877.853
Projektpraktikum

Alexander Ölzant
9301547

9. Juli 2005

Inhaltsverzeichnis

Kapitel 1

Einleitung

Wie besprochen, schreibe ich hier die Übungsaufgaben unter Verwendung von Debian GNU/Linux protokollarisch nieder.

Kapitel 2

Übungen

2.1 Übungen zum Apache Webserver

2.1.1 Installiere den Apache Webserver

```
# apt-get install apache
...
Setting up apache-ssl (1.3.33-6) ...
Starting web server: apache-ssl.
```

2.1.2 Schau in der chkconfig Liste nach, ob er gestartet wird, wenn der Rechner hochfährt. Wenn das nicht der Fall ist, dann trag ihn für die Runlevels 3 und 5 als zu startend ein und kontrolliere, ob das korrekt erfolgt ist.

```
# ls -l /etc/rc[35].d/*apache*
lrwxrwxrwx  1 root root 20 Sep 28  2003 /etc/rc3.d/S91apache-ssl ->
../init.d/apache-ssl
lrwxrwxrwx  1 root root 20 Sep 28  2003 /etc/rc5.d/S91apache-ssl ->
../init.d/apache-ssl
```

2.1.3 Starte jetzt Apache und rufe als Test in einem Browser (firefox, konqueror, ...) die Webseite deines Rechners auf (zriXY.pclab). Wenn dein Browser eine Fedora Core Test Page anzeigt, dann läuft der Apache!

```
# curl -s -o/dev/null localhost && echo ok || echo "Webserver down"
ok
```

2.1.4 Sieh dir die access_log Datei an, ob dein Aufruf dort aufscheint. Jede Zeile dort entspricht einer Anfrage. Versuche, einige Teile der Zeile zu interpretieren!

```
62.178.57.72 - - [25/May/2005:09:16:09 +0200] "SEARCH /\x90\x02...
```

Da versucht wohl wieder jemand/frau, einen alten Exploit auszuprobieren ...

```
127.0.0.1 - - [05/Jul/2005:18:42:14 +0200] "GET / HTTP/1.1" 200 4110 "-"
"curl/7.13.2 (i386-pc-linux-gnu) libcurl/7.13.2 OpenSSL/0.9.7e zlib/1.2.2
libidn/0.5.13" 0 chello062178208184.1.15.univie.teleweb.at
```

Das ist wohl das curl von grade eben (Source Host ist localhost aka 127.0.0.1, die Anfrage bezieht sich auf /, also das DocumentRoot, Zeit, nicht vorhandener Referer und Browser Id sind auch erkenntlich)

2.1.5 Rufe eine nicht existierende Datei per Browser auf und sieh dir die error_log an. Welchen HTTP-Statuscode verursachen nicht existierende Seiten? Scheinen solche Anfragen auch in der access_log auf?

404, immer wieder (und sei es nur ein favicon.ico)

2.1.6 Laß den apache auf Port 81 auf Connections warten und überprüfe das mit dem Browser. Ändere die Einstellung wieder auf Port 80 zurück, wenn es geklappt hat. Zur Erinnerung: Starte den Apache immer neu, wenn du Änderungen an seiner Konfiguration vornimmst!

```
# sed -i -e 's/:80/:81/' -e 's/Listen 80/Listen 81/' \
 /etc/apache-ssl/httpd.conf && apache-sslctl graceful && (curl -s \
 -o/dev/null localhost:81 && echo ok || echo "Webserver down") && sed -i \
 -e 's/:81/:80/' -e 's/Listen 81/Listen 80/' /etc/apache-ssl/httpd.conf && \
 apache-sslctl graceful && (curl -s -o/dev/null localhost && echo ok || \
 echo "Webserver down")
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
ok
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
ok
```

2.1.7 Konfiguriere ServerAdmin und ServerName für deinen Rechner.

```
# sed -i -e 's/ServerAdmin.*/ServerAdmin myaddress@mydomain/' \
         -e 's/ServerName.*/ServerName this.host.name/'
```

2.1.8 Erstelle ein Verzeichnis /www und lege eine index.html hinein (Hier gibts eine fertige index.html, mit Rechtsklick speichern). Ändere die beiden entsprechende Direktiven in der httpd.conf, wo das Basisverzeichnis des Webservers vorkommt, so ab, daß /www das neue Rootverzeichnis für den Apache ist. Versichere dich, daß deine Änderungen erfolgreich waren!

```
# mkdir /www ;  curl -s -o /www/index.html \
 http://www.mat.univie.ac.at/~martin/lehre/ss05/pp/apache/index.html && \
 sed -i -e ’s/\/var\/www/\/www/’ /etc/apache-ssl/httpd.conf && \
 apache-sslctl graceful && (curl -s localhost | grep -E "DocumentRoot \
 bereits in .*/www" || echo Fehler; true) && sed -i -e \
 ’s/\/www/\/var\/www/’ /etc/apache-ssl/httpd.conf && apache-sslctl \
 graceful && rm -rf /www
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
Wenn du das siehst, sollte dein Webserver sein DocumentRoot bereits in
<tt>/www</tt> haben!
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
```

