Security & Firewalls: SSH absichern mit Fail2Ban

Was ist Fail2Ban?

Eine BrutoForce-Attacke besteht aus hunderten von Versuchen sich z.B. per SSH mit beliebigen (oder gezielten, z.B. `root`) Benutzernamen und zufälligen (oder aus Wörterbüchern oder -Listen genommenen) Passwörtern einzuloggen.

Grundsätzlich sind diese Angriffe nicht wirklich tragisch, wenn man gewisse Sicherheitsregeln einhält wie z.B.:

- Einloggen als `root` nicht gestattet.
- Logins nur mit RSA-Schlüsseln erlauben.
- Oder ganz simpel: den SSH-Port verlegt.

Es gibt verschiedene Gründe die o.g. Maßnahmen alle oder teilweise abzulehnen. (Meist ist es das Unwissen der Admin's.)

Damit dennoch die Logfiles durch diese BruteForce-Attacken nicht überlaufen, kann man das Programm Fail2Ban als Logfile-Scanner laufen lassen. Sobald es eine stetige Wiederholung von einer IP in den Logfiles findet, kann es diese per `iptables` auf dauer oder für eine gewisse Zeit sperren.

Konfigurationsbeispiele findet man vor allem für SSH, Apache und FTP.

Installation:

Neben dem Programm selber, ist grundsätzlich eine installierte (nicht zwangsweise aktivierte) Firewall von Nöten. Fail2Ban kann mit sowohl mit `iptables`, `netfilter`, Shorwall oder mit dem simplen TCP-Wrapper arbeiten.

Empfohlen wird aber von mir `iptables`.

Da Fail2Ban in Python geschrieben wurde, wird natürlich auch die Python-Laufzeit-Umgebung benötigt.

Für die meisten Distributionen sind vorkonfigurierte Pakete von Fail2Ban erhältlich. Meistens sind die direkt zu ladenden Pakete aber aktueller als die vom jeweiligen Distributor. Daher empfehle ich

den Weg des manuellen Downloads und Installation.

Wer lieber automatische Updates erhalten will, kann wie folgt vorgehen:

Debian 3.1 (sarge)

Für Sarge muß man auf backports.org zurück greifen. D.h. in die `/etc/apt/sources.list` gehört folgender Eintrag:

```
deb http://www.backports.org/debian sarge-backports main contrib non-free
```

Danach holen wird installiert:

```
#sources.list neu einlesen:
apt-get update
#Installation:
apt-get -t sarge-backports install fail2ban
```

Debian 4.0 (etch)

Auch für Etch muß gibt es noch keine direkten Paket. D.h. die Vorgehensweise ist wie bei Sarge nur eben mit `etch`. Hier alles für Copy+Paste:

```
# deb http://www.backports.org/debian etch-backports main contrib
apt-get update
apt-get -t etch-backports install fail2ban
```

openSUSE 10.x

Für openSUSE liegt das Paket im "Packman Repository".

Um dies zu aktivieren startet man `yast` und geht dann wie folgt durch die Menüs:

Software -› Community Repositories -› Packman Repository (aktivieren) -› Fertig

Danach kann Fail2Ban einfach installiert werden:

```
yast -i fail2ban
```

Konfiguration

Die eigentliche Konfiguration wird in `/etc/fail2ban/jail.conf` umgesetzt. Diese ist bereits mit Kommentaren gut dokumentiert.

Das einzige was man tun muß, ist die entsprechende Software finden, die man installiert hat und überwachen lassen will und alles andere auskommentieren.

Starten

Gestartet wird Fail2Ban einfach über das mitgelieferte init-Script:

```
/etc/init.d/fail2ban start
```

Sicherheitshalber sollte man mit einem Runlevel-Editor überprüfen, ob alle Start-Einträge für einen Neustart korrekt gesetzt worden sind.

Weiter Links:

- fail2ban.org
- fail2ban - Manual

Eindeutige ID: #1284
huschi
2009-11-11 09:05