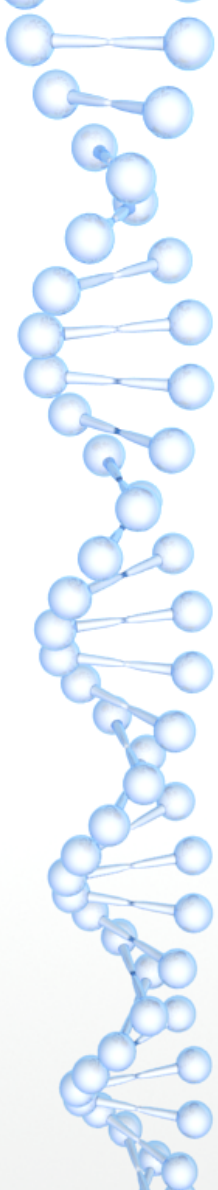
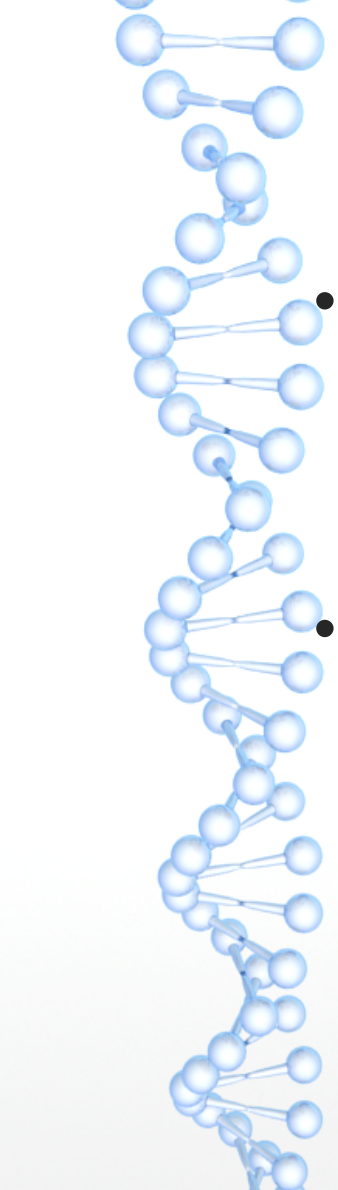


Linuxia ja verkkoa kybernäkökulmasta

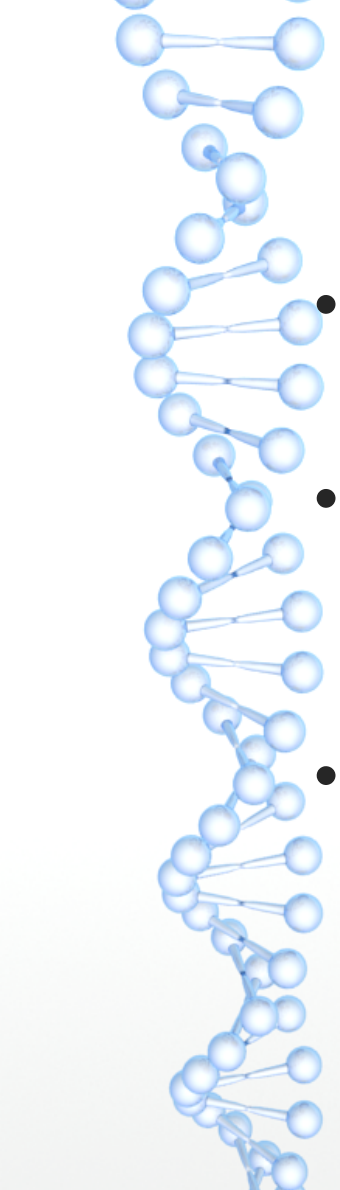
Tuomas Tenkanen

ITKST55



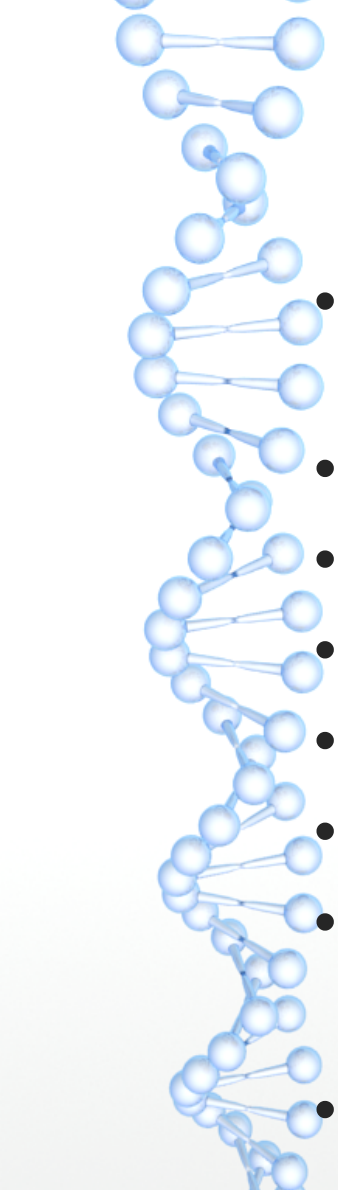
Linux

- tarkasti ottaen käyttöjärjestelmäydin, kernel
  - vrt. esim. Darwin, Windows NT Kernel
  - tarvitsee ympärilleen käyttöympäristön
- usein kuitenkin käyttöjärjestelmäjakelu, jossa ytimenä Linux
  - Ubuntu, Debian, Red Hat, Centos, SuSE
  - käyttöympäristönä tavallisesti GNU
  - yhtenä tärkeimpänä jakeluja erottavana tekijänä pakettienhallintajärjestelmät
    - deb, rpm, pacman



Miksi Linux?

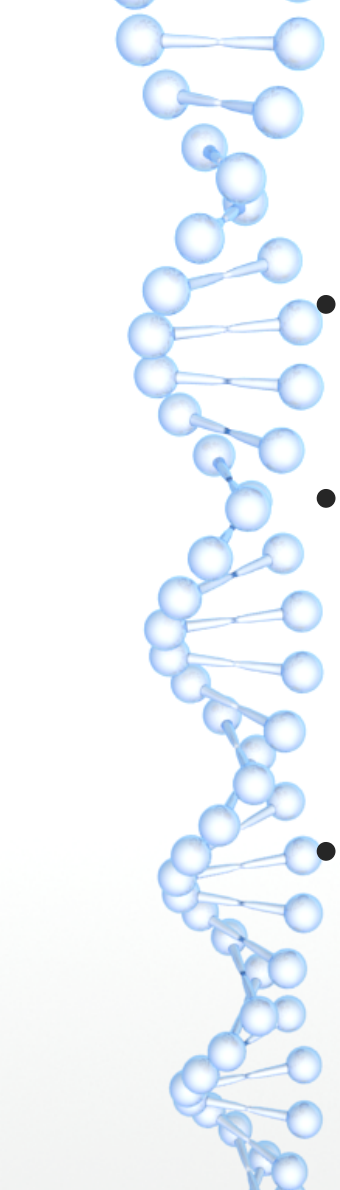
- vapaasti saatavilla
- n. 70 % maailman top 1 M –web-sivustoista joko Apache tai nginx [1]
- 90+ % Apachea käyttävistä Linux [2]:
  - CentOS 30 %, Debian 27 %, Ubuntu 24 %
  - Windows 7 %, Red Hat 5 %, FreeBSD 3 %