2.1.9 Benenne die neue index.html in index.htm um. Jetzt sollte wieder die Standardseite von Fedora kommen. Warum ist das so? (Tip: Scheint index.htm in der DirectoryIndex-Direktive auf?). Versuche, die Konfiguration entsprechend zu korrigieren.

Offenbar gibt es ein `index.php`, `index.cgi` oder ähnliches, das in der `DirectoryIndex` explizit genannt ist, das sieht hier z. B. so aus:

```
    DirectoryIndex index.html index.htm index.shtml index.cgi
```

2.1.10 Erstelle ein Verzeichnis /www/protected/, das nur von deinem eigenen Rechner zugänglich ist. Dazu mußt du einen Eintrag für das Verzeichnis in der Konfigurationsdatei erstellen und die Allow/Deny-Regeln entsprechend eintragen. Probiere es von einem Nachbar-PC aus!

```
<Directory /www/protected>
Order deny,allow
Deny from all
Allow from localhost
</Directory>
```

2.1.11 Erstelle analog ein Verzeichnis /www/prot2/, das diesmal aber nicht von deinem eigenen Rechner aus, sondern nur von deinem Nachbar-PC zugänglich ist. Überprüfe wieder, ob es geklappt hat!

```
<Directory /www/protected>
  Order deny,allow
  Deny from all
  Allow from Nachbar-PC
</Directory>
```

2.1.12 Lege (mittels adduser) einen Benutzer pinguin an. Die Dateien in seinem Unterverzeichnis html sollen angezeigt werden, wenn man sich auf http://zriXY.pclab/ pinguin/ verbindet. Vergiß nicht, das Verzeichnis html auch tatsächlich anzulegen (das kannst du als root tun). Als Index-Datei kannst du die Datei aus Übung 8 verwenden. Achtung: Das Benutzerverzeichnis (/home/pinguin) muß das Zugriffsrecht „x“für alle besitzen, sonst kann der Webserver nicht dorthin!

```
# adduser --disabled-password --gecos tux  pinguin && mkdir -p \
 ~pinguin/public_html && chmod -R a+x ~pinguin/public_html && curl -s -o \
 ~pinguin/public_html/index.html \
 http://www.mat.univie.ac.at/~martin/lehre/ss05/pp/apache/index.html && \
 chmod a+r ~pinguin/public_html/index.html && (curl localhost/~pinguin/ |\
 grep -E "DocumentRoot bereits in .*/www" || echo fehler ) ; deluser \
 pinguin; rm -rf /home/pinguin \
Adding user ‘pinguin’...
Copying files from ‘/etc/skel’
Wenn du das siehst, sollte dein Webserver sein DocumentRoot bereits in
<tt>/www</tt> haben!
Removing user ‘pinguin’...
done.
```

2.1.13 Schau dir eine nicht-existierende Datei auf deinem Webserver einmal mit ServerSignature, einmal ohne, an. Welche Daten stehen in der ServerSignature? Wenn du die Webmaster-Emailadresse dort nicht siehst, ändere die Konfiguration so ab, daß sie angezeigt wird. Ist es die Adresse, die du im Punkt 7 oben eintragen hast? Überlege kurz (nicht zu viel philosophisches „Blabla“ :-), auf welchen Wert du diese Option für deinen eigenen Webserver setzen würdest!

```
# sed -i -e 's/ServerSignature.*/ServerSignature On/' \
 /etc/apache-ssl/httpd.conf && apache-sslctl graceful && curl -s \
 localhost/asd | grep Apache
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
<ADDRESS>Apache/1.3.33 Ben-SSL/1.55 Server at
chello062178208184.1.15.univie.teleweb.at Port 80</ADDRESS>

# sed -i -e 's/ServerSignature.*/ServerSignature Off/' \
 /etc/apache-ssl/httpd.conf && apache-sslctl graceful && curl -s \
 localhost/asd | grep Apache
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted

# sed -i -e 's/ServerSignature.*/ServerSignature Email/' \
 /etc/apache-ssl/httpd.conf && apache-sslctl graceful && curl -s \
 localhost/asd | grep Apache
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
<ADDRESS>Apache/1.3.33 Ben-SSL/1.55 Server at <A
HREF="mailto:webmaster@chello062178208184.1.15.univie.teleweb.at">
chello062178208184.1.15.univie.teleweb.at</A> Port 80</ADDRESS>
```

Paranoide Leute setzen das üblicherweise auf „Off“, damit maliciöse Holzhacker den Wald vor lauter Bäumen nicht sehen. Ich bin nicht so paranoid, finde aber immer noch den Zugang von Alexander Talos, `sendmail` als „sandman“ und die Version als sein Geburtsdatum auszugeben, am originellsten.

