SSH vor Brute-Force-Angriffen härten

Um den SSH-Zugang im Internet zu schützen gibt es verschiedene Möglichkeiten:

- DenyHost (Python-script)
- Fail2ban [1] (python-script)
- recent [2](kernelmodul von iptables)

DenyHost und Fail2ban müssen einfach nur mittels „abt-get install“ installiert werden, eine Änderung der Standardkonfiguration ist im Normalfall nicht notwendig.

recent ist bereits bei der Standardinstallation enthalten, allerdings müssen einige IP-Tables regeln zur laufzeit erstellt werden:

secureSSHWithIptables

```
#!/bin/bash

# SSH erlauben - aber vor bruteforce schützen
iptables -N SSH-BruteForce
iptables -N SSH-Whitelist

iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -m
recent --set --name ssh
iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -j
SSH-Whitelist

iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -m
recent --update --seconds 600 --hitcount 4 --rttl --name ssh -j DROP

iptables -I INPUT -j SSH-BruteForce

#whitelist
iptables -A SSH-Whitelist -s 10.42.0.12 -m recent --remove --name ssh -
j ACCEPT


exit 0
```

In der Datei „/proc/net/xt_recent/ssh“ werden die BruteForce-Attacken mit IP's geloggt.

1)
https://wiki.ubuntuusers.de/fail2ban/
2)
http://www.gtkdb.de/index_36_2169.html