Jakeluja

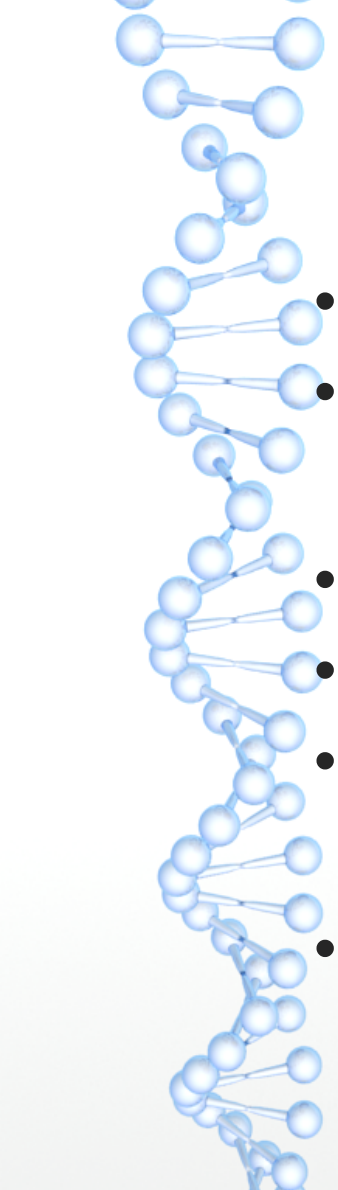
- Debian, Ubuntu, RedHat, CentOS, Fedora, openSUSE, SUSE
- Kali
- Tails
- SecurityOnion
- VyOS
- Raspbian
- Android

- LTS, Rolling Distribution



Pakettienhallinta

- deb, rpm
- asenna ohjelma a
  - tarvitsee kirjastot x, y, z
  - x tarvitsee vielä b, c
- pakettienhallinta hoitaa riippuvuudet
  - asentaa a, b, c, x, y, z

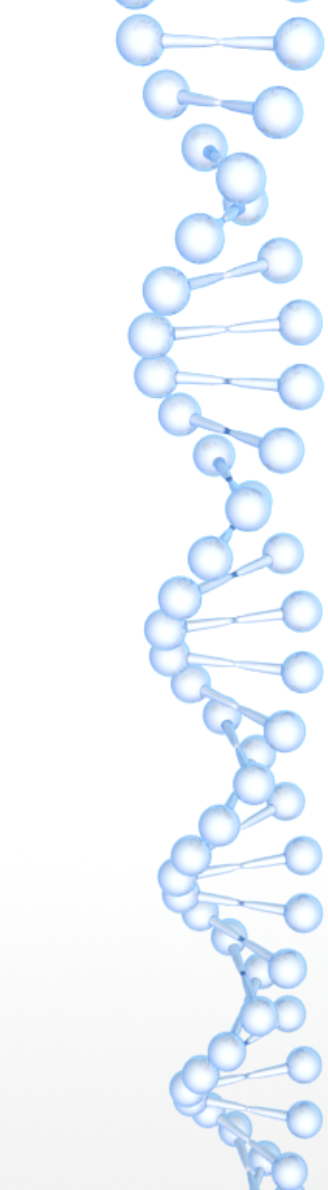


Palvelin

- nimessä vihje, tarjoaa jotain palvelua
- laite, kone, virtuaalikone, ohjelma

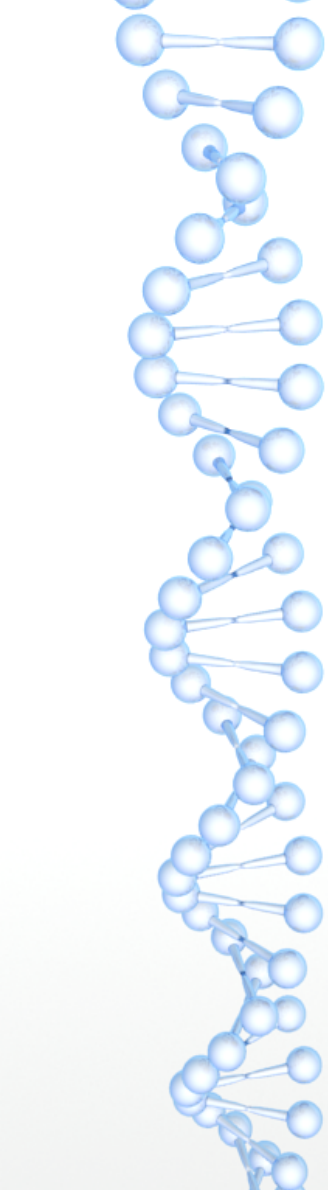
- usein aina päällä
- useita käyttäjiä
- käytetään etänä

- esim: www, levy, tulostus, sähköposti, tietokanta, laskenta, pikaviestit, verkon peruspalvelut: dns, ntp, dhcp, proxyt



Palvelun perusmalli

- suoritettava ohjelma, binääri
  - sidotaan johonkin porttiin, saa porttiin saapuvan liikenteen käsiteltäväkseen ja vastaa
- konfiguraatio yleensä tiedostossa (/etc)
- data jossain (esim. /var/www)
- lokit tiedostoon (/var/log)



Palveluiden luettelointi

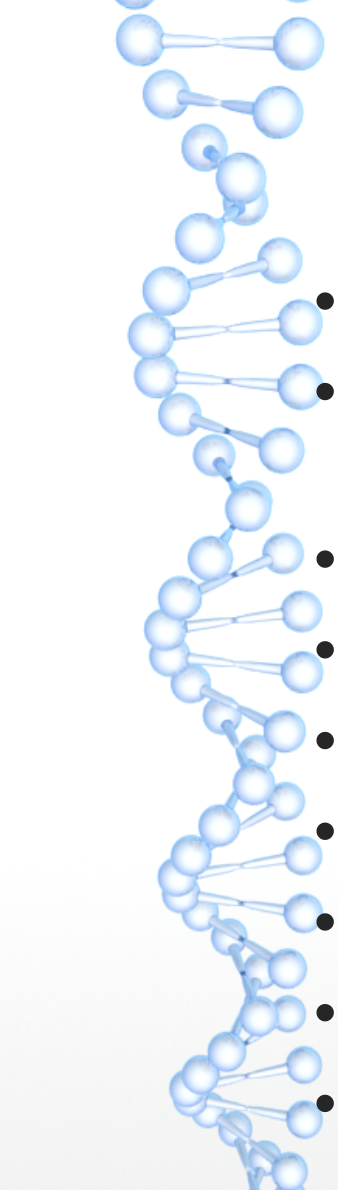
- service, systemctl
- service --status-all
- systemctl list-unit-files
- systemctl list-unit-files –type=service –state=running,failed

- https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units

Linux-palvelinten hallinta etänä

- “Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. The best known example application is for remote login to computer systems by users.” [4]

- “The shell is a user program or it is an environment provided for user interaction. It is a command language interpreter that executes commands read from the standard input device such as keyboard or from a file.” [5]



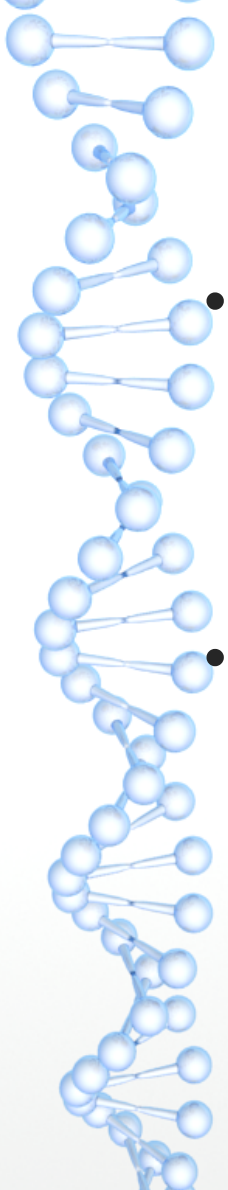
SSH, SSHD

- tcp/22
- tunnistautuminen käyttäjätunnus/salasanalla tai avaimilla
- /usr/bin/ssh, yleensä polussa
- ~/.ssh/config
- ~/.ssh/authorized_keys
- ~/.ssh/known_hosts
- ~/.ssh/id_rsa[.pub], ~/.ssh/id_dsa[.pub]
- /etc/ssh/ssh_config
- /etc/ssh/sshd_config