2.1.14 Erstelle einen eigenen Error-Handler für deinen Webserver, einmal für fehlende, einmal für „Access forbidden“-Dateien und vergewissere dich, daß der jeweils richtige aufgerufen wird. Access forbidden kannst du „provozieren“, indem du z.B. einem Verzeichnis oder einer Datei alle Rechte für „others“ wegnimmst.

```
# echo -e "ErrorDocument 404 /missing.html\nErrorDocument 403 \
 /forbidden.html" >> /etc/apache-ssl/httpd.conf ; \
```

```
 echo forbidden > /var/www/forbidden.html; \
 apache-sslctl graceful; \
 chmod a-r /var/www/index.html; \
 curl -s localhost/asd
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
The requested URL /asd was not found on this server.<P>
<P>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the
request.
<HR>
<ADDRESS>Apache/1.3.33 Ben-SSL/1.55 Server at <A
HREF="mailto:webmaster@chello062178208184.1.15.univie.teleweb.at">chello062178208184.1.15
Port 80</ADDRESS>
</BODY></HTML>

# curl -s localhost/
forbidden
```

2.1.15 Erstelle einen Redirect von /mat auf www.mat.univie.ac.at.

```
# echo Redirect /mat http://mat.univie.ac.at/ >> /etc/apache-ssl/httpd.conf;\
  apache-sslctl graceful; curl -s localhost/mat/|grep mat
/usr/sbin/apache-sslctl graceful: httpsd gracefully restarted
The document has moved <A HREF="http://mat.univie.ac.at//">here</A>.<P>
```

2.1.16 Zusatzaufgabe für Fleißige: Im DNS existieren CNAMEs von zriXYa.pclab auf zriXY.pclab (also z.b. zri20449a.pclab auf zri20449.pclab). Je nach im Browser eingegebenem Servername soll eine andere Webseite zurückgeliefert werden! (Bitte bei mir melden, wenn wer diese Übung machen will, dann erstelle ich den DNS-Eintrag!)

```
# echo "<VirtualHost *:80>
ServerName brasilia.aoe
DocumentRoot /asd
SSLDisable
</VirtualHost>
" >> /etc/apache-ssl/httpd.conf
```

```
# curl -s brasilia.aoe|grep server
The requested URL / was not found on this server.<P>
```

2.2 8. April 2005: Übungen zum IMAP/POP3 Server

2.2.1 Installiere das IMAP Paket.

```
# apt-get install uw-imapd
```

2.2.2 Lege einen lokalen User (mit adduser) an und gib ihm ein Paßwort!

```
# PASS=‘perl -e ’use Digest::MD5 qw(md5_base64);
    open U,"</dev/urandom";$p=$s=10x"x";read U,$p,10;read \
    U,$s,10; $pass=md5_base64($p);$salt=md5_base64($s); \
    print $pass," ",crypt($pass,$salt),"\n"’‘; \
  CRYPT=${PASS#* }; PASS=${PASS% *}; export CRYPT PASS; \
  useradd -p "$CRYPT" -c tux pinguin
```

2.2.3 Ändere in /etc/aliases die Zeile root: `root@miranda.pclab` und setze anstatt `root@miranda.pclab` den Namen des soeben angelegten Users ein! Führe danach newaliases aus, um die Änderung zu aktivieren!

```
# sed -ie ’s/root:.*/root: pinguin/’ /etc/mail/aliases; newaliases
/etc/mail/aliases: 79 aliases, longest 29 bytes, 1117 bytes total
```

2.2.4 Schicke einige Mails an root und an den angelegten User (am einfachsten z.b. mit `echo blabla | mail $user`

```
$ (export user=pinguin; </dev/null mail -s "test ignore" $user)
Null message body; hope that’s ok
```

2.2.5 Aktiviere jetzt im xinetd das imap und ipop3 Subsystem und starte den xinetd neu.

`xinetd` habe ich derzeit nicht installiert, und da dies ja eine pop3/imap4-Übung ist, werde ich mal den klassischen `inetd` verwenden.

```
# sed -ie ’s/#\(\(pop3\|imap2\).*\)/\1/’  /etc/inetd.conf ; killall -HUP inetd
# grep -E "pop|imap" /etc/inetd.conf|sed -e ’s/#\(pop3.*\)/\1/’
pop3   stream  tcp     nowait  root    /usr/sbin/tcpd   ipop3d
imap2   stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/imapd
```

2.2.6 Richte dir in einem Mailclient (z.b. kmail oder mozilla) ein IMAP und POP3 Postfach für den angelegten User ein. Wenn die Mails per POP3 geholt werden, sollen sie nicht gelöscht werden!

