Linux

How to stop ssh brute force attacks?

well, there are a few way, the way of my choosing is to just use the recent module from iptables:

- iptables -A INPUT -p tcp --dport 22 -i ethX -m state --state NEW -m recent --set
- iptables -A INPUT -p tcp --dport 22 -i ethX -m state --state ESTABLISHED -m recent --update --seconds 60 --hitcount 2 -j REJECT --reject-with tcp-reset

This actually blocks anybody trying to connect twice to your ssh daemon within 60 seconds. This is really great for defending easily (e.g. without running an extra daemon/script, etc) against brute force attacks, but also keep in mind: you might lock out yourself. At least for .. sometime!

Unique solution ID: #1061
Author: n/a
Last update: 2009-11-19 16:48