IP-osoitteet Linux-palvelimella

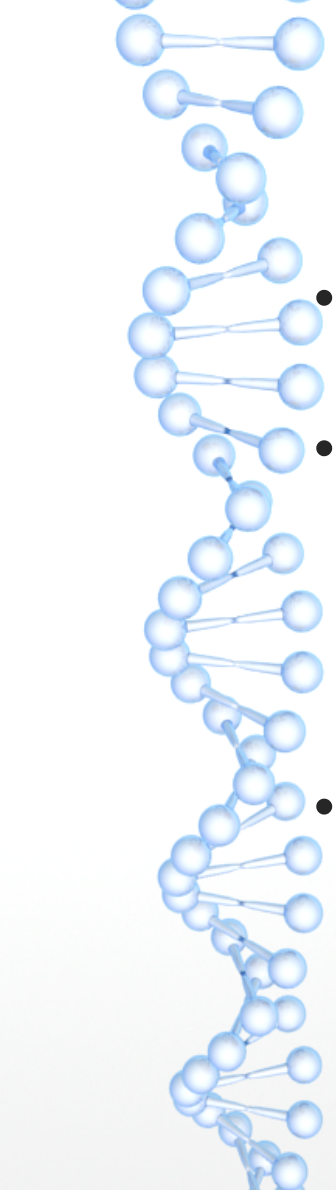
- service network-manager disable; service networking enable
- cat /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 172.20.209.45
        netmask 255.255.0.0
        network 172.20.0.0
        broadcast 172.20.255.255
        gateway 172.20.0.1

# dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 172.20.0.2
```



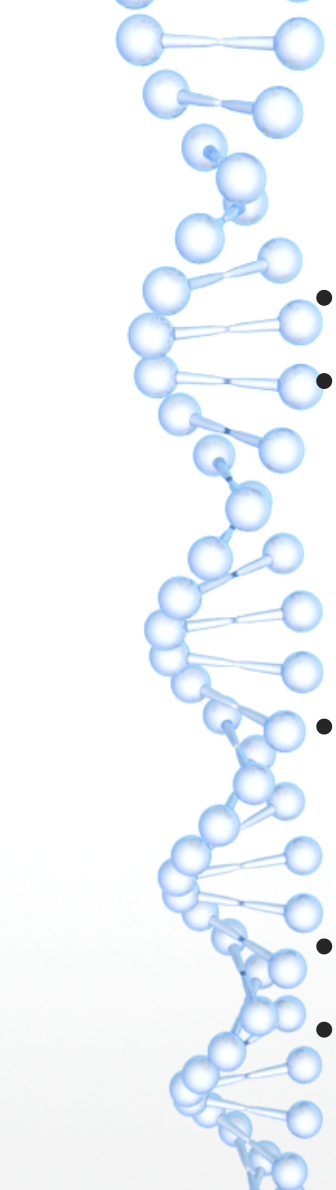
DNS-asiakasasetukset

- **resolv.conf, hosts**
  - Tiedostot /etc/resolv.conf ja /etc/hosts sisältävät määrittelyjä mistä koneita etsitään kun käytetään vain hostnamea ja tunnettujen koneiden osoitteita.
- **resolvconf uudemmissa jakeluissa**
  - Uudemmissa jakeluissa oletusverkkoasetuksilla /etc/resolv.conf kirjoitetaan automaattisesti yli verkkoasetusten päivittyessä esim. DHCP:n kautta. Ratkaisuna on asentaa paketti resolvconf, joka asentaa mm. tiedoston /etc/resolvconf/resolv.conf.d/base, jonne voi tehdä omia pysyviä määrityksiä.



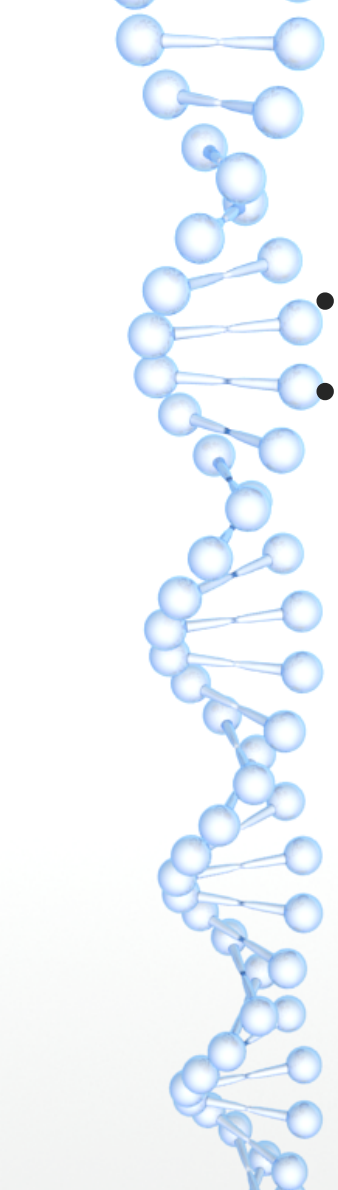
Reittien määrittely: ip route

- Mikä on reitti?
- ip route, ip r
  default via 172.20.0.1 dev eth0 metric 100
  172.20.0.0/16 dev eth0 proto kernel scope link src 172.20.209.45
- Reittien lisääminen, poistaminen, muuttaminen:
  - ip route add 192.168.1.0/24 dev eth0
  - ip route delete 192.168.1.0/24 dev eth0
  - man ip
  - ip route help



Portit, protokollat, palvelun liittäminen porttiin

- portti: IP-osoitteeseen liitetty 16-bittinen numero
- protokollat:
  - TCP (tilallinen, taataan pakettien perillemeno oikeassa järjestyksessä)
  - UDP (tilaton, ei taata mitään)
  - ICMP, IGMP, OSPF. 142 rekisteröityä, mahd. 255.
- esim. TCP/80 = HTTP
  - /etc/services
  - sopimuskysymys
- porttia kuuntelemaan sidotaan (bind) palvelinohjelma
- paketin sisältö kuuntelevan ohjelman käsiteltäväksi

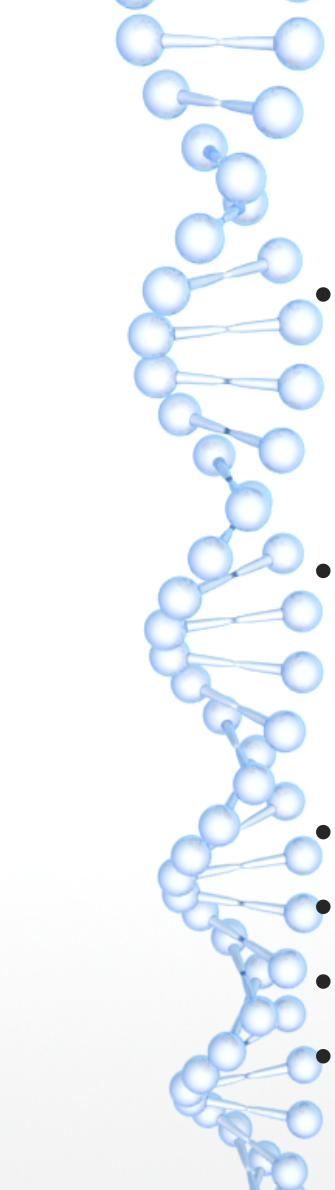


Käytössä olevat verkkoyhteydet

- ss
- netstat
  - a: kaikki yhteydet
  - t: tcp
  - u: udp
  - l: listen, portit joissa joku ohjelma kuuntelemassa
  - p: pid/program
  - n: numeric
  - e: extended, voi olla kaksikin
  - netstat -tulpen

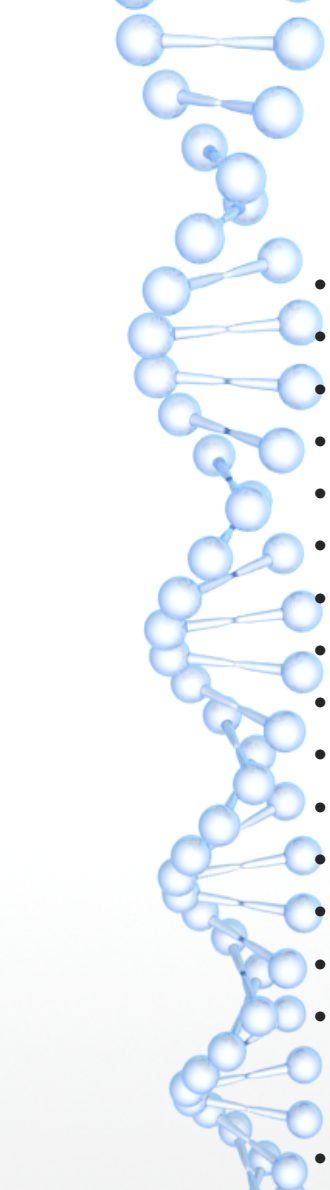
Levytila, osiot

- Kiintolevyt (tms) jaetaan osioihin:
  - yhdellä osiolla voi olla yksi tiedostojärjestelmä
- osioinnilla suojataan palvelinta ja käyttäjän tiedostoja
  - esim: käyttäjät eivät voi täyttää koko levyä
  - esim: villintyneen prosessin loki ei voi täyttää koko levyä
- osioinnilla voidaan saavuttaa parempi suorituskyky
- (perinteisesti) osioita on yhdellä levyllä voinut olla neljä
- osioita kolmen tyyppisiä:
  - primääri
  - extended (max 1), joka voi sisältää:
