Nimi:_____ Op.num:_____

Screen

Screen mahdollistaa terminaalisessioiden pitämisen elossa vaikka terminaaliyhteys olisi poikki.

1. Luo uusi sessio nimelle ”hakku”: *screen -S hakku*
2. Käynnistä tekstieditori luodussa sessiossa ja luo tiedosto hakku.txt
3. Katkaise yhteys sessioon: *CTRL-a d*
4. Luo toinen sessio nimelle ”kuokka” ja käynnistä sen sisään aptitude: *screen -S kuokka aptitude*
5. Listaa mitä screen-sessioita järjestelmässä on: *screen -ls*
6. Katkaise yhteys ”kuokkaan” ja liitä yhteys ”hakkuun”
7. Luo ”hakkuun” toinen ikkuna: *CTRL-a c*
8. Liitä ”kuokka” ”hakun” toiseen ikkunaan: *screen -r kuokka*
9. Sulje ”kuokasta” aptitude. Tällöin se screen sulkeutuu, koska sen viimeinen ikkuna poistui.

HUOM: älä avaa screenejä itsensä sisällä. Silmukat räjähtävät.

SSH

SSH on kryptografisesti suojattu terminaali-etäkäyttö-ohjelma.

1. Muodosta SSH-yhteys palvelimelle. Esimerkki: *ssh username@kosh.aalto.fi*
2. Nyt voit suorittaa terminaalikomentoja palvelimella paikallisen koneen sijaan.
3. SSH+Screen on äärimmäisen joustava työkalu yhdistämän terminaali-työskentely-sessiot koneelta toiselle siirtyessä.

SSH-asiakasohjelmia on useimmille alustoille:

- putty windowsilla
- openssh linux/unix/osx:llä
- JuiceSSH androidilla

SSH on pääasiallinen työkalu verkkopalvelimien säätämiseen.

Tiedostojen siirtäminen

SSH:n kylkiäisapuohjelmat sisältää tiedostojen siirtämisen:

- puttyllä pscp/psftp, linuxilla scp/sftp. GUI-softia filezilla, winscp.
- Siirrä tekstitiedosto linux-koneeltasi jollekin toiselle koneelle.
- Jos Linux-koneesi pyörii virtuaalikoneessa, siirrä tekstitiedosto isäntäkoneelle. Miltä tiedoston sisältö näyttää kun sen avaa isäntäkoneella? (esim notepad windowsilla)

Tunnelointi

SSH voi "tunneloida" graafisia sovelluksia. Tämä vaatii X11-palvelimen koneeltasi. Linuxissa X11 on mukana, MacOSX tarvii sen asentamisen lisäpakettina, Windows tarvitsee erillissoftan.

1. Muodosta ssh-yhteys käyttäen "-X" parametria. Esim. *ssh -X username@brute.aalto.fi*
2. Käynnistä graafinen sovellus: *xclock*
3. Ohjelma suoritetaan tällöin koneella johon otit yhteyden, mutta sen graafinen käyttöliittymä piirtyy omalle koneellesi SSH-tunnelin toiseen päähän.
4. Tämä toimii myös isommillekin sovelluksille: *matlab*
5. Siirtoyhteydestä aiheutuu jonkun verran yleisrasitetta toimintaan, että monimutkaisemmat/graafisemmat sovellukset eivät toimi erityisen hyvin.

SSH voi tunneloida myös geneerisesti TCP-yhteyksiä. TCP-tunneleita on kahta tyyppiä: paikalliset ja etäpään tunnelit.

- Paikalliset tunnelit tarkoittaa että SSH kuuntelee paikallista TCP-porttia ja välittää yhteyden etäpään kautta nimettyyn kohteeseen.
- Etäpääntunnelit toimivat päinvastoin; SSH kuuntelee etäpäässä TCP-porttia ja välittää yhteyden paikallisen koneen kautta nimettyyn kohteeseen.

Yksi käytännöllinen sovellus SSH-tunneleihin on kiertää palomuurirajoituksia. Esimerkki tällaisesta olisi käyttää jostain Aalto-yliopiston verkon ulkopuolelta Aallon wwwproxy.hut.fi palvelua Koshin kautta.

