 ms
 9 ex9k1.dc12.fsn1.hetzner.com (213.239.203.186)  63.142 ms  63.810 ms  63.881 ms
10 server4.noderia.com (136.243.23.69)  68.375 ms  68.018 ms  67.931 ms
```

**-T** Bruk TCP SYN for prober

```
$ sudo traceroute -T itfakultetet.no
```

```
traceroute to itfakultetet.no (136.243.23.69), 30 hops max, 60 byte packets
 1 _gateway (10.0.0.138)  1.535 ms  1.718 ms  1.976 ms
 2 ti0030a400-gw.ti.telenor.net (88.91.62.1)  39.949 ms  40.122 ms  40.429 ms
 3 ti0023c400-ae7-0.ti.telenor.net (146.172.101.9)  65.124 ms  65.390 ms  65.384 ms
 4 ti0016c360-ae2-0.ti.telenor.net (146.172.20.233)  54.888 ms  55.852 ms  56.077 ms
 5 ti3003c400-ae0-0.ti.telenor.net (146.172.23.90)  56.708 ms  57.306 ms  57.331 ms
 6 ti9006b400-ae2-0.ti.telenor.net (146.172.105.81)  62.424 ms  59.392 ms  59.437 ms
 7 decix2-gw.hetzner.com (80.81.193.164)  60.007 ms  62.953 ms  63.065 ms
 8 core23.fsn1.hetzner.com (213.239.229.74)  66.748 ms  65.494 ms  62.591 ms
```

```

 9  ex9k1.dc12.fsn1.hetzner.com (213.239.203.174)  62.611 ms
ex9k1.dc12.fsn1.hetzner.com (213.239.203.186)  57.440 ms
ex9k1.dc12.fsn1.hetzner.com (213.239.203.174)  62.462 ms
10  server4.noderia.com (136.243.23.69)  63.184 ms  62.787 ms  63.527 ms

```

## ➔ nmcli - håndter network manager fra kommandolinjen

Dersom maskinen bruker Network Manager er **nmcli** et nyttig verktøy for å vise og endre informasjon om nettverkstilkoblingen.

### Eksempler:

#### 1) Vis status for gjeldende tilkobling(er)

```

$ nmcli
enp0s3: tilkoblet to Kabeltilkobling 1
"Intel 82540EM"
ethernet (e1000), 08:00:27:8B:BF:97, hw, mtu 1500
ip4 default, ip6 default
inet4 10.0.0.34/24
route4 0.0.0.0/0
route4 10.0.0.0/24
route4 169.254.0.0/16
inet6 2001:4646:2c49:0:5d68:cba1:70ac:b01/64
inet6 2001:4646:2c49:0:78bf:1340:3205:4b4f/64
inet6 fe80::87a9:ecac:18ce:b2e3/64
route6 2001:4646:2c49::/64
route6 ::/0
route6 ff00::/8
route6 fe80::/64
lo: ikke håndtert
"lo"
loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
DNS configuration:
servers: 148.122.164.253 148.122.16.253
interface: enp0s3
servers: 2001:4600:4:1fff::253 2001:4600:4:fff::253
interface: enp0s3





```

#### 2) Vis status for alle maskinens nettverkskort

**\$ nmcli device**

DEVICE	TYPE	STATE	CONNECTION
wlp3s0	wifi	connected	Telenor0555pip-5GHz
mpqemubr0	bridge	connected (externally)	mpqemubr0
docker0	bridge	connected (externally)	docker0
virbr0	bridge	connected (externally)	virbr0
tap-1e376645a40	tun	connected (externally)	tap-1e376645a40
tap-f56b9ce0ac6	tun	connected (externally)	tap-f56b9ce0ac6
enp0s25	ethernet	unavailable	--
cdc-wdm1	gsm	unavailable	--
mpqemubr0-dummy	dummy	unmanaged	--
vboxnet0	ethernet	unmanaged	--
lo	loopback	unmanaged	--
virbr0-nic	tun	unmanaged	--

**3) Vis tilgjengelige trådløse nettverk og gjeldende tilkobling****\$ nmcli dev wifi**

IN-USE	BSSID	SSID	MODE	CHAN	RATE
SIGNAL	BARS	SECURITY			
97		WPA2			
	C8:54:4B:7B:44:EC	Telenor0555pip	Infra	2	130 Mbit/s
*	C8:54:4B:7B:44:EB	Telenor0555pip-5GHz	Infra	36	405 Mbit/s
94		WPA2			
	44:F0:34:F0:99:54	Gunnar	Infra	1	130 Mbit/s
17		WPA2			
	44:F0:34:F0:99:4F	--	Infra	100	540 Mbit/s
17		WPA2			

**4) Konfigurer en statisk ipv4-adresse på enp0s3**