  - looginen
- osiotaulu kertoo miten levy jaettu (MBR, GPT)
- käyttöjärjestelmän asennus yleensä ehdottaa jotain osiointia, palvelinasennuksessa syytä tietää mitä tapahtuu
- Windowsissa osiot nimetty C:, D:, ym (drive letter)
- Linuxissa levyt esim. /dev/sda, /dev/sdb, /dev/vda, /dev/hda
- Linuxissa osiot /dev/sda1, /dev/sda2, /dev/sda5
- työkaluja: fdisk, parted



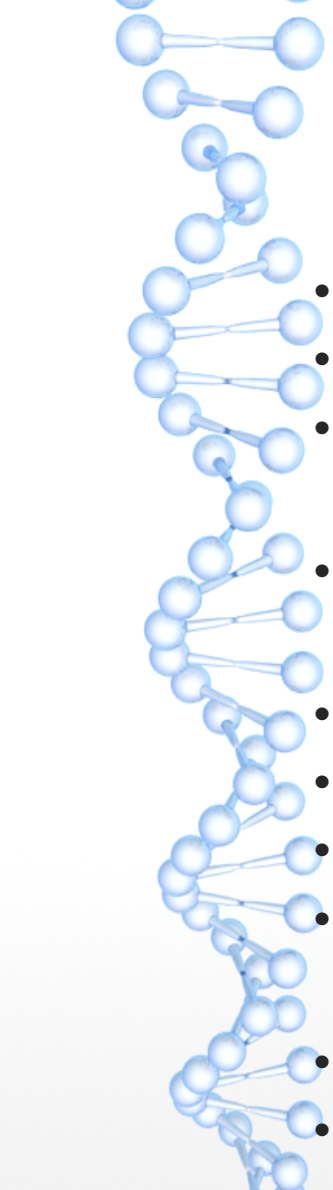
Levytila, tiedostojärjestelmät

- Tiedostojärjestelmätyypit
  - ext2, ext3, ext4, xfs, tmpfs
  - Tiedostojärjestelmän luonti osiolle: mkfs.ext4 /dev/vda5
  - Tiedostojärjestelmän tarkistus: fsck (oltava irrotettuna)
- mount point, liitospiste: hakemisto, johon osio liitetään
  - Liittäminen/irroittaminen:
    - mount /dev/vda5 /home
    - umount /home, umount /dev/vda5
- /etc/fstab
- blkid
- LVM
- md (RAID)



Tiedostojärjestelmän rakennetta

- /boot: käynnistystiedostot, kernel, initramdisk
- /dev: laitteet
- /etc: konfiguraatiotiedostot
- /home: käyttäjien tiedostot
- /lib, /lib64: kirjastot
- /media, /mnt: liitospisteitä ulkoisille levyille
- /opt: muu softa (pakettienhallinnan ulkopuolelta)
- /proc: (ajonaikainen) järjestelmän tiedot, prosessit
- /root: rootin kotihakemisto
- /run: ajonaikasta dataa
- /sbin: system binaries
- /srv: palvelinsoftien data
- /sys: laitetiedot
- /tmp: tilapäistiedostot
- /usr: käyttäjien yhteiset pysyväisluonteiset tiedostot: ohjelmia, lähdekoodia, käyttöohjeita
  - /usr/local: (pakettienhallinnan ulkopuolelta)
- /var: muuttuva data: lokit, cachet, postit, tietokannat



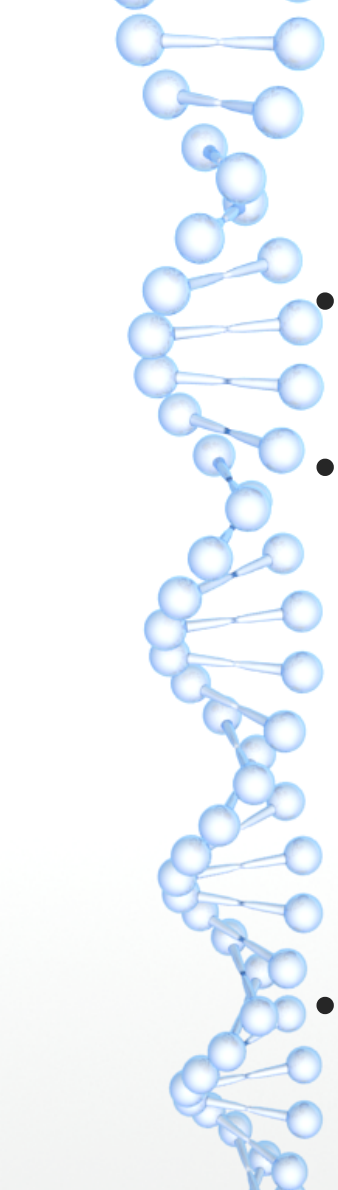
Levytilan käyttö ja tarkastelu

- mount
- ls /dev/disk/by-id
- ls /dev/disk/by-uuid

- blkid

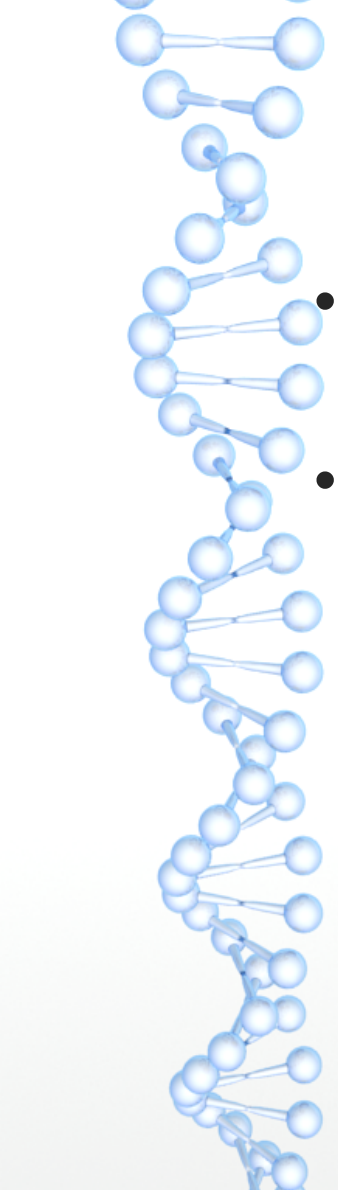
- df, df -h, df -i
- du, du -hs *
- find /home/tusatenk -type f -size +10000
- lsof –s

- tail /var/log/syslog
- tail -f /var/log/syslog



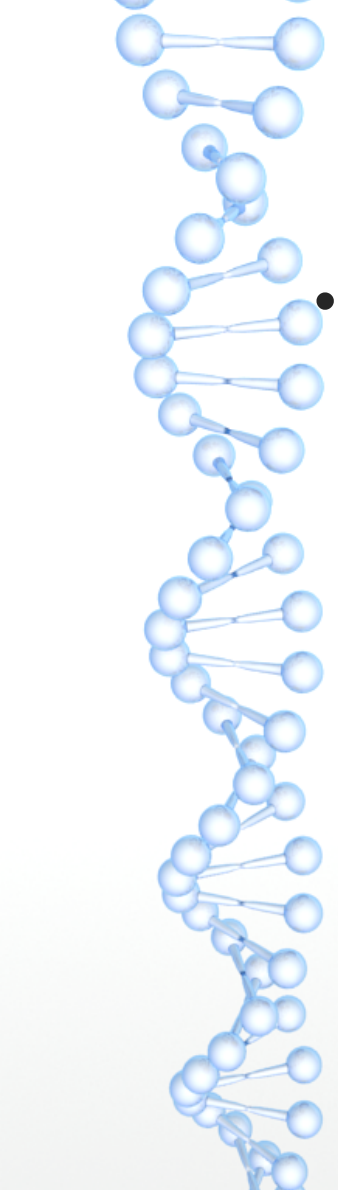
Prosessit

- Prosessi on ajossa oleva ohjelman instanssi, jolle on varattu resursseja, esim. muistia
- Prosessien tarkasteluun
  - pstree
  - ps, ps x, ps aux, ps -ef
  - top
  - &, bg, fg
  - kill, killall
  - lsof
- **Prosessilla auki olevaa tiedostoa ei pidä poistaa ennen prosessin tappamista!**



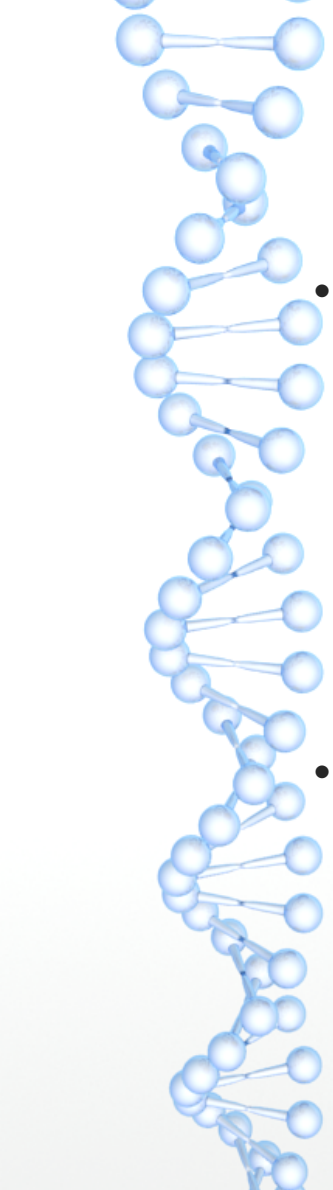
Tiedostot, linkit

- Tiedoston data tallennettuna jonnekin päin levyä
