Secure

Traffic-Kontrolle mit iam leichtgemacht (HowTo)

IAM Install-HowTo für einen Rootserver

Da es immer wieder im Forum auftaucht, hier nochmal eine kleine Zusammenfassung einiger typischer Probleme rund um das Traffic-Überwachungstool iptables accounting monster (IAM). Die wichtigen Schritte sind auch in der mitgelieferten HOWTO Datei beschrieben, allerdings in englisch.

Anhand einer typischen Installation (zum ansehen des Traffics per Web) will ich auf die Probleme kurz eingehen. Weitere Optionen und Konfigurationen sind natürlich gerne willkommen.

Die Befehle und Kommandos sind auf der Shell per ssh einzugeben.

* Archiv downloaden, entpacken und kopieren:

cd /usr/local/src
wget ftp://intevation.de/iam/iam-0.0.2.tar.gz
oder wget ftp://ftp.gwdg.de/pub/misc/freegis/intevation/iam/iam-0.0.2.tar
tar -xzvf iam-0.0.2.tar.gz
mkdir /usr/local/iam
cp -r /usr/local/src/iam-0.0.2/* /usr/local/iam/
cd /usr/local/iam

* Das Skript iptables kopieren, modifizieren und starten

- Kopieren:

cp iptables.server /etc/init.d/iptables

Mit dem Editor pico öffnen...

pico /etc/init.d/iptables

- Modifizieren (u.a. dank der Infos von Thomas Koester, dem Entwickler):

DUMPFILE=/usr/local/iam/dump

anpassen.

extif=eth0

können wir so lassen. Es ist das Device, an dem dieser Rechner an das Internet angeschlossen ist. Bei Rechnern mit nur einer Netzwerkkarte in Richtung Firewall meist eth0.

extip=217.160.xxx.yyy

Die IP-Adresse, die dieser Server vom Internet aus betrachtet hat, also deine Server-

IP.

intif=lo

Die "interne Netzwerkkarte" lo (local). Verkehr vom Rechner zu sich selbst soll ja sicherlich nicht berechnet werden.

intnet=195.20.224.72

Die Netzmaske für das LAN am Serverstandort. Dort kann man z.B. die IP des Updateservers von Puretec eintragen, denn der Traffic dorthin ist ja kostenlos. Diese IP entspricht der des Backupservers, zu dem der Traffic ebenfalls kostenlos ist, wenn man ihn gemietet hat.

Die Zeile hq= kann gelöscht werden. Sie hilft beim Beschreiben des Traffics zwischen eigenem Server und dem Server von intevation.de. Hq waere dann die Netzmaske fuer das Buero (HeadQuarter) von intevation.

Ebenso kann die Kette intevation gelöscht werden, d.h. folgende Zeilen löschen:

new_chain intevation
acc_ip intevation $hq

Dann sorgen wir dafür, dass das /var/log/warn Log nicht mit Meldungen überflutet wird. Die folgenden Zeilen im Bereich `other traffic` müssen so aussehen:

new_chain fragment
acc_ip fragment 0/0 -f

new_chain unknown
acc_ip unknown 0/0

Danach STR+O drücken und RETURN um zu speichern, sowie STR+X um pico zu verlassen.

- Starten:

/etc/init.d/iptables start

und es sollte erscheinen:

Starting iptables ip accounting: iptables.

Dann noch einen ersten Dump machen:

/etc/init.d/iptables dump

und die Datei dump im Verzeichnis /usr/local/iam sollte vom Skript angelegt sein.

* Das Skript an eigene Bedürfnisse anpassen
Der Satz aus dem original-HOWTO

quote:

Edit chains.py to set categories, names, rates and their descriptions.
---

dürfte selbsterklärend sein. Das ist nur eine Frage des persönlichen Geschmacks.

Zumindest folgende Zeile kann bedenkenlos gelöscht werden, wenn oben die Kette zum intevation-Server gelöscht wurde:

"intevation" : (free, "Intevation office"),

* Das Skript iam_report anpassen
Folgendes sollte so in iam_report stehen:

```
IAM=/usr/local/iam/iam
DUMP=/usr/local/iam/dump
WWWDIR=/home/Pfad_zum_Webverzeichnis
```

wobei WWWDIR den absoluten Pfad zu dem Webverzeichnis darstellt, in dem iam seine einsehbaren html-Dateien ablegt. Das Verzeichnis muss existieren bzw. noch angelegt werden und natürlich per Web erreichbar sein.

