Lauri Partinen ktkt23sp

# Stateless Firewall

Tehtävä
Opintojakson nimi Kirjasinkoko 16

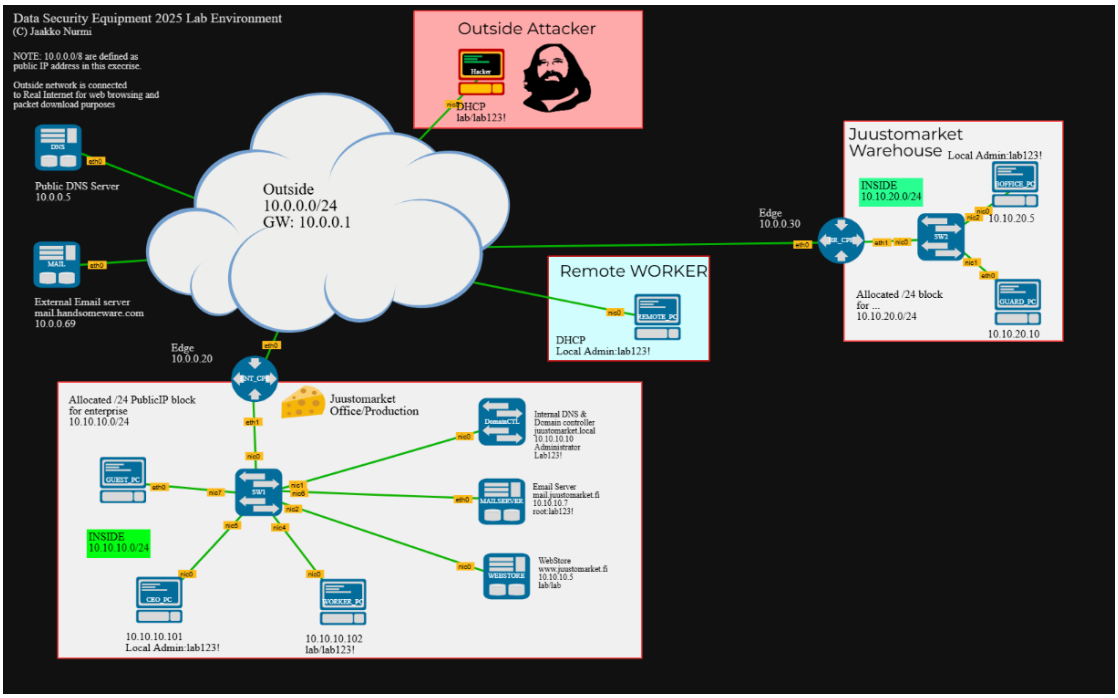
2025

Kaakkois-Suomen
ammattikorkeakoulu

**SISÄLLYS**

# 1 STATELESS FIREWALL TEHTÄVÄ

Kuvassa on ympäristö, johon palomuurisääntöjä sovelletaan. Tehtävän suorittamiseen tarvitaan ent_cpe:tä ja worker_pc:tä. Worker_pc käytetään esimerkiksi porttien tai toimintojen testaamiseen käytännössä. Kaikki palomuurisäännöt lisätään ENT_CPE terminaalia käyttäen.




Avataan ENT_CDP, johon teemme kaikki palomuurisäännöt. Ennen palomuurisääntöjen kirjoittamisen aloittamista lisää komennot:

#eth0 = OUTSIDE
#eth1 = INSIDE

#removes all rules
iptables -F

#Drop all packet coming from outside
iptables -A FORWARD -i eth0 -j DROP

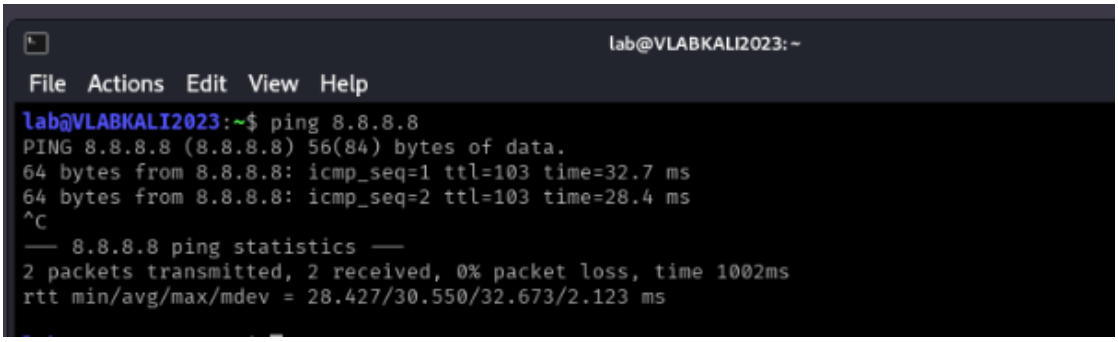
#Drop all packet coming from inside
iptables -A FORWARD -i eth1 -j DROP

### 1.1 Ensimmäiseksi sallitaan ICMP-liikenne sisältä ulospäin.

Avataan ENT_CDP , johon syötetään komennot. Komennoissa sallitaan ICMP-liikenne porteista eth0 ja eth1.

```
#Allow ICMP In->OUT
iptables -A FORWARD -i eth0 -p ICMP --icmp-type=0 -j ACCEPT
iptables -A FORWARD -i eth1 -p ICMP --icmp-type=8 -j ACCEPT
```

Käytännön testaaminen tapahtuu avaamalla ympäristöstä WORKER_PC, josta avataan terminal. Testataan ICMP-liikenteen toimivuus pingaamalla osoitetta 8.8.8.8 .




ICMP-liikenteen salliminen mahdollistaa ping-komennon käytön, jolla voidaan testata verkkoyhteyksiä ja yhteyksiä laitteiden välillä.  Sääntö varmistaa, että sisäverkon käyttäjät voivat tarkistaa ulkoisten palveluiden saatavuuden, josta on hyötyä organisaation toiminnassa.

Turvallisuusriski: ICMP-tunnelointi voi mahdollistaa tietovuotoja tai palomuurin ohituksen, jos valvonta ei ole asiallista.

Vaihtoehtoinen keino voisi olla rajoittaa ICMP käyttö vain tiettyihin IP-osoitteisiin.

### 1.2 Estetään ICMP-liikenne sisäänpäin

Säännön puuttuminen voi johtaa ulkopuolisten käyttäjien ICMP-pyyntöihin sisäverkkoon, mikä altistaa sen mahdolliselle verkkotiedostelulle.

Turvallisuusriski: ICMP-echo pyynnöt voivat auttaa hyökkääjää tutkimaan verkkoa ja mitkä palvelimet ovat käytössä.

Parannuskeinoja: Ulkoiset ICMP-viestit tulisi estää kokonaan tai rajoittaa.

### 1.3 Salli ulkoinen pääsy WebStore-palveluun http://10.10.10.5

Ensin tehdään palomuuri sääntö http ja https liikenteelle.
Palomuurisäännössä avataan tulo ja vastaanotto portit 80 ja 433, jotta webstoreen pääse sisään.

```
#Allow http ja https outside

iptables -A FORWARD -i eth0 -d 10.10.10.5 -p TCP --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -d 10.10.10.5 -p TCP --dport 443 -j ACCEPT

#Allow return of http
iptables -A FORWARD -i eth1 -s 10.10.10.5 -p TCP --sport 80 -j ACCEPT
iptables -A FORWARD -i eth1 -s 10.10.10.5 -p TCP --sport 443 -j ACCEPT
```