- Tiedostojärjestelmässä kirjanpito osoitteista:
  - tiedostonimi toimii linkkinä dataan
  - linkkejä voi olla useita (hard link, ln)
  - tiedosto "poistetaan" kun ei enää linkkiä
    - oikeasti dataa ei poisteta, vain kirjanpidosta
    - tila vapaa käytettäväksi muuhun, voi kirjoittaa päälle
    - jos tiedosto auki ja kirjoitetaan..
  - symlinkit vain viitteitä (soft link, symbolic link, ln –s)
    - vrt pikakuvake Windowsissa



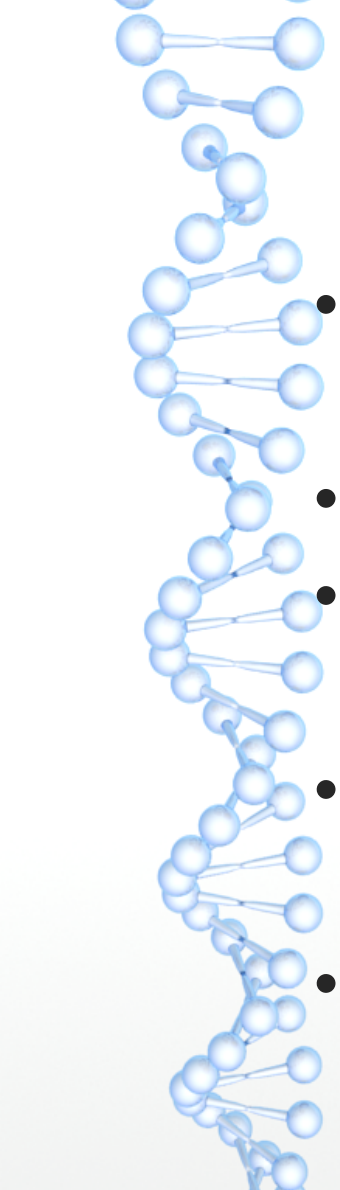
Tiedostojen oikeudet

- luku, kirjoitus, suoritus/haku (rwx)
  - lisäksi suid (s), sticky (t)
  - esim. -rwxr-x—:
    - user rwx
    - group r-x
    - others —
  - esim. 0755 == -rwxr-xr-x
  - esim. 0600 == -rw———-
    - ts r = 4, w = 2, x = 1
  - muuttamiseen: chmod, chown, chgrp



Käyttäjät

- käyttäjätunnus, ryhmät, others (ugo)
  - /etc/passwd
    - tunnus:salasana:**uid**:ryhmä:näyttönimi:kotihakemisto:**shell**
  - /etc/shadow
  - /etc/group
  - PAM, Kerberos, LDAP, AD
  - adduser, deluser (useradd, usermod, groupmod, newgrp)
  - id, groups
- root: superuser, käyttäjä jolla kaikki oikeudet
  - kirjautuminen nykyään usein estetty, joskus välttämätön
  - yleensä parempi tapa: sudo komento
  - sudo -u
  - /etc/sudoers, /etc/sudoers.d
  - sudo –i, sudo su –
  - su, su -



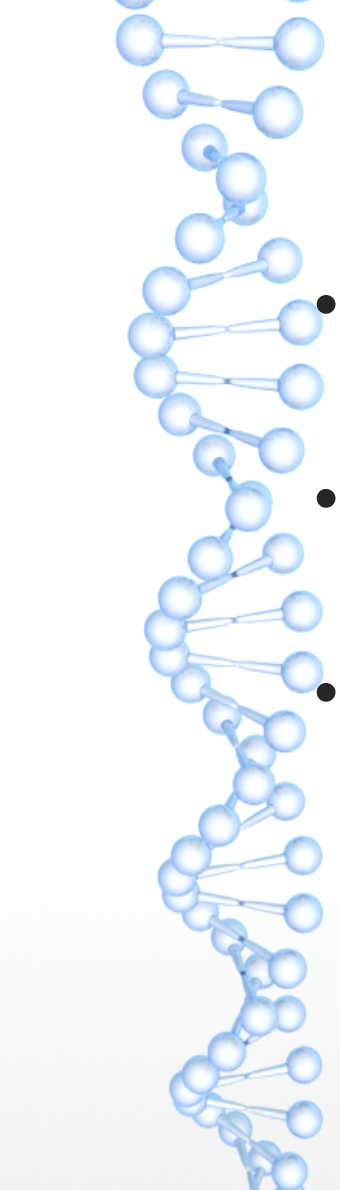
Lokit

- /var/log

- syslog – järjestelmän pääloki
- auth.log – kirjatumisiin liittyviä

- alihakemistot, esim. apache2, nginx, mysql

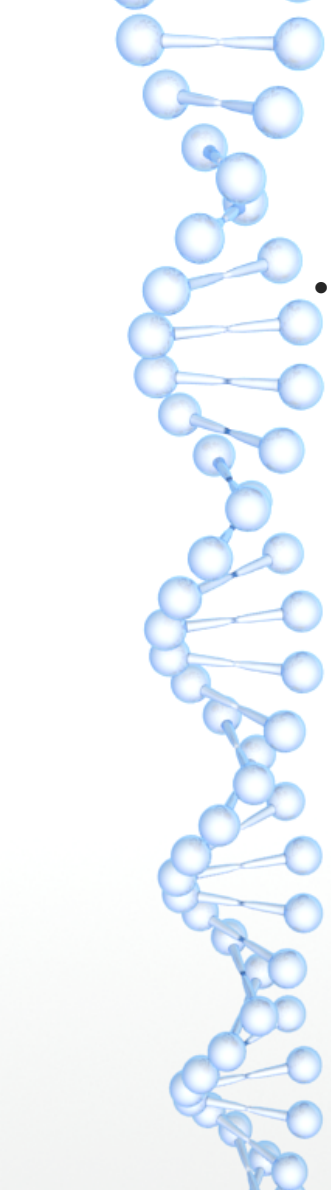
- dmesg – laitteiden/ajureiden viestit



Root

- käyttäjä, uid 0
- tiedostojärjestelmän juuri, /
- pid 1
  - init, nykyään usein systemd

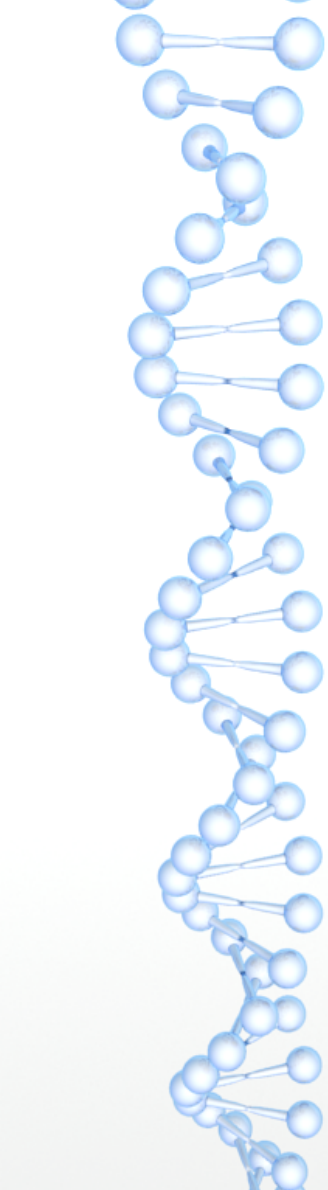
deb-pakettien hallinta



- Pakettienhallinnan tarkoitus on huolehtia ohjelmien tarvitsemista kirjastoista ja muista riippuvuuksista käyttäjän puolesta
  - apt-get update (apt update)
  - apt-get dist-upgrade (apt dist-upgrade)
  - apt-get install (apt install)
  - apt-get remove
  - apt-get purge
  - apt-get autoremove
  - apt-get -f install
  - apt-get clean
  - apt-cache search
  - dpkg -l (dpkg -l | awk '{print $2})
  - dpkg -L
  - dpkg -i
  - dpkg-reconfigure (-a)
  - apt show

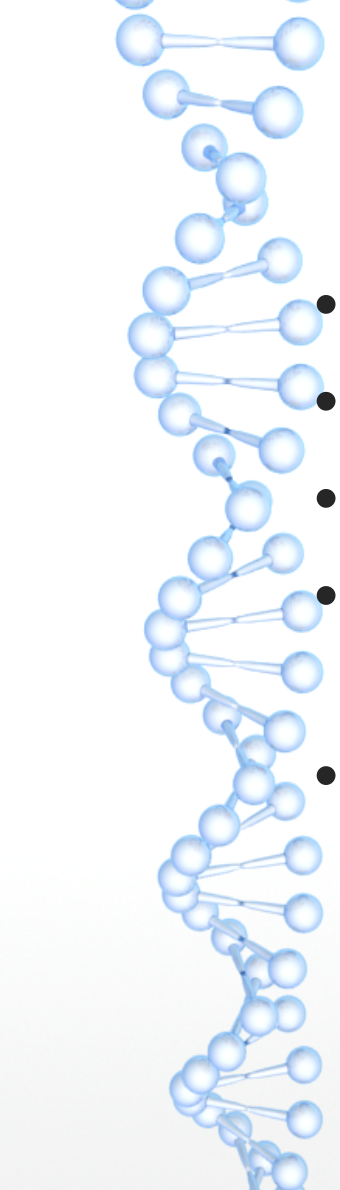
Pakettienhallinnan asetukset

- /etc/apt/sources.list (repositoryt)
- /etc/apt/apt.conf (proxy)