```
$ nmcli con mod enp3s0 ipv4.addresses 192.168.2.20/24
```

Konfigurer default gateway

```
$ nmcli con mod enp3s0 ipv4.gateway 192.168.2.1
```

Konfigurer DNS server:

```
$ nmcli con mod enp3s0 ipv4.dns "8.8.8.8"
```

Bytt fra DHCP til statisk.

```
$ nmcli con mod enp3s0 ipv4.method manual
```

Lagre endringene

```
$ nmcli con up enp3s0
```

### ➔ ss - socket utility program

ss er et program som gir lignende informasjon som **netstat**, men kan gi mer detaljert informasjon om socket tilkoblinger

#### Eksempler:

(Parameterene **-r** og **-t** står for henholdsvis **--resolve** og **--tcp**)

```
$ ss -rt
```

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	wp530:39648	server4.noderia.com:imap
CLOSE-WAIT	1	0	wp530:34468	133.247.244.35.bc.googleusercontent.com:https
ESTAB	0	0	wp530:39632	server4.noderia.com:imap
ESTAB	0	0	wp530:39324	server4.noderia.com:imap
ESTAB	0	0	wp530:54174	10.0.0.82:ssh
ESTAB	0	0	wp530:53306	xx-fbcdn-shv-01-arn2.fbcdn.net:https
ESTAB	0	0	wp530:39370	server4.noderia.com:imap
ESTAB	0	0	wp530:39436	server4.noderia.com:imap
ESTAB	0	0	localhost:33373	localhost:51144
ESTAB	0	0	localhost:51144	localhost:33373
ESTAB	0	0	wp530:53310	xx-fbcdn-shv-01-arn2.fbcdn.net:https
ESTAB	0	0	wp530:39634	server4.noderia.com:imap
ESTAB	0	0	wp530:34018	ec2-52-12-8-165.us-west-2.compute.amazonaws.com:https
CLOSE-WAIT	1	0	wp530:60700	arn09s22-in-x0a.1e100.net:https
ESTAB	0	0	wp530:35738	[2606:4700::6810:5814]:https
CLOSE-WAIT	1	0	wp530:33448	[2600:9000:20a5:c400:a:da5e:7900:93a1]:https
CLOSE-WAIT	1	0	wp530:54150	oscp-router01.gnome.org:https
ESTAB	0	0	wp530:49372	arn11s01-in-x03.1e100.net:https

Parameteret **-4** viser kun ip v4 - adresser

```
$ ss -4
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
tcp	ESTAB	0	0	10.0.0.89:33174	10.0.0.21:ssh
tcp	ESTAB	0	0	10.0.0.89:53440	136.243.23.69:imap
tcp	ESTAB	0	0	10.0.0.89:54274	136.243.23.69:imap
tcp	ESTAB	0	0	10.0.0.89:38940	31.13.72.12:https
tcp	ESTAB	0	0	10.0.0.89:53450	136.243.23.69:imap
tcp	ESTAB	0	0	10.0.0.89:53442	136.243.23.69:imap

### Parameteret -s viser summert statistikk

```
$ ss -s
Total: 1858
TCP:    79 (estab 15, closed 35, orphaned 1, timewait 2)

Transport Total      IP          IPV6
RAW          1           0           1
UDP         33          24           9
TCP          44          31          13
INET        78          55          23
FRAG         0           0           0
```

