Linux-harjoitus, palomuurit

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://linux.fi/index.php/Palomuuri, Linux.fi-Wikin perusteet palomuureista.
http://users.tkk.fi/~tkarvine/firewall-iptables.html, yksinkertainen peruspalomuuriskripti
http://iptables-tutorial.frozentux.net/iptables-tutorial.html, iptables-tutorial

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

Tehtäväosion palautettavat tehtävät ovat sivulla 2.

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
iptables -P OUTPUT ACCEPT
```

Ensimmäisellä ja toisella rivillä määritellään, että kaikki liikenne sisään ja eteenpäin estetään. Viimeisellä rivillä sallitaan kaikki ulosmenevä liikenne. Yleensä on järkevää nollata kaikki vanhat säännöt, sillä ketjun idea on, että sen perään lisätään uusia sääntöjä.

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

```
iptables -A INPUT -i lo -j ACCEPT
```

Lähiverkon kaikki liikenne voidaan sallia:

```
iptables -A INPUT -s 192.168.0.0/255.255.255.0 -j ACCEPT
```

Sallitaan lisäksi ssh-yhteydet sisään:

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

Harjoituksia

Toteuta tehtävissä olevat palomuurimääritykset koneellesi (palvelin). Palauta tehtävien vastaukset osoitteeseen *ilpo.kuivanen@stadia.fi*. Laita otsikoksi ”**Palomuuritehtävät**”.

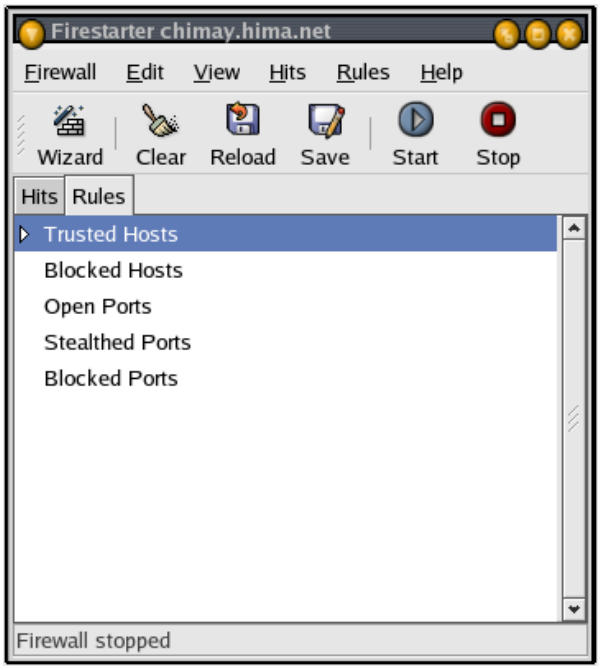
Huom! Vain nämä tehtävät palautetaan, muita tässä dokumentissa olevia ei tarvitse palauttaa!

1. Selvitä, mitä tarkoittavat *iptables*-ohjelman optiot -A ja -P?
2. Kuinka palomuurisäännöt talletetaan?
3. Mitä tekee komento *iptables -L INPUT*? Entä FORWARD tai OUTPUT?
4. Aloita palomuurin toteutus estämällä kaikki liikenne sisään ja sallimalla ulos. Kokeile sen jälkeen Windows-koneelta yhteyttä joko www-selaimella (jos on Apache päällä) taikka ssh-clientillä.
5. Salli kaikki liikenne 172.16.1.0-verkossa.
6. Avaa nyt ssh ja http siten, että myös Windows-koneilta pääsee näille. Tee sama myös samballe, jotta voit käyttää Linux-koneelle aiemmassa tehtävässä määrittämääsi levyjakoa Windows-koneelta.
7. Jos olet asentanut koneeseesi Webmin-hallintaohjelman, avaa myös portti 10000 Webminin käyttöä varten.

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. Itse asiassa varsin usein nämä laittavat omat määrittelynsä omiin tiedostoihinsa ja liittävät nämä tiedostot sitten iptables-määrityksiin.

Harjoituksia, osa 2:

8. Varmista Firestarterin uusin versio ja asenna se koneeseesi.

9. Aja Firestarterin wizard-toiminto. Valitse avattaviksi porteiksi ainakin ssh, http, https, sekä nfs.

10. Tarkista nyt iptables-komennolla, miten palomuurisäännöt muuttuivat.

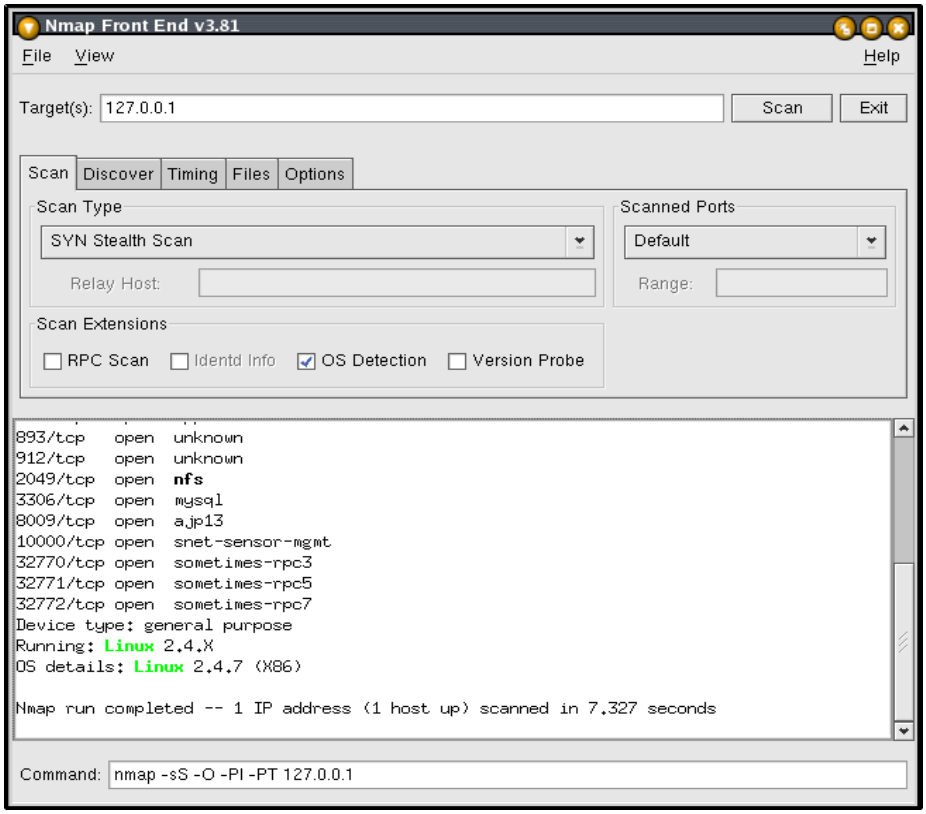
11. Tutustu Firestarterin mahdollisuuksiin tehdä omia määrityksiä. Määritä nyt koko 172.16.1.x-verkko turvallisiksi yhteyksiksi.

12. 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 yleensä *nmapfe*.



Harjoituksia, osa 3

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

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

15. 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.