Katsotaan nmap 10.10.10.5 komennon avulla ovat portit 80 ja 433 auki.

```
lab@VLABKALI2023:~$ nmap 10.10.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 00:38 EET
Nmap scan report for 10.10.10.5
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:57:D4:0A:15:10 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Verkkokauppa on liiketoiminnan kannalta kriittinen palvelu, joten http/https protokollien tulisi olla saavutettavissa julkisesti.

Turvallisuusriski: Julkinen pääsy lisää hyökkäysrajapintaa esimerkiksi palvelunestohyökkäykset.

Toiminallinen vaikutus yritykselle: Jos palomuurisääntöä ei olisi asiakkaat eivät voisi käyttää verkkokauppa, joka vaikuttaa liiketoimintaan.

Vaihtoehtoinen toteutus voisi olla vain vahvistettujen käyttäjien sisäänpääsy.

Toteutusta voisi parantaa ottamalla käyttöön Web application firewallin, joka suodattaa haitallisia http-pyyntöjä.

### 1.4 Salli verkon selaus sisäverkosta

Komennoilla sallitaan verkon selaus verkon sisältä. Komennoissa avataan 80 ja 433 portit molempiin suuntiin. Verkon selaus vaatii dns palomuurisäännöt, jotka lisätään myöhemmin.

```
#ALLOW web browsing in -> out

iptables -A FORWARD -i eth1 -s 10.10.10.0/24 -p TCP --dport 80 -j
ACCEPT
iptables -A FORWARD -i eth1 -s 10.10.10.0/24 -p TCP --dport 443 -j
 ACCEPT

#ALLOW web browsing out -> in

iptables -A FORWARD -i eth0 -d 10.10.10.0/24 -p TCP --sport 80 -j
ACCEPT

iptables -A FORWARD -i eth0 -d 10.10.10.0/24 -p TCP --sport 443 -j
ACCEPT
```

Seuraavaksi laitetaan dns toimimaan kuvan komennoilla. Komennossa avataan portti 53 liikenteelle.

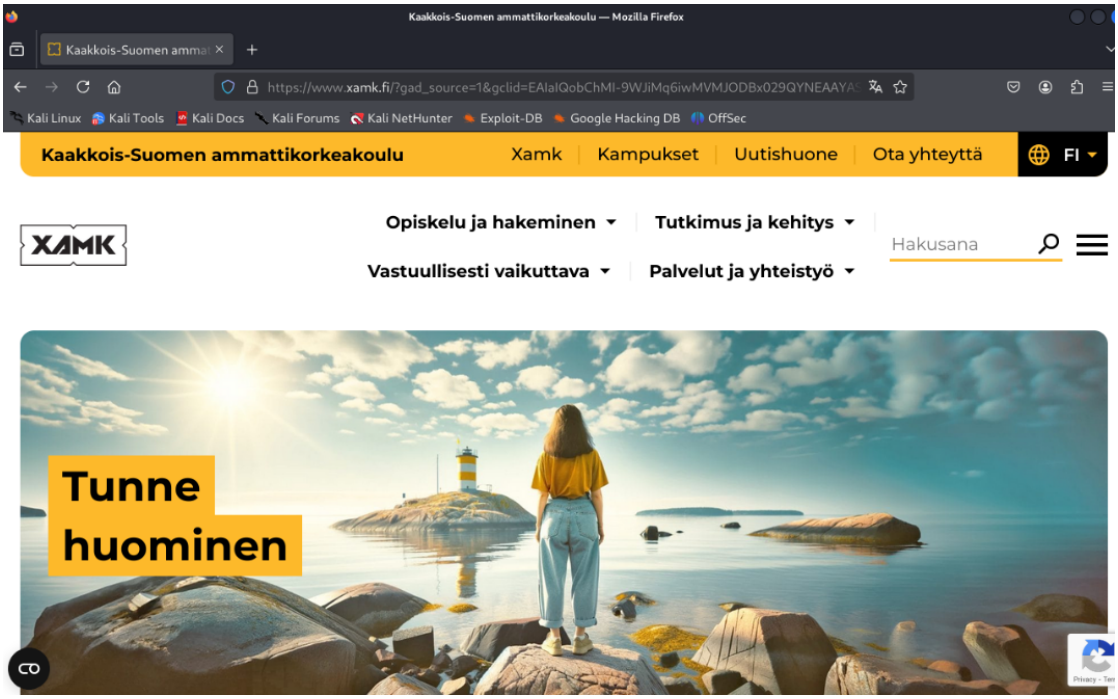
```
#allow DNS in -> out
iptables -A FORWARD -i eth1 -p UDP --dport 53 -j ACCEPT

#allow dns return out -> inside
iptables -A FORWARD -i eth0 -p UDP --sport 53 -j ACCEPT
```

Avataan HACKER tietokone ja avataan terminaali. Testataan dns toimivuus pingaamalla google.fi osoitetta.