### Eksempler fra manualen (man ss)

```
ss -t -a
    Display all TCP sockets.
ss -t -a -Z
    Display all TCP sockets with process SELinux security
contexts.
ss -u -a
    Display all UDP sockets.
ss -o state established '( dport = :ssh or sport = :ssh )'
    Display all established ssh connections.
ss -x src /tmp/.X11-unix/*
    Find all local processes connected to X server.
ss -o state fin-wait-1 '( sport = :http or sport = :https )' dst
193.233.7/24
    List all the tcp sockets in state FIN-WAIT-1 for our apache
to network 193.233.7/24 and look at their timers.
ss -a -A 'all,!tcp'
    List sockets in all states from all socket tables but TCP.
```

## ➡ iwlist - informasjon om trådløse nettverk

**iwlist** er en nytting kommando som gir informasjon om trådløse nettverk og nettverkskort. Her er en oversikt over funksjonene til iwlist:

```
iwlist [interface] scanning
iwlist [interface] frequency
iwlist [interface] rate
iwlist [interface] keys
iwlist [interface] power
```

```

iwlist [interface] txpower
iwlist [interface] retry
iwlist [interface] event
iwlist [interface] auth
iwlist [interface] wpakeys
iwlist [interface] genie
iwlist [interface] modulation
iwlist --help
iwlist --version

```

### Eksempler:

#### 1) Finn navnet på tilgjengelige trådløse nettverk

```

$ iwlist wlp3s0 scan | grep ESSID
      ESSID:"Telenor0555pip-5GHz"
      ESSID:"Gunnar"
      ESSID:"Telenor0555pip"

```

#### 2) Få detaljert informasjon om tilgjengelige nettverk:

```

$ iwlist wlp3s0 scan
wlp3s0    Scan completed :
          Cell 01 - Address: C8:54:4B:7B:44:EB
              Channel:36
              Frequency:5.18 GHz (Channel 36)
              Quality=66/70  Signal level=-44 dBm
              Encryption key:on
              ESSID:"Telenor0555pip-5GHz"
              Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                        36 Mb/s; 48 Mb/s; 54 Mb/s
              Mode:Master
              Extra:tsf=0000003b6f59c9b5a
              Extra: Last beacon: 150ms ago
              IE: Unknown:
001354656C656E6F72303535357069702D3547487A
              IE: Unknown: 01088C129824B048606C
              IE: Unknown:
07344E4F202401172801172C01173001173401173801173C011740011764011E68011E6C01
1E70011E74011E84011E88011E8C011E00
              IE: Unknown: 200100
              IE: Unknown: 23021200
              IE: IEEE 802.11i/WPA2 Version 1
              Group Cipher : CCMP

```





**wireshark** er et populært gui-basert program for å overvåke nettrafikk. Det kommer også med en terminalclient som heter **tshark**.

**tshark** kan installeres ved å installere pakken **wireshark-cli**, f.eks. slik:

```
$ sudo dnf install wireshark-cli
```

Når pakken er installert kan du sjekke nettrafikken med kommandoen **tshark**. Output er til skjermen, men du kan om dirigere den til fil med flagget **-w** etterfulgt av et filnavn, eller ved **> filnavn**

