Aus dem Alltag eines Sysadmin: Webalizer Xtended

Neues Logmittel

Webalizer ist ein Spezialist für das Auswerten von Webserver-Logfiles. Einen neues Patch erweitert das Tool um eine Komponente – es macht sichtbar, was nie da war. Charly Kühnast

Inhalt

Ab und zu stöbere ich durch die Logfiles meines Webservers, aber wirklich nur ab und zu. (Von den Dingern lese ich berufsbedingt schon oft genug.) Dass ich dabei Einträge finde, die mit „falsch verbunden“ zu erklären sind, ist alltäglich. Manchmal gibt es tolle Sachen wie

```
tharis.xxxxx.at - - [03/Dec/2005:08:24:43?
 +0100] "GET /LOST HTTP/1.1" 404 1025 "-"?
 "Mozilla/4.0"
```

zu bestaunen. Das ist zwar bizarr, aber harmlos. Anders wenn jemand gezielt und systematisch Dateien ansteuert, über die ich ein Security Advisory gelesen habe. In den letzten Wochen gab es zum Beispiel Meldungen über Sicherheitsmacken in PHP-MyAdmin und PHP-BB. In diese Kategorie fallen wohl auch die Zugriffe auf Dateien mit den Endungen ».mdb« und ».asp«, die ich heute im Log fand. Listing 1 zeigt eine Auswahl.

Der langen Rede kurzer Sinn: Ich will erfahren, welche Zugriffe auf meinen Webserver ins Leere laufen. So erkenne ich Angriffsmuster, die vielleicht auf meinen anderen Servern zu Ärger führen werden. Als netten Nebeneffekt sehe ich, welche Site-Links tot sind und dringend meiner Korrektur bedürfen.

Der 404 hat System

An dieser Stelle kommt Webalizer, ein guter Bekannter, ins Spiel. Patrick Frei hat ein Patch für Webalizer programmiert, mit dem die Logauswertung eine weitere Statistik liefert: über Requests, die der Webserver mit einem »404 - File not found« quittiert hat. Abbildung 1 zeigt sie für meinen Webserver am 6. Dezember 2005. Auf den ersten Blick ist zu erkennen, dass die Einträge, die ich beim manuellen Durchstöbern des Logfile gesehen hatte, keine Einzelfälle sind. Außerdem ist zu sehen, dass es tatsächlich ein paar kaputte Links gibt, um die ich mich mal kümmern müsste.

Es gibt zwei Möglichkeiten, den aufgebohrten Webalizer zu bekommen: Unter [1] gibt es den vollständigen Code inklusive appliziertem Patch. Er kompiliert mit: »./configure«, »make« und »make install«. Voraussetzung ist nur, dass sich die Pakete Zlib, Libpng und GD sowie die zugehörigen Devel-Pakete auf dem System befinden. Bei [1] gibt es auch ein Patch, mit dem das Webalizer-Original zum Webalizer Xtended aufsteigt. Dazu begibt man sich in das Verzeichnis, in dem der Webalizer-Source liegt, und führt

Code 404 Monthly Statistics for December 2005

#	Hits		URL
1	212	32.82%	/robots.txt
2	337	52.17%	/blog/
3	9	1.39%	/lbw
4	5	0.77%	/lbw/faq.html
5	5	0.77%	/bbs/data/dvbbs7.mdb
6	1	0.15%	/upfile_flash.asp
7	6	0.93%	/data/dvbbs7.mdb
8	8	1.24%	/upfile_flash.asp
9	1	0.15%	/manage/login.asp
10	1	0.15%	/Upfile_AdPic.asp
11	1	0.15%	/Upfile_Article.asp
12	1	0.15%	/Upfile_OrderPic.asp
13	4	0.62%	/tmdqq.asp
14	10	1.55%	/bbs/diy.asp
15	11	1.70%	/diy.asp
16	2	0.31%	/qq.txt
17	1	0.15%	/bbs/Data/dvbbs7.MDB
18	1	0.15%	/s9y/feeds
19	5	0.77%	/lbw/faq.htm
20	1	0.15%	/s9y/archives/20-Schatz
21	1	0.15%	/qq/qq.txt
22	3	0.46%	/upfile.asp
23	2	0.31%	/bbs/upfile.asp
24	2	0.31%	/upfile_soft.asp
25	1	0.15%	/bbs/upfile_soft.asp
26	4	0.62%	/s9y/P2.html

Abbildung 1: Webalizer Xtended liefert für den 6. Dezember die Falsch-verbunden-Meldungen.

```
patch -Np1 -i /Pfad?
/webalizer-2.01-10-RB06-patch
```

aus. Danach den Webalizer wie beschrieben kompilieren. Für Gentoo-Benutzer gibt es gar ein Ebuild. Ich wünsche allen nur wenig falsch Verbundene! *(jk)*

Listing 1: Webserver-Zugriffe

```
01 cncln.online.ln.cn - - [05/Dec/2005:22:09:04 +0100] "GET /bbs/upload.asp?action=upfile HTTP/1.1" 404 1025 "-"
   "InetURL:/1.0"
02 58.241.228.180 - - [06/Dec/2005:03:32:54 +0100] "GET /bbs/diy.asp HTTP/1.1" 404 1025 "-" "Mozilla/4.0"
03 222.62.228.179 - - [06/Dec/2005:07:19:49 +0100] "GET /bbs/diy.asp HTTP/1.1" 404 1025 "-" "InetURL:/1.0"
04 220.191.42.203 - - [13/Oct/2005:10:12:23 +0200] "GET /data/dvbbs6.mdb HTTP/1.1" 404 1025 "-" "InetURL:/1.0"
05 220.191.42.203 - - [13/Oct/2005:10:12:24 +0200] "GET /data/dvbbs7.mdb HTTP/1.1" 404 1025 "-" "InetURL:/1.0"
```

Infos

[1] **Webalizer:** [http://www.webalizer.go.to]

Der Autor

Charly Kühnast administriert Unix-Betriebssysteme im Rechenzentrum Niederrhein in Moers. Zu seinen Aufgaben gehören die Sicherheit und Verfügbarkeit der Firewalls und der DMZ (demilitarisierte Zone). In seiner Freizeit lernt er Japanisch, um endlich die Bedienungsanleitung seiner Mikrowelle lesen zu können.