- /etc/apt/apt.conf.d/
- /etc/update-manager
- do-release-upgrade: päivitä käyttöjärjestelmäversio



Ajastetut toiminnot

- Cron
  - crontab -l, crontab -e, crontab -u
  - /etc/cron*
- At, atq, atrm
- Batch

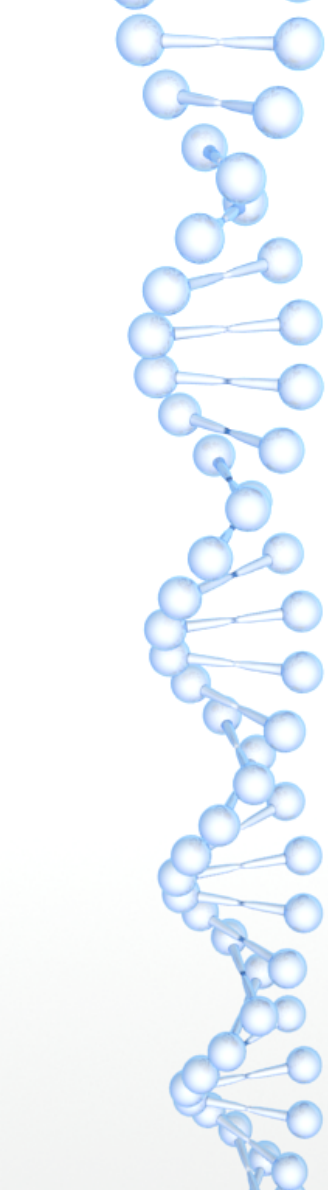


Iptables (netfilter)

- Kernelin palomuuri
- iptables –L
- pakettitason palomuuri
- lisämoduleilla mahdollista seurata esim. yhteyksiä
- TCP-flägit

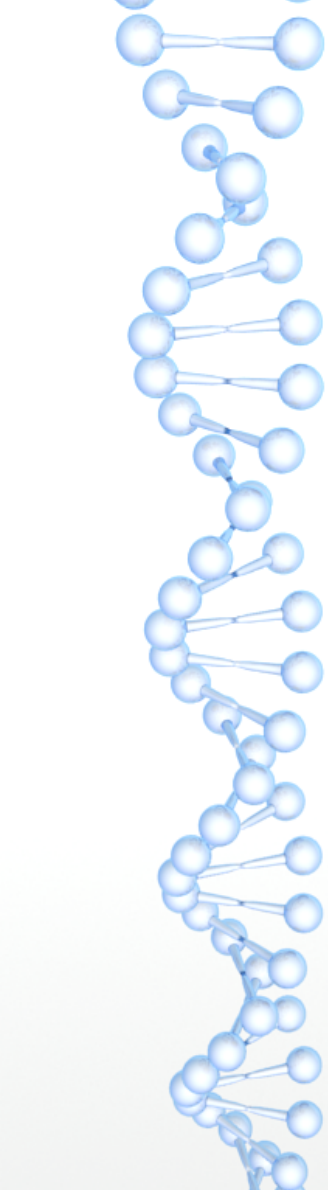
Iptables

- iptables-persistent
- iptables-apply –t 60 -c ./palomuuriskripti.sh
  - #!/bin/sh -e
  - iptables –F
  - iptables –X
  - iptables –j LOG
  - http://users.jyu.fi/~tusatenk/opetus/ties478/2017-kevat/myfw.txt



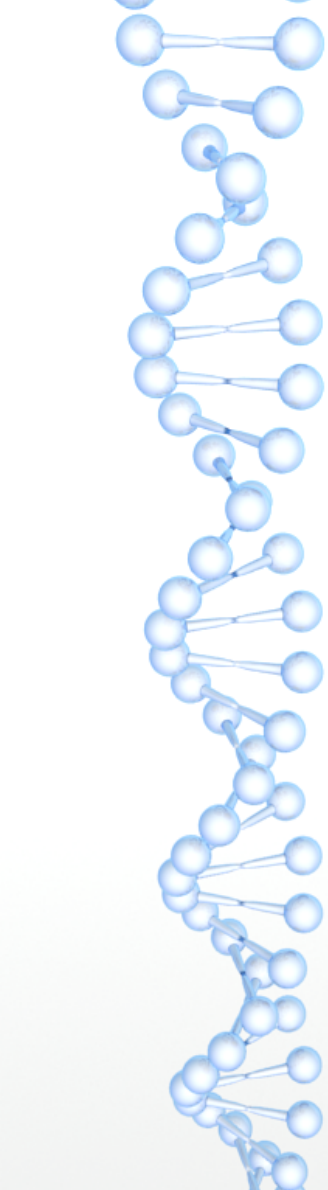
Tarkistettavia

- history
- alias, alias alias, .bashrc
- shellin vaihto
- tuntemattomat tiedostot: file



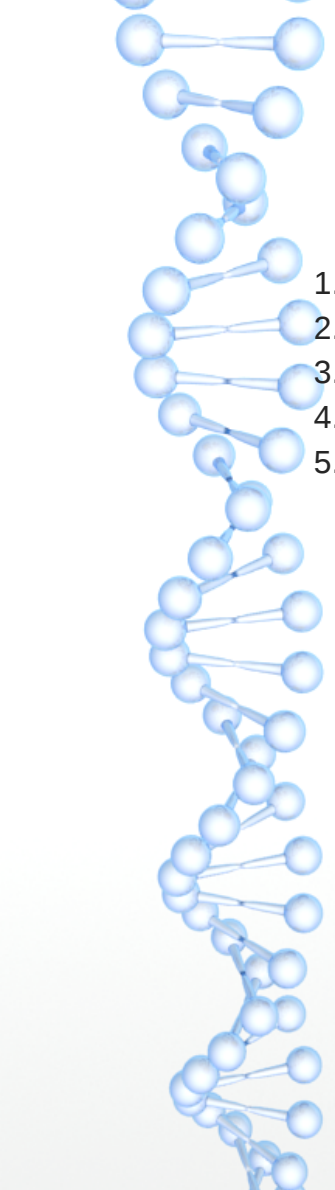
Reverse shell

- Tavallisesti: asiakas ottaa yhteyttä palvelimelle, jossa avataan shell. Komentoja ajetaan palvelimella
- Reverse shell: uhrikone ottaa yhteyttä palvelimeen ja lähettää oman shellin palvelimelle. Palvelimelta syötetyt komennot suoritetaan uhrikoneella
- Tavallisesti ulkoa palvelimille tulevat yhteydet helppo rajata, sisältä ulos huomattavasti vaikeampaa



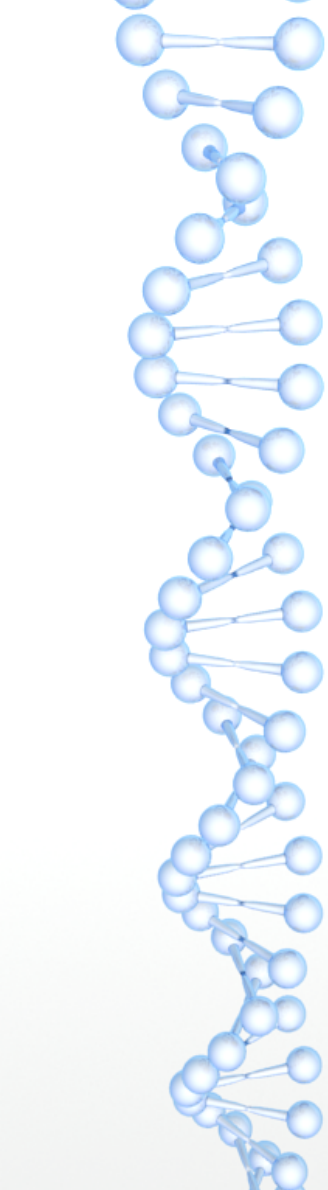
Tunnelointi

- Yhden protokollan mukaista liikennettä sijoitetaan toisen protokollan pakettien sisään
- esim. ssh -R 80:localhost:80 palvelin
  - avataan ssh-yhteys palvelimelle
  - ohjataan palvelimen porttiin 80 saapuva liikenne oman koneen porttiin 80
  - edellyttää käyttöoikeuksia palvelimelle ja konfigurointia siellä, privileged port käytännössä rootin oikeuksia
- DNS-tunnelointi
  - DNS-liikenteen sisällä kuljetetaan muuta liikennettä



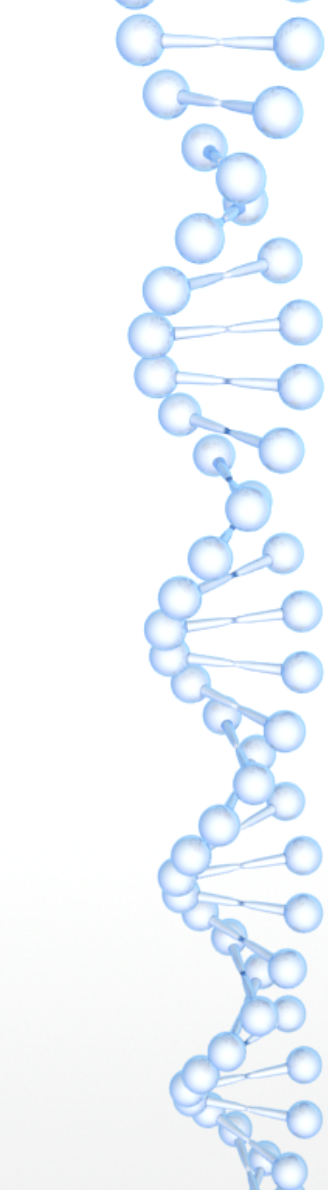
Lähteet

1. https://news.netcraft.com/archives/2017/10/26/october-2017-web-server-survey-13.html
2. https://secure1.securityspace.com/s_survey/data/man.201710/apacheos.html
3. https://www.vmware.com/solutions/virtualization.html
4. https://en.wikipedia.org/wiki/Secure_Shell
5. https://bash.cyberciti.biz/guide/What_is_Linux_Shell



Verkkoalueiden jaottelua

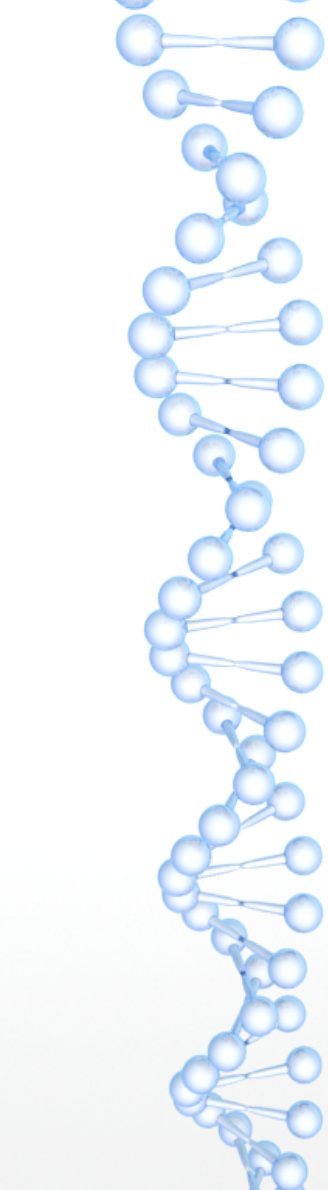
- Verkkoalueita ainakin
  - julkinen (internet)
  - dmz (julkiset palvelut: www, sähköposti, nimipalvelut, vpn)
  - sisäverkon palvelimet (levyt, tulostimet, tietokannat, nimipalvelut)
