MySQL-Datenbank für Snort +ACID

1. Partitionieren

/dev/hda1	ext2	50 M	/boot
/dev/hda5	swap	250 M	swap
/dev/hda6	reiserfs	500 M	/var/log
/dev/hda7	reiserfs	1.5 G	/var/lib/mysql
/dev/hda8	reiserfs	500 M	/

2. Software

I) Bei der Basis-Installation minimal

II) Nachträglich von SuSE:

- openSSH,
- mc,
- mysql.
- mysql-client,
- apache,
- mod_php4,

II) Nachträglich nicht SUSE:

- phplot,
  (http://www.phplot.com/)

- adodb,
  (http://php.weblogs.com/adodb)

- create_mysql
  (http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/contrib/)

3. Installation der Komponenten:

I) adodb:

Inhalt des Paketes nach /usr/local/httpd/htdocs kopieren

II) phplot:

Inalt des Paketes nach /usr/local/httpd/htdocs kopieren

III) acid:

Inalt des Paketes nach /usr/loca/httpd/htdocs kopieren

IV) MySQL-Datenbank starten:

```
/etc/rc.d/mysql start
```

V) Datenbank anlegen:

Auf die DB connecten:

```
mysql -u root -p
```

Passwort für root setzen:

```
set password for 'root'@'localhost'=password('***');
```

Datenbank snort anlegen:

```
create database snort;
exit
```

Datenbank snort einrichten:

```
mysql -u root -p
connect snort;
source /tmp/create_mysql;
```

Zugriffsrechte einrichten:

```
grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to snort;
grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to
    snort@localhost;
grant CREATE,INSERT,SELECT,PDATE on snort.* to acidviewer;
grant CREATE,INSERT,SELECT,UPDATE on snort.* to
    acidviewer@localhost;
```

Kennwörter für DB-Benutzer setzen:

```
connect mysql;
set password for 'snort'@'localhost'=password('***');
set password for 'snort'@'%'=password('***');
set password for 'acidviewer'@'localhost'=password('***');
set password for 'acidviewer'@'%'=password('***');
flush privileges;
```

VI) ACID-Konfigurieren:

`/usr/local/httpd/htdocs/acid_conf.php` anpassen:

```
....
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "***";
....
```

VII) Web-Server anpassen:

`/etc/httpd/httpd.conf` anpassen: htdocs konfigurieren:

VIII) Zugriff auf ACID einrichten:

In `/usr/local/httpd/htdocs` folgende Dateien anlegen:

```
.htaccess
      AuthType Basic
      AuthName SnortSnarf
      AuthUserFile /usr/local/httpd/htdocs/.users
      require valid-user
.users
      admin:DpcwYVBd4iwM.
```

Apache neu starten: `/etc/rc.d/apache` restart

IX) Härten:

Folgendes deinstallieren:
- cpp,
- providers,
- dhcpd

`/etc/cron.daily`:
Alles bis auf logrotate löschen,

`/etc/rc.d/rc3.d` anpassen:

```
K11atd                  S08portmap
K12nfs                  S10atd
K13sshd                 S11cron
K16network              K10cron
S05network              K11nscd
S08hwscan               K13portmap
S09nfs                  K15syslog
S10nscd                 S01random
K11fbset                S07hotplug
K13hwscan               S08sshd
K14hotplug              S10fbset
K20random               S11kbd
S06syslog
```

4. Snort mit MySQL

I) Paket: `snort-mysql-1.8.7-1snort.i386.rpm`

`snort-mysql` nach `/usr/sbin/snort`

II) Paket: `libpcap-0.6.2-9.i386.rmp`

`libpcap.so.0.6.2` nach `/usr/lib` kopieren

III) `/etc/snort/snort.conf`

```
output database: log, mysql, user=snort password=test
    dbname=snort host=localhst port=3306
```