DUMP und IAM bezeichnen keine Verzeichnisse, sondern den kompletten Pfad samt Dateinamen des Skriptes iam (/usr/local/iam ist das Verzeichnis, /usr/local/iam/iam das Verzeichnis samt Dateinamen dahinter). Bei dump analog.

Wer den Anzeigezeitraum von iam dem Abrechnungszeitraum von 1&1 anpassen will, kann das durch folgende Änderungen in iam_report erreichen (angenommen der 9. des Monats ist euer Stichtag bei 1&1):

```
#!/bin/sh

IAM=/usr/local/iam
DUMP=/usr/local/iam/dumpfile
WWWDIR=/usr/local/iam/report

YM_CURRENT=`date '+%Y-%m'`
YM_LAST=`date --date='1 month ago' '+%Y-%m'`
YM_NEXT=`date --date='1 month' '+%Y-%m'`

$IAM -f $YM_CURRENT-09 -t $YM_NEXT-09 -w $WWWDIR/$YM_CURRENT.html $DUMP
$IAM -f $YM_LAST-09 -t $YM_CURRENT-09 -w $WWWDIR/$YM_LAST.html $DUMP

ln -sf $WWWDIR/$YM_CURRENT.html $WWWDIR/current.html
```

ln -sf $WWWDIR/$YM_LAST.html $WWWDIR/last.html

exit $?

Hier muss 09 natürlich durch deinen Abrechnungstag ersetzt werden.

* Reports automatisch erstellen lassen
Dazu müssen in der crontab folgende cronjobs erstellt werden:

export EDITOR=pico
crontab -e

zum aufrufen des Cron-Editors, dann dort folgende Zeilen einfügen (die jede halbe Stunde einen dump erstellen und zwei Minuten später den Report schreiben)

0,30 * * * * /etc/init.d/iptables dump >/dev/null
2,32 * * * * /usr/local/iam/iam_report
@reboot /etc/init.d/iptables start

Ebenso wieder STR+O und RETURN zum speichern und STR+X zum verlassen von pico.

* Testreport ausgeben (optional)
Jetzt noch einen ersten Report auf der Konsole erstellen lassen:

./iam -r dump

und es sollte ein Report erscheinen, der allerdings noch nicht viel enthält.

So, fertig ist die Installation.

Wenn auf dem Server Tools wie Nagios o.ä. laufen, gibt es natürlich immer etwas lokalen Traffic, also nicht wundern.

Wer weitere Ports speziell aufgelistet haben will (wie z.B. bei einigen Gameservern nötig), muss weitere chains erstellen. Wer damit nicht zurecht kommt, kann jederzeit im Forum suchen und ggf. posten, wenn`s noch keine Lösung gibt.

Viel Spass mit iam und nochmal THX an alle, die bei der Entwicklung des HowTos durch Tipps, Erklärungen und Verbesserungen mitgewirkt haben, vor allem an deepinpowder, der sich als unermüdlicher Betatester bewährt hat,

RootForum-Team
Mehr Informationen unter:
http://www.rootforum.de/forum/viewtopic.php?p=17396

2. Abrechnungszeitraum des Traffics ändern:

Secure

FALSCH:
YM_CURRENT=`date `+%Y-%m``
YM_LAST=`date --date=`1 month ago` `+%Y-%m``
YM_NEXT=`date --date=`1 month` `+%Y-%m``

RICHTIG:
YM_CURRENT=`date '+%Y-%m'`
YM_LAST=`date --date='1 month ago' '+%Y-%m'`
YM_NEXT=`date --date='1 month' '+%Y-%m'`

3. Falls man sich unsicher ist, wie das "Device" (meistens eth0) für seine Netzwerkkarte ist, kann man dies mit "ifconfig" herausfinden.

Eindeutige ID: #1018
Verfasser: Michael Stender
Letzte Änderung: 2007-08-08 03:06