## Eksempler

```
$ tshark -w captured
Capturing on 'enp2s0'
42 ^C (avbrutt med <ctrl>+c)
$ cat captured
  1 0.000000000 85.166.78.145 → 136.243.23.69 TCP 66 50468 → 31333 [ACK]
Seq=1 Ack=1 Win=501 Len=0 TSval=207404803 TSecr=2224613649
  2 0.279945757 157.230.226.7 → 136.243.29.75 TCP 60 45593 → 28669 [SYN]
Seq=0 Win=1024 Len=0
  3 0.308624218 45.150.206.103 → 136.243.23.114 TCP 60 61485 → 8014
[SYN] Seq=0 Win=1024 Len=0
  4 0.466938363 136.243.23.69 → 85.166.78.145 TCP 118 31333 → 50468
[PSH, ACK] Seq=1 Ack=1 Win=316 Len=52 TSval=2224614179 TSecr=207404803
  5 0.485010486 45.142.120.147 → 136.243.23.69 SMTP 96 C:
cGVudGVzdEBub2RlcmllhLmNvbQ==
  6 0.485185220 136.243.23.69 → 45.142.120.147 SMTP 84 S: 334
UGFzc3dvcmQ6
  7 0.509512591 45.142.120.147 → 136.243.23.69 SMTP 78 C: AUTH LOGIN
  8 0.509792174 136.243.23.69 → 45.142.120.147 SMTP 84 S: 334
VXNlcm5hbWU6
  9 0.519794448 45.142.120.147 → 136.243.23.69 TCP 66 2748 → 25 [ACK]
Seq=31 Ack=19 Win=30 Len=0 TSval=196896130 TSecr=1806824081
 10 0.529742330 85.166.78.145 → 136.243.23.69 TCP 66 50468 → 31333 [ACK]
Seq=1 Ack=53 Win=501 Len=0 TSval=207405333 TSecr=2224614179
 11 0.544397321 45.142.120.147 → 136.243.23.69 TCP 66 50530 → 25 [ACK]
Seq=13 Ack=19 Win=30 Len=0 TSval=196896154 TSecr=1806824105
 12 0.856981075 212.70.149.53 → 136.243.23.69 TCP 74 50042 → 25 [SYN]
Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3889589187 TSecr=0
WS=1024
 13 0.857006542 136.243.23.69 → 212.70.149.53 TCP 74 25 → 50042 [SYN,
ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1405617128
TSecr=3889589187 WS=128
 14 0.885462603 212.70.149.53 → 136.243.23.69 TCP 66 50042 → 25 [ACK]
Seq=1 Ack=1 Win=29696 Len=0 TSval=3889589215 TSecr=1405617128
 15 0.885626938 136.243.23.69 → 213.133.100.100 DNS 86 Standard query
0x6ae9 PTR 53.149.70.212.in-addr.arpa
```

```

16 0.885852051 213.133.100.100 → 136.243.23.69 DNS 146 Standard query
response 0x6ae9 No such name PTR 53.149.70.212.in-addr.arpa SOA
pri.authdns.ripe.net
17 0.886377133 136.243.23.69 → 212.70.149.53 SMTP 105 S: 220
server4.noderia.com ESMTP Postfix
18 0.914859110 212.70.149.53 → 136.243.23.69 TCP 66 50042 → 25 [ACK]
Seq=1 Ack=40 Win=29696 Len=0 TSval=3889589245 TSecr=1405617157

```

Hvis vi vil se på trafikken til og fra en bestemt ip-adresse eller domenenavn, kan vi sette det etter parameteret **host**, slik:

```
$ tshark host itfakultetet.no
```

Vil vi se resultatet i hex-format istedenfor i binærformat, kan vi legge til flagget **-x**, og vi kan også spesifisere hvilket netterkskort som skal brukes, med flaget **-i**:

```

$ tshark -x -i wlp3s0 host itfakultetet.no
Capturing on 'wlp3s0'
0000  6c 88 14 65 87 88 c8 54 4b 7b 44 ea 08 00 45 00  l..e...TK{D...E.
0010  00 4c 93 f4 40 00 37 06 05 27 88 f3 17 45 0a 00  .L...@.7...'...E..
0020  00 59 01 bb bb 24 bd d7 3c a5 55 e8 35 43 80 18  .Y...$...<.U.5C..
0030  01 02 bb ca 00 00 01 01 08 0a 8f c5 eb 73 0d 36  .....s.6
0040  4c 63 17 03 03 00 13 77 50 5f 7b 3b 6f c5 df 5d  Lc.....wP_{;o..]
0050  85 6f c8 49 43 2c e6 b5 38 11                    .o.IC,..8.

```

## ➔ Øvelse: Finn tilkoblede maskiner i et nettverk med fping og arp-scan

I denne øvelsen skal vi se på ulike måter kartlegge et nettverk på.

