Linux-harjoitus 8

Harjoituksessa tutustutaan Linuxin palomuuriominaisuuksiin sekä hieman testataan Linuxin turvallisuutta.

Palomuurit

Palomuurilla (firewall) rajoitetaan liikennettä koneeseen sekä myöskin tarvittaessa koneelta internetiin. Nykyisin tavanomaisin Linuxin palomuuriratkaisu on *iptables*.

Iptables-määrityksillä luodaan säännöt sille, mitä liikennettä päästetään sisään koneeseen. Jos ei tarvita mitään ulkopuolisia palveluja, voidaan *iptables*:lla sulkea kaikki yhteydet koneeseen päin. Pääsääntö on aina, että vain ne palvelut (portit) avataan, mitä tarvitaan. Kaikki muu on oletusarvoisesti kiinni.

Tarkempaa tietoa iptables:sta saat mm. seuraavista osoitteista:

http://users.tkk.fi/~tkarvine/firewall-iptables.html, yksinkertainen peruspalomuuriskripti
http://www.oulu.fi/atkk/tietoturva/sisalto/yllapito/linux/linux_suojautuminen.html, toinen vastaava, suomeksi selitetty.
http://iptables-tutorial.frozentux.net/iptables-tutorial.html, iptables-tutorial
http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html, howto-dokumentti

Vanhempi Linuxin palomuuriohjelma oli *ipchains*. Siitäkin näyttää vielä olevan paljon dokumentaatiota netissä, mutta sen käyttö nyky-kerneleillä ei enää ole mielekästä.

Yksinkertainen palomuuri

Iptables-palomuurin kolme perusketjua ovat INPUT, FORWARD sekä OUTPUT. Näistä ensimmäinen käsittelee sisääntulevaa liikennettä, seuraava edelleenohjausta ja viimeinen ulosmenevää liikennettä.

Palomuurille hyvä lähtökohta on seuraava:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

Ensimmäisellä ja toisella rivillä määritellään, että kaikki liikenne sisään ja eteenpäin estetään. Yleensä on järkevää nollata kaikki vanhat säännöt, sillä ketjun idea on, että sen perään lisätään uusia sääntöjä. Ks. esimerkiksi ensimmäisestä linkistä, miten tarkalleen ottaen menetellään.

Kuitenkin jotakin pitää sallia, kuten esim. loopback-osoitteen toiminta:

```
iptables -A INPUT -i lo --source 127.0.0.1 --destination 127.0.0.1 -j
ACCEPT
iptables -A INPUT -m state --state "ESTABLISHED,RELATED" -j ACCEPT
```

