Allgemeinwissen: Umgang mit iptables

Problem

Wer sich etwas in seinen Logfiles umschaut, findet immer wieder IP's die ständig (erfolglos) auf den SSH-Port oder FTP-Port zugreifen wollen.
Evtl. auch (Spam-)Emails einliefern oder sonstige schlimme Dinge versuchen.

Wenn man dann danach googled oder sich in seinem lieblings Server-Support-Forum umschaut, findet man meist den Tipp:

"Sperr ihn doch mit iptables!"

iptables

Eine kurze allgmeine Erklärung zu `iptables`:

Grundsätzlicher Aufbau einer Regel:

```
iptables -A/D INPUT/OUTPUT --protocol --destination --dport --source --sport -i/o --jump ACCEPT/DROP/REJECT/LOG
```

Die häufigsten benutzten Parameter:

- Grundlegendes Commando: Was soll gemacht werden?

  `A` = Anlegen (add) oder `D` löschen (delete) einer Regel

- `INPUT` und `OUTPUT` gibt die Grundlegende Chain an.

  (Wer eigene Chains definiert hat, kann auch diese hier angeben.)

  `INPUT` und `OUTPUT` beziehen sich direkt auf die IP-Pakete die über die Netzwerkkarte rein oder rausgehen.

- `protocol` (oder `-p`) bezeichnet das Protokol.

  Gängige Protokolle: `TCP`, `UDP` und `ICMP`.

- Mit `--destination` (oder `-d`) wird die Zieladresse angegeben. (optional)
- Und mit `--dport` wird der Zielport (oder Range) angegeben. (optional)
- Entsprechend andersrum ist `--source` (oder `-s`) die Absendeadresse. (optional)

- Und ebenfalls `--sport` ist der Absendeport. (optional)
- Wer mehrere Netzwerkkarten hat, spezifizert mit `-i` oder `-o` das (Incomming-/Outgoing-)Interface (meist eth0).
- Und nun der wichtigste Teil der Regel: `--jump` (oder `-j`) bezeichnet die Chain, in der das Paket weiter abgelegt wird.

  Hierbei gibt es die entsprechenden statischen Chains vom System.

Und dann gibt es noch die "Policy". Sie beschreibt, was mit alen Paketen gemacht werden soll, für die keine definierte Regel greift. (Siehe unter Beispiel.)

Beispiele:

Wir wollen einen speziellen Freak vom SSH-Port fern halten:

```
iptables -A INPUT -s 123.123.123.123 -p TCP --dport 22 -j DROP
```

Nun machen wir es umgekehrt: Alle Ports schließen und nur die aufmachen die wir brauchen (hier SSH und HTTP):

```
#Policy setzten:
iptables -P INPUT DROP
iptables -P OUTPUT DROP
#Ausnahmen definieren:
iptables -A INPUT -p TCP -d 0/0 --dport 22 -s 0/0 --sport 1024:65535 -o eth0 -j ACCEPT
iptables -A INPUT -p TCP -d 0/0 --dport 80 -s 0/0 --sport 1024:65535 -o eth0 -j ACCEPT
```

ACHTUNG:

Auf ein wesentliches Risiko muß aber hingewiesen werden:

Wenn irgendwas an den Regeln falsch gemacht wird (z.B. vergessen den SSH-Port freizugeben), kann man sich schnell aussperren.

Dann hilft nur noch eine serielle Konsole oder ähnliches.

Eindeutige ID: #1283
huschi
2008-02-22 16:16