Først skal vi se hvilke maskiner som er aktive på nettverket, dvs. er tilkoblet. For dette kan vi bruke programmet **fping**. **fping** er ofte ikke installert i en standard distro, men vi kan enkelt installere det med:

```
$ sudo dnf install fping
```

Her er kommandoen som returnerer IP-adressen til maskiner som er tilkoblet nettverket:

```

$ fping -a 10.0.0.1/24 -g 2>/dev/null
10.0.0.16

```

```
10.0.0.20
10.0.0.57
10.0.0.82
10.0.0.89
10.0.0.138
```

**Forklaring:** Parametreret **-a** (alive) lister kun aktive maskiner, 10.0.0.1/24 angir nettverket som skal undersøkes. Parameteret **-g** (generate) lager en liste av ip-adresser som skal sjekkes. 2>/dev/null sender feilmeldinger til bit-bøtta (/dev/null). Det hindrer at skjermen blir full av feilmeldinger for alle ip-adressene som ikke kan nås, slike som denne:

ICMP Host Unreachable from 10.0.0.89 for ICMP Echo sent to 10.0.0.166

## arp-scan

Vi kan også bruke programmet arp-scan til samme oppgave. Det må også som regel installeres, som man kan gjøre med kommandoen:

```
$ sudo dnf install arp-scan
```

Slik brukes arp-scan på et lokalt nettverk:

```
$ sudo arp-scan 10.0.0.0/24
Interface: wlp3s0, type: EN10MB, MAC: 6c:88:14:65:87:88, IPv4: 10.0.0.89
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.0.20    fc:87:43:6c:bc:96    HUAWEI TECHNOLOGIES CO.,LTD
10.0.0.16    b4:f6:1c:63:b1:69    Apple, Inc.
10.0.0.57    08:00:27:b5:03:29    PCS Systemtechnik GmbH
10.0.0.82    08:00:27:b5:03:29    PCS Systemtechnik GmbH
10.0.0.41    38:f9:d3:63:9d:02    Apple, Inc.
10.0.0.55    e4:19:c1:78:71:d9    HUAWEI TECHNOLOGIES CO.,LTD
10.0.0.138   c8:54:4b:7b:44:ea    Zyxel Communications Corporation
7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.954 seconds (131.01
hosts/sec). 7 responded
```

## ➡ Øvelse: Hva er min eksterne ip-adresse?

Dette er en enkel, liten øvelse, som ikke anbefales i jobbsammenheng, av sikkerhetsgrunner, men kan være en nyttig ting å gjøre når du er på et hjemmenettverk og raskt vil vite hva din eksterne i-adresse er.

1) Sjekk adressen hos *ifconfig.me* med kommandoen

```
$ curl -s ifconfig.me
```

3) legg til et linjeskift:

```
$ curl -s ifconfig.me | ech
```

3) Legg til som et alias i [.bashrc](#), med f.eks vim

```
alias me="curl -s ifconfig.me && echo"
```

4) reload [.bashrc](#)

```
$ source .bashrc
```

5) Sjekk at det virker:

```
$ me  
85.165.21.92
```

# Kapittel 10

## Skallskripting

### ➔ Øvelse: Skript som teller antall forekomster av ordene i en tekstfil

Dette skriptet er basert på en en-linjes kode som leser inn en fil fra disk eller url, setter hvert ord på en egen linje, luker bort tegnsetting og tall, oversetter ordene til små bokstaver, teller opp antall forekomster av hvert ord og sorterer etter antall forekomster, i synkende orden.

Vi bruker denne filen til øvelsen: <https://web.itfakultetet.no/war-and-peace.txt>

Filen inneholder hele teksten (alle 16 bøkene) til Tolstojs Krig og Fred. (hentet fra [www.gutenberg.org](http://www.gutenberg.org))

Her er trinnene som skal utføres:

1) Lese inn tekstfilen.

a) Fra URL: `curl https://web.itfakultetet.no/war-and-peace.txt`

b) fra fil: `cat war-and-peace.txt`

2) Erstatt alle mellomrom med linjeskift: `sed 's/\s/\n/g'`

3) Fjern all tegnsetting og tall: `sed 's/[:punct:]]\|[0-9]//g'`

4) Gjør om alle ord til små bokstaver: `tr '[:upper:]' '[:lower:]'`

5) Sorter alfabetisk: `sort`

6) Tell antall forekomster av hvert ord: `uniq -c`

7) Sorter etter antall (dvs numerisk) i synkende rekkefølge: `sort -n -r`

8) Lagre resultatet i en fil: `> forekomster_av_ord_i_$1` (filnavnet ender med navnet til en opprinnelige filen)