  - työasemat (kiinteät, liikkuvat)
- Erotetaan kytkimillä, reitittimillä, muureilla
- Hyvänä käytäntönä kaikki liikenne kielletään ja sallitaan vain tarpeelliset poikkeukset



Liikennesuuntia

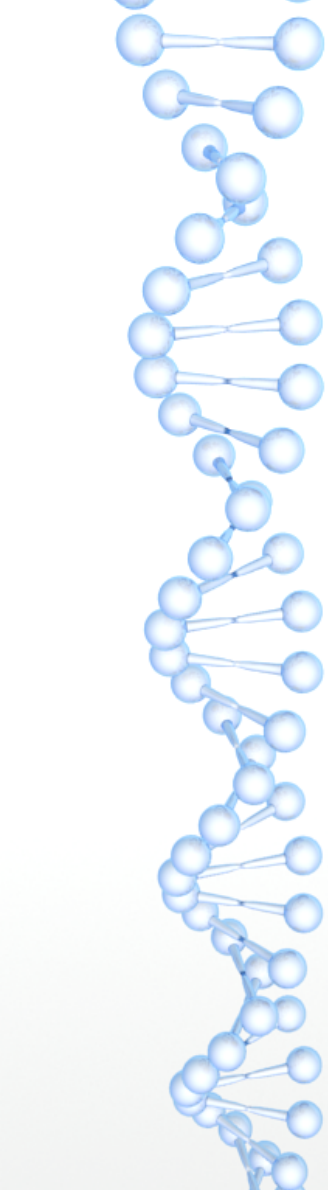
- Mistä on ok **avata** yhteyksiä mihinkin?
- Huomioi tavallinen käyttö vs ylläpito/hallinta

- internet <-> dmz
- internet <-> sisäverkon palvelimet
- internet <-> työasemat
- dmz <-> palvelimet
- dmz <-> työasemat
- dmz <-> dmz
- palvelimet <-> palvelimet
- palvelimet <-> työasemat
- työasemat <-> työasemat



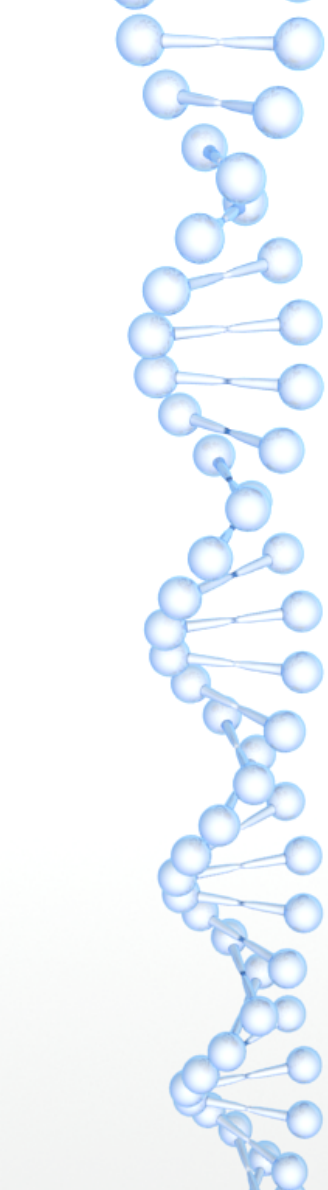
Palomuureista

- peruspolitiikka: lähtökohtaisesti kiellettään (tai sallitaan) kaikki
- säännöstö: poikkeukset politiikkaan
- paketit, yhteydet, yhteyksien sisältö
- palomuureissa usein myös IDS, VPN-palvelin
- mitä lokitetaan?
- mikä segmentti/palvelut minkäkin interfacen takana
- kurssilla käytössä PFSense reititinmuurina
  - web-käyttöliittymä
- palvelimet ja työasemat: host-muurit Microsoft & iptables



Julkisten palvelujen suojaaminen

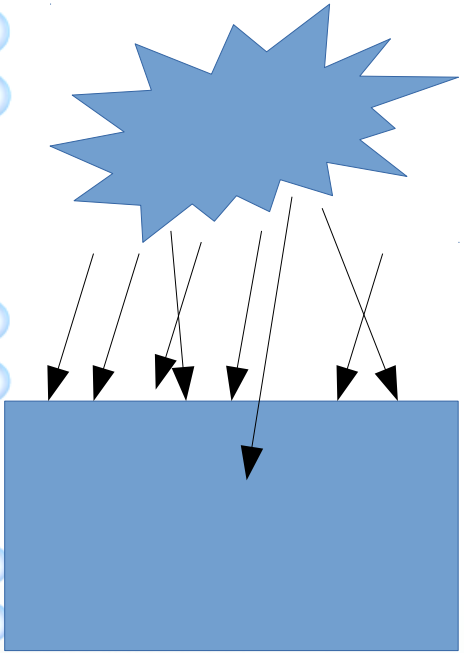
- Jotain on pakko paljastaa
- Useita palveluita, miten tarjotaan maailmalle?
  - erilliset palvelimet
    - yksi korkattu, muut suojassa?
  - yksi palvelin, jossa kaikki
    - helpompi hahmottaa, kaikki munat samassa korissa
  - erilliset palvelimet, joista palvelut tuodaan keskitetysti ulos
    - suojatumpi, mutta monimutkaisempi

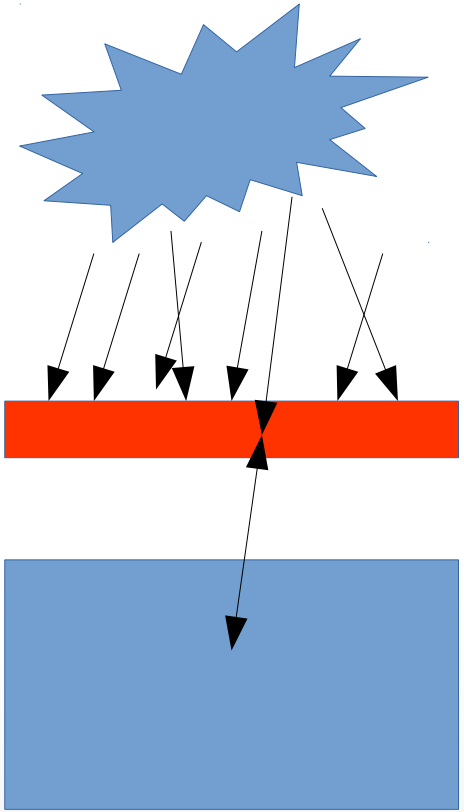


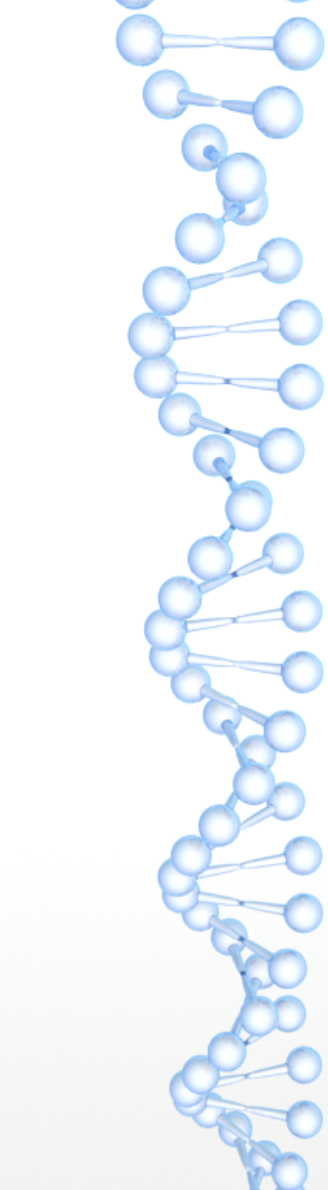
Port forwarding

- Palomuuri internetiin
- Palvelu, jota halutaan tarjota: ajetaan suojassa muurin takana, ei suoraa yhteyttä internetistä
- Ohjataan muurille ko. palvelua varten tullut liikenne palvelimelle ja vastaukset takaisin
- Palvelimesta paljastuu vain palvelun portti, ei koko palvelin

Sama kuvana







Tehtävä

- Tunnista käytön ja ylläpidon kannalta tarpeelliset palvelut ja niihin liittyvät liikenteen suunnat
- Suunnittele edellisen perusteella palomuurisäännöt
  - segmenttitasolla; IP-tasolla; palvelun/porttien tasolla
- Suunnittele ajan ja osaamisen puolesta toteutettavissa olevat verkkotason muutokset
- Suunnittele muut suojaukset
- Toteuta edelliset ja dokumentoi
- Raportti wikiin TI 1700 mennessä
- Valmistaudu esittämään oma ratkaisu KE 0815