```
lab@VLABKALI2023:~$ ping google.fi
PING google.fi (142.250.74.67) 56(84) bytes of data.
64 bytes from arn09s23-in-f3.1e100.net (142.250.74.67): icmp_seq=1 ttl=107 time=19.9 ms
64 bytes from arn09s23-in-f3.1e100.net (142.250.74.67): icmp_seq=2 ttl=107 time=19.7 ms
^C
--- google.fi ping statistics ---
```

Testataan, toimiiko internetin selaus. Kuvassa esimerkki sivusto xamk.fi.




Palomuurisääntö on välttämätön työntekijöiden työn kannalta, sillä ilman sääntöä internetin käyttö ei olisi mahdollista.

Turvallisuusriski: Haitalliset verkkosivustot ja haittaohjelmat.

Vaihtoehtoisena ratkaisuna voisi olla rajoittaa verkkoselaus vain hyväksyttyihin verkkosivustoihin, joka vähentäisi mahdollisuutta mennä haitallisille verkkosivuille.

## 1.5 Mysql-yhteyden salliminen varastoverkosta

Tämä sääntö sallii verkosta, jossa MySQL -palvelin on 10.10.20.0/24 tulevan TCP-liikenteen portista 3306 Warehouse verkkoon, 10.10.10.0/24 palomuurin läpi.

```
#Allow Mysql accessible from Warehouse

iptables -A FORWARD -i eth1 -p TCP -d 10.10.20.0/24 -s 10.10.10.0/24 --sport 3306 -j ACCEPT
iptables -A FORWARD -i eth0 -p TCP -d 10.10.10.0/24 -s 10.10.20.0/24 --dport 3306 -j ACCEPT
```

Varastojärjestelmät tarvitsevat reaaliaikaisen pääsyn MySQL-tietokantaan tilausten käsittelyyn ja varastoseurantaan. Ilman tätä sääntöä varastonhallinta viivästyisi, mikä voisi vaikuttaa toimituksiin.

Turvallisuus: Varmista, että MySQL-palvelin on suojattu vahvoilla salasanoilla ja käyttöoikeuksilla.

Vaihtoehtoinen ratkaisu voisi käytää IP-whitelisting toimintoa, jotta vain hyväksytyt järjestelmät voivat muodostaa yhteyden MySQL-palvelimeen.

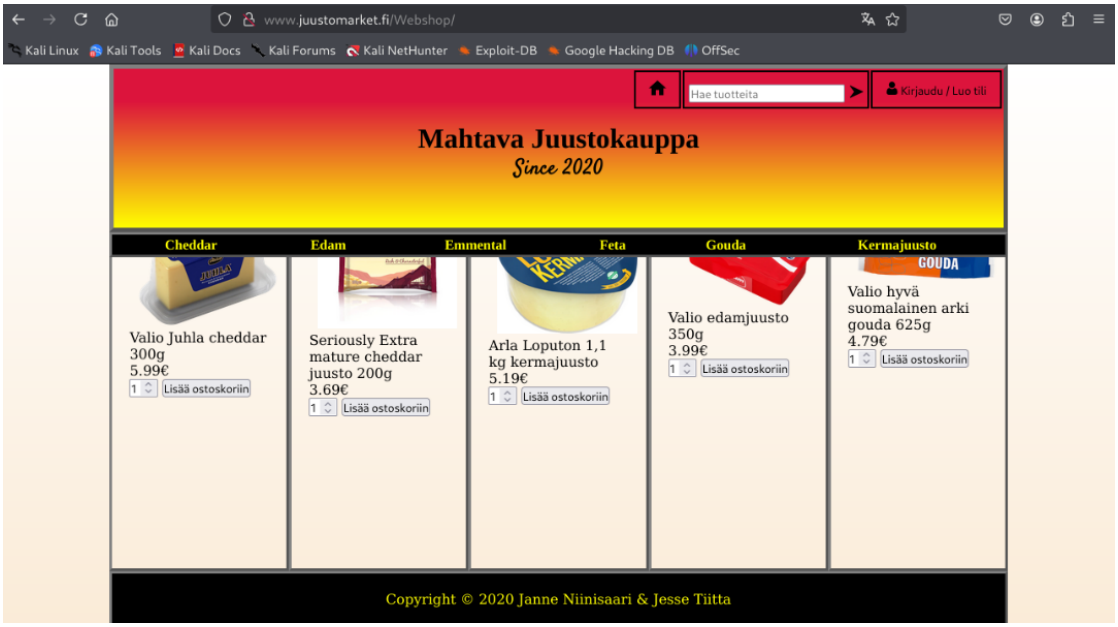
Verkkotietokantayhteydet ovat kriittinen hyökkäyskohde, ja väärin suojattu yhteys voi mahdollistaa SQL-injektiot tai tietomurrot.

### 1.6 Verkkoselailun salliminen warehouse verkosta

Sääntö sallii http- ja https-liikenteen warehouse verkosta verkkosivustolle avaamalla portin 80.