**Slik kan skriptet se ut:**

```

#!/bin/bash

## Sjekk om det er sendt et parameter til programmet.
## Variablen $# inneholder antall parametere
if [ $# -eq 1 ]; then

    cat $1 \
    | sed 's/\s/\n/g' \
    | sed 's/[[[:punct:]]\|[0-9]]//g' \
    | tr '[:upper:]' '[:lower:]' \
    | sort \
    | uniq -c \
    | sort -n -r \
    > forekomster_av_ord_i_$1

else
    echo "Bruk: gi ett filnavn som parameter"
fi

```

**MERK:** \ på slutten av en linje lar oss fortsette koden på neste linje - men det må ikke stå noe, ikke engang et mellomrom etter \

Sett kjøretillatelse på filen med kommandoen:

```
chmod +x tellord.sh
```

(gitt at filen heter tellord.sh)

Kopier den til /usr/local/bin/tellord , så kan du bruke den uansett hvilken mappe du er i:

```
sudo cp tellord.sh /usr/local/bin/tellord
```

## ➔ Øvelse: Skript for analyse av logger - som kan kjøres av cron

Her er et skript som sjekker innloggingsforsøk via SSH og lagrer resultatet i filer som kopieres via SSH til en annen maskin



```
#!/bin/bash
# sjekk logger og lagre resultater
fgrep "Failed" /var/log/auth.log > /tmp/failed.txt
fgrep "Accepted" /var/log/auth.log > /tmp/accepted.txt

# beregn login-forsøk
flog=`less /tmp/failed.txt | wc -l`
vlog=`less /tmp/accepted.txt | wc -l`

# Lag litt tekst
feilede="$flog Feilede innlogginger via ssh til Serveren"
vellykkede="$vlog Vellykkede innlogginger via ssh til Serveren"

# lagre i summeringsfil
echo -e $feilede'\n'$vellykkede > /tmp/summary.txt

# lag filnavn
f=logs.($(date +%d-%m-%Y).tgz

# lag zippet arkiv
tar -czf /tmp/$f /tmp/{summary.txt,failed.txt,accepted.txt}

# scopy filene
scp -P 2222 /tmp/$f terje@localhost:Logger

# clean up
rm -f /tmp/$f /tmp/accepted.txt /tmp/failed.txt /tmp/summary.txt

# exit med status fra siste handling
exit $?
```

For å legge kjøring av scriptet inn i crontab, bruk kommandoen:

```
$ crontab -e
```

Sett inn f.eks. denne linjen:

**0 1 \* \* \* /usr/bin/sendlogger.sh**

så kjøres skriptet hver natt kl. 1

## ➔ Øvelse: Skript for oppretting eller konvertering av bilder

Kommandolinjen gir deg muligheter som de grafiske programmene ikke har - eller som de bruker mye lengre tid på å utføre. For eksempel kan du konvertere hele mapper med lyd eller bildefiler filer med én kommando, noe som er uendelig mer effektivt enn å åpne hver fil i f.eks. Gimp eller Audacity, konvertere, lagre og åpne neste fil etc. Mange av de grafiske programmene har også et kommandolinje-grensesnitt - slik at man kan få f.eks. Gimp eller Open Office til å utføre kommandoer skrevet i et terminlvindu.

### Bildebehandling med ImageMagick

**ImageMagick** er et glimrende program-bibliotek for å manipulere bildefiler. Det brukes som underliggende "slave" av flere grafiske programmer, og man kan også bruke det hvis man programmerer i f.eks. Python eller PHP. Hvis det ikke allerede er installert på PCen din, kan du gjøre dette slik:

**Ubuntu:** `sudo apt-get install imagemagick`

**Suse:** `zypper install imagemagick`

**Fedora:** `yum install imagemagick`

Eller bruk Synaptic (eller din distros grafiske pakkehåndterer).

