

h4

x) Ekat stepit omalla virtuaalipalvelimella

Ensimmäisellä kerralla kun etäpalvelimen ottaa käyttöön täytyy sinne kirjautua ssh-yhteydellä rootkäyttäjällä.

Rootkäyttäjällä kannattaa päivittää paketit `sudo apt-get update` ja sen jälkeen asentaa tulimuuri `sudo apt-get install ufw`

Tulimuuriin kannattaa tehdä reikä porttiin 22/tcp jotta voidaan koneeseen ottaa yhteys ssh:lla

Kun reikä tulimuuriin on tehty kannattaa tulimuuri laittaa päälle komennolla `sudo ufw enable`

Tämän jälkeen pitää lisätä joku käyttäjätunnus, jotta root-tunnuksella ei tarvitse konetta hallita.

Komennolla `sudo adduser` lisätään käyttäjä ja uudella käyttäjätunnuksella kannattaa kokeilla ssh-yhteys.

Uudelle käyttäjätunnukselle pitää antaa sudo oikeudet ja kunhan sudo oikeudet on testattu, kannattaa root käyttäjä laittaa lukkoon `sudo usermod -s /bin/bash root`

Name based virtual hosts



Jos käytössä on vain yksi palvelin voidaan samalle ip-osoitteelle osoittaa monta eri domain-nimejä. Tämä mahdollistaa sen, että yhdellä palvelimella voidaan pyörittää monta eri nettisivua, joilla on kaikilla eri domain nimi.

a)

Tein Linoden palveluun oman virtuaalipalvelimen ja tein ensimmäiset stepit palvelimelle samalla tavalla kuin ensimmäisessä tehtävässä on kerrottu.

Vuokrasin namecheap sivulta Widercrantz.com osoitteen.

Laitoin widercrantz.com osoitteen osoittamaan palvelimeeni.

<input type="checkbox"/> Type	Host	Value	TTL	
<input type="checkbox"/> A Record	@	172.104.228.59	Automatic	
 ADD NEW RECORD				

d)

palvelin kannattaa suojata tulimuurilla. Lähtökohtaisesti kannattaa kaikki sisään tuleva liikenne estää ja kaikki ulos lähtevä sallia. Sisään tulevaa liikennettä voi avata tarpeen mukaan.

Tässä tapauksessa avasin tulimuurista portin 22 SSH-yhteyttä varten.

Avasin portin komennolla `sudo ufw allow 22/tcp`

Sen jälkeen laitoin vasta tulimuurin päälle komennolla `sudo ufw enable`

Möhemmin tehtävässä e) avasin vielä tulimuurista portin 80 http-liikennettä varten

e)

Asensin webbi palvelimen komennolla `sudo apt-get install apache2`

Kokeilin tehdä reiän tulimuriin porttiin 80 http-liikennettä varten

Komennolla `sudo ufw allow 80/tcp`

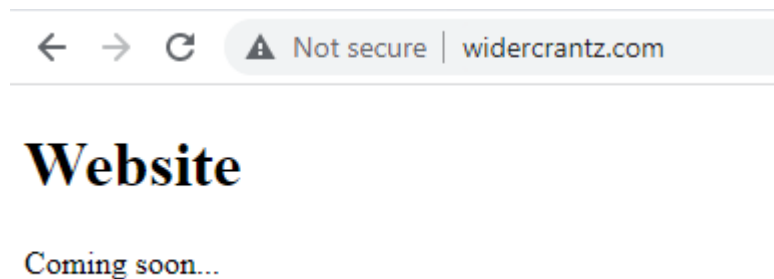
Kokeilin ip-osoitteella ja widercrantz.com haulla selaimeen ja apachen default sivu näkyy

Suljin tulimuurilla liikenteen porttiin 80 sen ajaksi, että teen säätöjä.

Vaihdoin apachen default sivun osoitteesta `var/www/html`

Avasin uudelleen portin 80

Testasin selaimella ja nyt näkyy uusi sivu



f)

`Sudo apt-get update` – kaikki ajantasalla

g)

Kuten lokeista huomaa palvelimeeni on yritetty kirjautua usealla eri käyttäjätunnuksella virheellisesti. Hyökkääjä on kokeillut luultavasti erilaisia helppoja default tunnuksia ja salasanoja. Palvelimeen on yritetty kirjautua esimerkiksi tunnuksella testuser. Hyökkäykset ovat tulleet kaikki samasta ip-osoitteesta mutta hyökkääjä on kokeillut useita eri portteja, sekä käyttäjätunnuksia.

```
Sep 21 12:47:24 localhost sshd[7554]: Failed password for root from 43.143.82.193 port 37730 ssh2
Sep 21 12:47:24 localhost sshd[7556]: Failed password for invalid user testuser from 43.143.82.193 port 37692 ssh2
Sep 21 12:47:25 localhost sshd[7527]: Failed password for root from 43.143.82.193 port 37714 ssh2
Sep 21 12:47:25 localhost sshd[7534]: Failed password for root from 43.143.82.193 port 37686 ssh2
Sep 21 12:47:25 localhost sshd[7531]: Failed password for invalid user ubuntu from 43.143.82.193 port 37670 ssh2
Sep 21 12:47:25 localhost sshd[7530]: Failed password for invalid user es from 43.143.82.193 port 37682 ssh2
Sep 21 12:47:25 localhost sshd[7528]: Failed password for invalid user git from 43.143.82.193 port 37688 ssh2
Sep 21 12:47:25 localhost sshd[7547]: Failed password for root from 43.143.82.193 port 37710 ssh2
```

