iptables - block ipnummer

iptables is de (software) firewall van (o.m.) CentOS. In dit stukje leer je hoe je ipnummers kunt blokkeren met iptables.

Check op invalid logins. Meestal ssh

```
sudo grep failed /var/log/audit/audit.log* | grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | sort | uniq -c
```

Dit laat een lijstje zien van ip nummers waarvandaan failed login's zijn geregstreerd. Het getal voor het ip nummer is het aantal keren dat er een failed login heeft plaatsgevonden.

Stel ipnummer 45.119.53.58 komt meer dan 1000 keer voor. Dan kun je eerst proberen op te zoeken waar dit nummer vandaan komt. Daar zijn verschillende sites (bijvoorbeeld http://whois.domaintools.com) voor en je kunt zelf ook databases downloaden. In dit geval komt dit nummer uit China.

Nu kun je dit ipnummer blokkeren. Beter nog is om heel het netwerk te blokeren. Meestal kun je als subnetmask /24 nemen daarmee blokkeer je 256 ip adressen. In dit geval blokkeer je dan 45.119.53.*

Je kunt ook nog meer blokkeren, bijvoobeeld het /16 netwerk oftewel 45.118.* dan blokkeer je 65 536 (64K) ip adressen. Maar dan moet je wel weten welke netwerken je dan allemaal blokkeert. Om dit te controleren heb je een uitgebreide datasabase nodig, die je kunt downloaden bij bijvoorbeeld https://lite.ip2location.com Op deze site kun je zelf ook een een lijst krijgen van bijvoorbeeld alle ipnummers uit Nederland. Dan kun je in ieder geval controleren of je geen Nederlandse ipnummers blokkeert.

Blokkeren zelf gebeurt met:

```
sudo iptables -A INPUT -s 45.119.53.0/24 -j DROP
```

In dit geval blokkeer je 45.119.53.*

Om te zien wat je hebt geblokeerd:

```
sudo iptables -L
```

Om alle blokkades op te heffen:

```
iptables -F INPUT
```

Revision #2
Created 2019-12-10 07:35:10 UTC by Admin
Updated 2019-12-10 08:08:31 UTC by Admin