Sallitaan lisäksi ssh-yhteydet sisään:

```
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

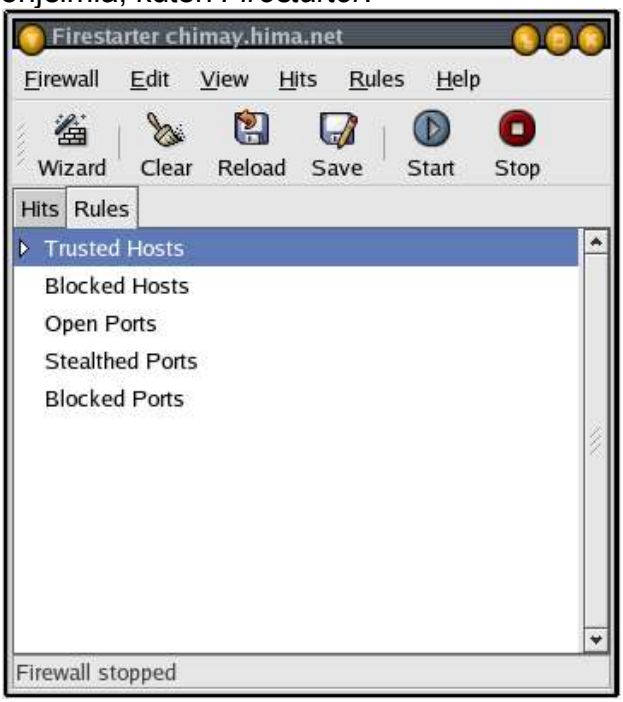
Harjoituksia

1. Selvitä, mitä tarkoittavat *iptables*-ohjelman optiot -A ja -P?
2. Mitä tekee komento *iptables -L INPUT*? Entä FORWARD tai OUTPUT?
3. Avaa koneesi ssh-, http- ja https-portit sisääntulevaa liikennettä varten. Testaa että nämä toimivat.

Muut palomuuriohjelmat

Iptables-palomuurille on olemassa useita erilaisia graafisia front-end-ohjelmia. Fedoran oma on nimeltään Security level:

Tämä on varsin kevyt ohjelma, kuten näkyy. Itse asiassa tämän käyttäminen ei muutenkaan ole mielekästä, kun on olemassa paljon parempia ja monipuolisempia ohjelmia, kuten *Firestarter*:



Tällä ohjelmalla voikin tehdä paljon monipuolisempia palomuurisäätöjä kuin Fedoran omalla työkalulla. *Firestarterin* pitäisi nykyisin kuulua jo suoraan Fedora Core-jakeluun, mutta sen löytää myös *Firestarterin* omilta sivuilta osoitteesta *http://www.fs-security.com/*.

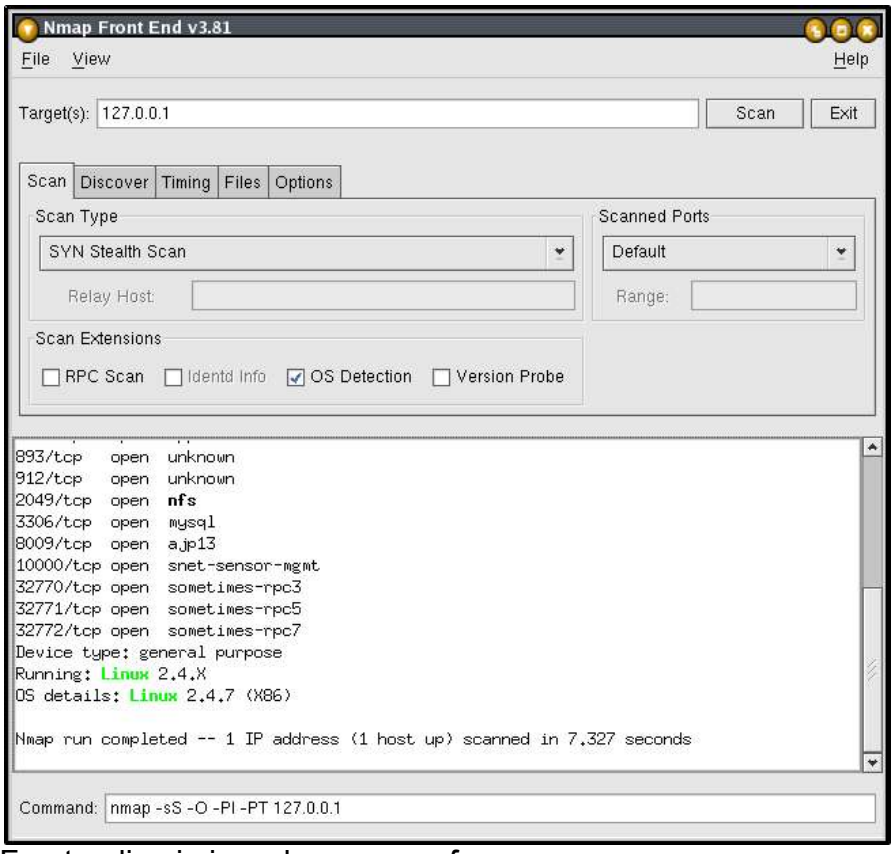
HUOM!: erilaisia tapoja säätää palomuuria ei pidä käyttää sekaisin! Näillä on taipumus on sotkea toistensa sääntöjä.

Harjoituksia, osa 2:

4. Varmista Firestarterin uusin versio ja asenna se koneeseesi.
5. Aja Firestarterin wizard-toiminto. Valitse avattaviksi porteiksi ainakin ssh, http, https, sekä nfs.
6. Tarkista nyt iptables-komennolla, miten palomuurisäännöt muuttuivat.
7. Tutustu Firestarterin mahdollisuuksiin tehdä omia määrityksiä. Määritä nyt koko 172.16.1.x-verkko turvallisiksi yhteyksiksi.
8. Voiko Firestarterilla toteuttaa porttien edelleenohjauksia? Jos voi, miten?

Yhteyksien testaaminen

Pelkkään palomuuriin ei kannata luottaa. Yhteyksien turvallisuutta tulee myös tarvittaessa testata. Yksi tällainen ohjelma testaamiseen on *nmap*. Nmap tulee jakeluiden mukana, joten sitä ei tarvitse muualta latailla. Korkeintaan *nmap*:n graafinen front-end saattaa puuttua. *Nmap*:n kotisivut ovat kuitenkin osoitteessa *http://www.insecure.org/nmap/*. Front-end näyttää tältä:



Frontendin nimi on yleens *nmapfe*.

Harjoituksia, osa 3

9. Varmista, että koneeseesi on asennettu nmap ja testaa localhost:n (127.0.0.1), mitä kaikkea on auki koneesta.

10. Testaa kaverisi koneen aukot (taikka serverin 172.16.1.2).

11. Saatko oletus-gateway:stä (172.16.1.1) mitään tietoa irti?

Huomautus lopuksi

Vaikka *nmap* onkin tehokas työkalu avoimien porttien ym. turva-aukkojen testaamiseen, ei sillä ole tarkoitus eikä syytä lähteä mitään suurisuuntaisempaa porttiskannailua tekemään. Se katsotaan yleensä nettiliikenteen häirinnäksi.