
IPTables

By rac

Published: 02.01.2008 - 13:21

SSH Bruteforce blocken

FOO durch den Namen der Firewall Chain und eth0 durch den Richtigen Netzwerkadapter ersetzen und natürlich sudo iptables davor.

```
# SSH: mehr als 3 neue Verbindungen/60 Sek.: BruteForce loggen
-A FOO -i eth0 -p tcp --dport 22 -m state --state NEW -m recent --rcheck --seconds 60 --hitcount 3
--rttl --name SSH -j LOG --log-level 7 --log-prefix "SSH_BruteForce "
# SSH: mehr als 3 neue Verbindungen/60 Sek.: BruteForce dropen
-A FOO -i eth0 -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 3
--rttl --name SSH -j DROP
# SSH: neue Verbindungen merken, aber durchlassen, wenn wir bis hierhin gekommen sind
-A FOO -i eth0 -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH -j ACCEPT
# SSH: bestehende Verbindungen erlauben
-A FOO -i eth0 -p tcp --dport 22 -j ACCEPT
```

Drop all Incoming

```
iptables -I INPUT ! -i lo -m state --state NEW,INVALID -j DROP
```

Links / Referenzen

- <http://downtown-dmz.de/index.php?archives/78-HowTo-sshd-absichern.html>
- <http://www.cyberciti.biz/tips/linux-iptables-10-how-to-block-common-attack.html>

- <http://www.cyberciti.biz/tips/how-can-i-enable-or-setup-log-message-in-the-iptables-firewall.html>

-->

Trackback URL for this post:

<http://www.2030.tk/trackback/24>