The Good: mutt

```
# echo -e "set folder=imap://localhost/INBOX
set spoolfile=imap://localhost/INBOX
set imap_user=$USER
" >> .muttrc
```

The Bad: pine

```
# echo -e "folder-collections= Remote-Mail {localhost/user=${USER}}INBOX.[]
inbox-path={imap.unet.univie.ac.at/user=${USER}}INBOX
rsh-command=/dev/null
disable-these-authenticators=cram-md5
" >> .pinerc
```

The Ugly: fetchmail

```
# echo "poll localhost\nuser pinguin\npass $PASS" > .fetchmailrc; \
  chmod 0710 .fetchmailrc
# fetchmail -p POP3 -k -u pinguin -a -m cat -v | head
fetchmail: Unknown command in AUTHORIZATION state
fetchmail: Repoll immediately on pinguin@localhost
fetchmail: 6.2.5 querying localhost (protocol POP3) at Wed Jul  6 13:20:20 2005: poll sta
fetchmail: POP3< +OK private.oelzant.priv.at POP3 3.3(20) w/IMAP2 client
(Comments to MRC@CAC.Washington.EDU) at Wed, 6 Jul 2005 13:20:20 +0200 (CEST)
fetchmail: POP3> CAPA
fetchmail: POP3< -ERR Unknown command in AUTHORIZATION state
fetchmail: POP3< +OK private.oelzant.priv.at POP3 3.3(20) w/IMAP2 client
(Comments to MRC@CAC.Washington.EDU) at Wed, 6 Jul 2005 13:20:20 +0200 (CEST)
fetchmail: POP3> USER pinguin
fetchmail: POP3< +OK User name accepted, password please
fetchmail: POP3> PASS *
fetchmail: POP3< +OK Mailbox open, 3 messages

# fetchmail -p IMAP -k -u pinguin -a -m cat -v |tail
fetchmail: Server CommonName mismatch: private.oelzant.priv.at != localhost
fetchmail: Server CommonName mismatch: private.oelzant.priv.at != localhost

 not flushed
fetchmail: IMAP> A0015 STORE 3 +FLAGS (\Seen)
```

```
fetchmail: IMAP< * 3 FETCH (FLAGS (\Seen))
fetchmail: IMAP< A0015 OK STORE completed
fetchmail: IMAP> A0016 LOGOUT
fetchmail: IMAP< * BYE private.oelzant.priv.at IMAP4rev1 server terminating
connection
fetchmail: IMAP< A0016 OK LOGOUT completed
fetchmail: 6.2.5 querying localhost (protocol IMAP) at Wed Jul  6 12:59:41 2005: poll com
fetchmail: normal termination, status 0
```

2.2.7 Versuche jetzt, beide eingerichteten Postfächer abzufragen. Bekommst du die Mails, die du vorher geschickt hast?

Siehe vorige Frage, die Mails sind natuerlich als gelesen markiert und nur mit „fetch all“ erneut verfügbar.

2.2.8 Versuche jetzt, als Server den Rechner deines Nachbarn und auch seinen User einzutragen. Kannst du auch von dort Mails abrufen?

Wenn der port nicht per tcp wrappers, firewall oder pop3/imapd-config gesperrt ist, sicherlich.

2.2.9 Ist es möglich, die Mails für root per POP3/IMAP abzurufen?

```
# fetchmail -p IMAP -k -u root -a -m cat -v |tail
fetchmail: Server CommonName mismatch: private.oelzant.priv.at != localhost
fetchmail: Server CommonName mismatch: private.oelzant.priv.at != localhost
fetchmail: Authorization failure on root@localhost
fetchmail: IMAP> A0004 LOGIN "root" *
fetchmail: IMAP< A0004 NO LOGIN failed
fetchmail: IMAP> A0005 *
fetchmail: IMAP> A0006 LOGOUT
fetchmail: IMAP< A0005 BAD Command unrecognized/login please: *
fetchmail: IMAP< * BYE private.oelzant.priv.at IMAP4rev1 server terminating
connection
fetchmail: IMAP< A0006 OK LOGOUT completed
fetchmail: 6.2.5 querying localhost (protocol IMAP) at Wed Jul  6 13:11:41
2005: poll completed
fetchmail: Query status=3 (AUTHFAIL)
fetchmail: normal termination, status 3
```