```
#ALLOW Access to webstore
#out->in
iptables -A FORWARD -i eth1 -d 10.10.20.0/24 -s 10.10.10.10 -p TCP --sport 80 -j ACCEPT
#in->out
iptables -A FORWARD -i eth0 -d 10.10.10.10 -s 10.10.20.0/24 -p TCP --dport 80 -j ACCEPT
```

Testataan toiminta. Avaa WORKER_PC ja kirjoita selaimen hakukenttään http://www.juustomarket.fi.




Verkkoselailuun liittyy turvallisuusrikejä, joten suojattu ja päivitetty selain on tärkeää.

Vaihtoehtoisena ratkaisuna voisi käyttää sisällönsuodatinta, mikä estää pääsyn haitallisille sivustoille.

### 1.7 Sisäisen DNS:n käyttö warehouse verkosta

Palomuurisäännön avulla pystytään sallimaan DNS-kyselyt warehouse verkosta DNS-palvelimelle.

```
#Allow internal dns
iptables -A FORWARD -i eth1 -d 10.10.20.0/24 -s 10.10.10.10 -p UDP --sport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -d 10.10.10.10 -s 10.10.20.0/24 -p UDP --dport 53 -j ACCEPT
```

Sisäisen dns-palvelimen käyttö voi olla turvallisuusriski, joten dns-palvelin tulisi olla suojattu ja käyttöoikeus vain sallituilla käyttäjillä.

Vaihtoehtoisena ratkaisuna voitaisiin käyttää julkista dns-palvelinta esimerkiksi Cloudfare DNS.

## 2 REFLEKTIO

Tehtävässä opin perusteita palomuurisääntöjen luomisesta. Tehtävän aikana sain selville konkreettisesti, miten eri säännöt toimivat testaamalla esimerkiksi menikö portti päälle palomuurisäännön seurauksena nmap-hyödyntäen. Eikä vain kirjoittaa sääntöjä tietämättä, mitä ne oikeasti tekevät. Vaikka en saanut tehtävää tehtyä loppuun onnistuneesti. Tehtävästä jäi asian tiimoilta paljon uutta asiaa. Tulevaisuudessa sääntöjen harjoittelusta tulee olemaan hyötyä, joten on tärkeää ymmärtää niiden toiminta. Seuraavissa tehtävissä pyrin pyytämään apua, jos jään jumiin ongelman kanssa.