1. Tällöin tunneli muodostettaisiin seuraavasti: *ssh username@kosh.aalto.fi -L localhost:8080:wwwproxy.hut.fi:80*
2. Aseta tämän jälkeen webbiselaimesi proxy-asetukseksi: *localhost:8080* (firefox: preferences/advanced/network/
3. Vahvista toiminta vaikkapa `http://whatismyipaddress.com`

Julkisen avaimen autentikointi

SSH-yhteydet yksinkertaisimmillaan ovat salasanalla autentikoituja. Salasanan tietäminen vahvistaa että käyttäjä on kyseisen käyttäjätunnuksen omistaja. Julkisen avaimen autentikointimenetelmässä muodostetaan ns. julkinen avain ja ns. yksityinen avain. Yksityisen avaimen omistaminen vahvistaa käyttäjän identiteetin.

1. Suorita komento: *ssh-keygen -f testi*
2. Tämä luo "testi"-nimisen yksityisen avaimen, ja sitä vastaavan julkisen avaimen "testi.pub". Julkinen avain voidaan vapaasti kopioida palvelimelle (sen tietäminen ei auta mahdollisia hakkereita varastamaan tunnuksiasi).
3. Tämän voi tehdä joko manuaalisesti kopioimalla "testi.pub" palvelimella kotihakemistoosi ".ssh/authorized_ho tiedostoon. Tai automaattisesti komennolla: *ssh-copy-id -i testi username@palvelin*
4. Nyt voit kirjautua ilman salasanaa: *ssh -i testi username@palvelin*

Jos et käytä "-f" parametria niin julkinen avain luodaan profiiliisi oletusavaimeksi ja sitä käytetään automaattisesti (ilmankin "-i" parametria).
Julkisen avaimen menetelmiä käytetään usein myös mahdollistamaan automaattiset ylläpitotoimet ssh-yhteyksiä käyttäen; palvelinohjelmisto käyttää ssh-avainta ottaakseen yhteydet. Ei tarvita ihmistä tekemään jokaikistä asiaa.

Verkkodiagnostiikat

Ethernet/WirelessLAN-verkoissa toimintamalli on että "naapurit", eli samassa segmentissä ja subnetissä olijat, ovat suoraan saavutettavissa. Pääsy muuhun verkkoon tapahtuu "gateway" noodin läpi. Gateway on reititin, joka viestittelee muiden reitittimien kanssa kunnes viesti saadaan perille.

Ping-komento

1. Selvitä *ip addr* komennolla oma osoitteesi. Vastaako tämä pingiin?
2. Selvitä *ip route* komennolla gatewaysi. Vastaako tämä pingiin?
3. Selvitä "www.aalto.fi" palvelimen osoite nslookup -komennolla.
4. Testaa vastaako "www.aalto.fi" ping komentoon. Mikä on keskimääräinen vasteaika (rtt avg)? Onko tuloksesi sama kuin muilla?

Pää pyörällä IP-osoitteiden ja subnettien kanssa? Numerojen pyörittämiseen on näppärä apuohjelma nimeltä *ipcalc*. Asenna tämä (*apt-get install ipcalc*). Poimi *ip addr* komennon tulosteesta IPv4 osoitteesi (inet -sanan jälkeen "x.x.x.x/x") ja syötä tämä tyyliin *ipcalc x.x.x.x/x*.

Reitinselvitys

1. Millaisen näkymän antaa *traceroute www.google.fi*? Entä *traceroute www.aalto.fi*?
2. Kokeile *mtr* komentoa samoille kohteille.

Liikenteen dumppaaminen

Seuraavat vaativat ylimääräisiä oikeuksia, joten suorita komennot joko roottina tai sudo-komennon avulla.

1. Samalla kun suoritat yhdessä ikkunassa ping-komentoa, aja toisessa ikkunassa *sudo tcpdump -i verkkolaite icmp* (missä verkkolaite on käyttämäsi laite)
2. Suorita *sudo tcpdump -i verkkolaite tcp port 80* ja lataa joku http:tä käyttävä webbisivu, esimerkiksi `http://www.aalto.fi/` (https käyttää eri porttia).

Wireshark on graafinen työkalu, joka voi dumpata liikennetta ja tarkastella sen sisältöä. Näiden työkalujen käytöstä lisää *ELEC-C7240 Internet-tekniikat*.