DDoS Angriffe abwehren

Hier soll erklärt werden, wie DDoS (Distributed Denial of Service) Angriffe mit Linux Bordmitteln abgewehrt werden können. Je nach Angriff funktionieren diese Methoden allerdings nur schlecht oder gar nicht. In diesem Fall muss der Angriff soweit möglich auf vorgelagerter Hardware (Router) geblockt werden oder der Dienst hinter einen Anbieter wie CloudFlare umgezogen werden.

Wie erkenne ich einen DDoS?

Server hat hohe Load, Ping zeigt Packetloss, Login oder Arbeiten auf der Shell ist kaum möglich.

Abwehrmaßnahmen

Bei protocol-ddos TCP/UDP, Synflood

Syncookies auf den betroffenen Servern/Loadbalancern aktivieren:

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Angreifer identifizieren

Hosts mit den meisten Verbindungen:

```
netstat -atun | awk '{print $5}' | cut -d: -f1 | sed -e '/^$/d' |sort | uniq -c | sort -n
```

Anhand der Apache Zugriffslogs:

```
cat access.log | awk '{print $1}' | cut -d: -f1 | sed -e '/^$/d' |sort | uniq -c | sort -n | tai
```

Angreifer blocken

Per IP:

```
iptables -I INPUT -s <angreifer-IP> -j DROP
```

SYN-Pakete per iptables limitieren

```
/sbin/iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 4 -j DROP
/sbin/iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 25 -j REJECT --reject-with t
```

Revision #1
Created 2021-05-31 12:43:19 UTC by magenbrot
Updated 2021-05-31 12:44:03 UTC by magenbrot