Når Imagemagick er installert får du tilgang til kommandoen ***convert***. Denne kan du bruke f.eks. slik:

```
$ convert bilde.jpg bilde.png    (konverterer fra jpg- til png-format)
$ convert bilde.gif bilde.jpg    (konverterer fra gif- til jpg -format)
```

Men du kan gjøre utrolig mye mer enn dette. F.eks:

```
$ convert -resize 650 bilde.jpg bilde.png    (konverterer og endrer
bredden til 650 px)
$ convert -border 10 bilde.jpg bilde.png    (konverterer og legger til en
10px bred grå ramme)
```

Kommandoen ***mogrify*** lar deg konvertere en hel mappe med filer fra ett format til et annet. F.eks.:

```
$ mogrify -format png *.jpg
```

Dette vil konvertere alle jpg-filer i den aktuelle mappen til png-format.

## Lagre tekst som bilde

---

```
$ convert -size 870x110 canvas:none -font Bookman-DemiItalic \  
-pointsize 90 -draw "text 25,80 'God Jul fra Terje'" \  
-channel RGBA -blur 0x6 -fill darkred \  
-stroke magenta -draw "text 20,75 'God Jul fra Terje'" GodJul.png
```

Kommandoen over resulterer i dette bildet - **GodJul.png** :



## Endre størrelsen på alle bildene i en mappe

---

Her er et skript som endrer størrelsen på alle jpg-bilder i en mappe, oppretter en undermappe og kopierer de endrede bildene dit. (Skriptet forutsetter at imagemagick er installert). Kopier teksten nedenfor til en fil du kaller f.eks. **konverter\_bilder.sh** Gi filen kjøretillatelse, f.eks. ved åpne et terminalvindu i mappen filen ligger i og skrive:

```
$ chmod +x konverter_bilder.sh
```

Kildekode:

```
#!/usr/bin/bash  
echo -n "Tast inn en bildebredde: "  
read format  
mkdir bilder_$format  
for bilde in *.jpg  
do convert -resize $format -border 20 $bilde bilder_$format/$format_$bilde  
echo Formaterer $bilde  
done  
echo Suksess! Bildene ligger i mappen bilder_$format
```

**Tips:** Hvis du f.eks. kaller filen **konverter**(uten .sh) og kopierer den til mappen /usr/bin eller /usr/local/bin, kan du endre bildene i hvilken som helst mappe ved å gå til mappen og taste inn **konverter** , slik:

```
/home/bruker/bilder$ konverter
```

Merk: Du må bruke sudo for å kopiere til /usr/bin eller /usr/local/bin

## ➔ Et par enkle triks

Her er noen enkle "triks" som kan brukes fra kommandolinjen for å gjøre noen oppgaver enklere:

### 1. Start en webserver med en linje kode:

---

```
$ python -m SimpleHTTPServer
```

eventuelt:

```
$ python2 -m SimpleHTTPServer
```

Denne linjen gjør at det startes en webserver som lister opp innholdet i den mappen du er i når kommandoen skrives. Webserveren lytter på port 8000, så for at du eller andre skal se filene med nettleseren, taster du inn:

```
http://localhost:8000
```

eller

```
http://petters_desktop:8000 (hvis petters_desktop er vertsnavnet til maskinen din)
```

eller

```
http://10.0.0.2:8000 (hvis 10.0.0.2 er IP-adressen til maskinen din på lokalnettverket)
```

Drep webserveren med ctrl+c når du ikke har bruk for den lenger

## 2. Sjekk hvilken web-server et nettsted kjører

---

Lynx er en tekstbasert nettleser som kan brukes til dette - f.eks. slik:

```
$ lynx -dump -head http://vg.no | grep -i server
```

Et enkelt skript kan gjøre det enklere:

```
#!/usr/bin/bash  
  
lynx -dump -head https://www.$1 | grep -i server
```

Kall skriptet f.eks. webserver.sh, gi det kjøretillatelse med chmod +x og kopier det (med sudo) til f.eks. /usr/local/bin/webserver

### Bruk:

```
$ webserver regjeringen.no
```

### Output:

```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
```