Traffic: Trafficauswertung mit IAM

Dieses Tutorial soll euch zeigen, wie man mit Hilfe von IAM und einem Perlscript den Traffic an den Ports des Webservers überwacht und bei zu hohem Trafficaufkommen eine Mail an den Administrator schickt. So lassen sich beispielsweise DDoS Attaken schneller erkennen und abwehren.

Installation von IAM

IAM bekommt man auf dieser Webseite: http://www.intevation.de/iam

Hier laden wir uns die aktuelle Version (0.0.2) herunter und entpacken sie im /usr/src Verzeichniss:

```
cd /usr/local/src
wget ftp://ftp.intevation.de/iam/iam-0.0.2.tar.gz
tar xvfz iam-0.0.2.tar.gz
cd  iam-0.0.2
```

Da IAM mit iptables arbeitet kopieren wir die Datei `iptables.server` ins `/etc/init.d`-Verzeichniss.

```
cp iptables.server /etc/init.d/iam
chmod +x /etc/init.d/iam
```

Nun bearbeiten wird die Datei `/etc/init.d/iam` mit unserem favourisierten Texteditor und nehmen noch ein paar Einstellungen vor:

(Beachtet dabei, daß auf vServern evtl. `venet0` statt `eth0` eingetragen werden muß.)

```
DUMPFILE=/var/log/iamdump
extif=eth0
extip=IP DEINES SERVERS
intif=lo
hq=127.0.0.1/29
intnet=127.0.0.1/16
```

Evtl. kann man auch hq ganz auskommentieren:

```
#hq=212.227.80.7/32
[...]
#       new_chain intevation
#       acc_ip intevation $hq
```

Wenn andere iptables genutzt werden empfield sich in der Funktion start_firewall() den Aufruf von allow_all auszukommentieren.

Und nun starten wir schon mal die Filterung und setzen im Erfolgsfall den 'autostart':

```
/etc/init.d/iam start
#fuer SuSE:
insserv iam
#fuer Fedora/RedHat:
chkconfig iam
#fuer Debian:
update-rc.d iam defaults
```

Nun erstellen wir noch ein Verzeichnis für die restlichen IAM-Scripts die später benötigt werden und kopieren alles rein:

```
mkdir /usr/local/iam
cp * /usr/local/iam/
```

Jetzt erstellen wir für den Benutzer 'root' noch zwei Einträge im Crontab:

```
*/5  *  *  *  *  /etc/init.d/iam dump ›/dev/null
59  23  *  *  *  /usr/local/iam/traffikmail.sh
```

Für eine tägliche Nachricht über den angefallenen Traffic modifizieren wir noch die `traffikmail.sh`:

```
#!/bin/bash

STARTDATUM=$(date "+%Y%m%d")
ENDDATUM=$(date "+%Y%m%d")

/usr/local/iam/iam -r -f $STARTDATUM -t $ENDDATUM /var/log/iamdump | mail -s
"Traffikreport von meinem Server" root
```

Überwachungsscript:

Nun laden wir uns das zusätzlich benötigte Script runter:

```
cd /usr/local/src
wget http://www.huschi.net/download/traffic_check.tgz
tar xvfz traffic_check.tgz
mv traffic_check.pl iam/.
```

Nun müssen wir das Script `traffic_check.pl` noch entsprechend anpassen:

```
$IAM = '/usr/local/iam/iam';
$DUMPFILE = '/var/log/iamdump';
$MAIL_FROM = 'root@domain.tld';
$MAIL_TO = 'DEINE@MAILADDR.DE';
```

Nun kommt der Teil der etwas "tricky" ist:
Wir finden im dem traffic_check Script folgende Werte:

```
%CHAINS = ('outgoing (without other listed services)' => 0.1,
           'www (http/https/caudium)' => 0.1,
           'internet services'        => 0.1
);
```

Diese Werte geben an, wie groß der Wert sein darf an Traffic bei dem NICHT verwarnt wird.

Also:

Im Abschnitt 'www', das ist der Traffic vom Apache Webserver (80), dürfte nach oben in 15 min nicht mehr als 0.1 MB Traffic entstehen, alles was größer ist lößt die Warnung an den Webmaster aus. Das ist natürlich Schwachsinn (0.1 MB), diese Werte kann man eigentlich nur durch Erfrahrung oder Ausprobieren anpassen.

Meine Chains sehen so aus:

```
'outgoing (without other listed services)' => 10.0,
'www (http/https/caudium)'    => 30.0,
'other traffic (unspecified)' => 50.0,
'internet services'           => 30.0
```

Für einen kleinen nicht ausgelasteten Webserver reicht das.

Nun brauchen wir noch einen Cronjob um das Traffic_Check Script 15 minütlich auszuführen:

```
*/15 * * * * /root/traffic_check.pl >/dev/null 2>&1
```

Logrotate:

Da die Datei `iamdump` mit der Zeit entsprechend wächst, sollte man es noch dem `logrotate` füttern. (Wie das geht, muß jeder in seiner Distribution selber entdecken. Erster Ansatzpunkt wäre aber `/etc/logrotate.conf` oder `/etc/logrotate.d/`

Quelle:

Server-Support-Forum

Fragen, Fehler, Anregungen bitte (auch) im o.g. Forum posten.

Eindeutige ID: #1081
djrick, huschi
2006-01-01 22:50