nein

2.2.10 Welche Informationen über deine Mail-Abrufe siehst du in der Logdatei?

```
# grep -iE "pop|imap" /var/log/secure /var/log/messages /var/log/maillog
Jul  6 12:59:41 comitan imapd[5906]: Login user=pinguin host=localhost [127.0.0.1]
Jul  6 12:59:41 comitan imapd[5906]: Logout user=pinguin host=localhost [127.0.0.1]
Jul  6 13:11:38 comitan imapd[6399]: imap service init from 127.0.0.1
Jul  6 13:11:41 comitan imapd[6399]: Logout user=root host=localhost [127.0.0.1]
...
Jul  6 13:11:38 comitan imapd[6399]: Login failed user=root auth=root
host=localhost [127.0.0.1]
...
Jul  6 13:17:55 comitan ipop3d[6819]: connect from localhost (127.0.0.1)
Jul  6 13:17:55 comitan ipop3d[6820]: connect from localhost (127.0.0.1)
```

bei imapd user und host, bei ipop3d nur die zeit (vermutlich konfigurierbar)

2.3 Übungen zum vsftpd FTP Server

2.3.1 Installiere `vsftpd`. Starte den Server.

```
# apt-get install vsftpd
...
Starting FTP server: vsftpd.
```

2.3.2 Der Server soll auch beim Booten gestartet werden (wie „üblich“ per chkconfig)

`chkconfig` ist (wie „üblich“) auf Debian GNU/Linux nicht vorhanden, update-rc.d meint, der Dienst würde bereits getartet.

```
# update-rc.d vsftpd defaults
 System startup links for /etc/init.d/vsftpd already exist.
```

2.3.3 Lege ein Verzeichnis /ftp an und mache es zu deinem FTP Hauptverzeichnis.

```
# echo anon_root=/ftp >> /etc/vsftpd.conf; killall -HUP vsftpd
```

2.3.4 Lege einige Dateien und Verzeichnisse (egal welchen Inhalts) in /ftp an.

```
# mkdir -p /ftp/dir1/dir2; curl -s ftp://localhost/dir1/
drwxr-xr-x    2 0        0            4096 Jul 06 11:49 dir2
```

```
# echo xyz > /ftp/jkl; curl -s ftp://localhost/jkl
xyz
```

2.3.5 Logge dich als anonymer User ein und überprüfe, ob das Root Verzeichnis ok ist (d.h. ob die Dateien, die du hingelegt hast, tatsächlich zu sehen sind).

Siehe vorige Übung.

2.3.6 Versuche, eine Datei vom Server herunterzuladen.

Siehe vorige Übung.

2.3.7 Ändere die Nachricht, die erscheint, wenn du dich am Server einloggst.

```
# sed -i -e 's/^#ftpd_banner.*/ftpd_banner=Welcome in/' /etc/vsftpd.conf; \
  /etc/init.d/vsftpd restart; \
  sleep 1; \
  curl -v ftp://localhost/ 2>&1 | grep 220
Restarting FTP server: vsftpd.
< 220 Welcome in
```

(oder, als dir message fürs root dir:)

```
# echo Hello World > /ftp/.message
# curl -v  ftp://localhost/ 2>&1 | grep 230
< 230-Hello World
< 230 Login successful.
```

2.3.8 Lege ein Verzeichnis in /ftp (z.b. /ftp/tmp), auf das alle Benutzer alle Zugriffsrechte haben.

```
# mkdir /ftp/tmp; chmod 1777 /ftp/tmp
# sed -i -e 's/#anon_upload_enable=YES/anon_upload_enable=YES/' \
    -e 's/#write_enable=YES/write_enable=YES/'  /etc/vsftpd.conf; \
  /etc/init.d/vsftpd restart
```

2.3.9 Versuche, eine Datei auf den Server in das soeben angelegte Verzeichnis hinaufzuladen. Wenn es nicht geht, kontrolliere die dafür zuständigen Optionen in der Konfigurationsdatei noch einmal!

```
# echo 123 > upload_file; \
  curl -T upload_file ftp://localhost/tmp/
```

```
-rw-------    1 111      65534           4 Jul 06 12:08 upload_file
# curl ftp://localhost/tmp/ ftp://localhost/tmp/upload_file
curl: (19) Failed to open file.
```

2.3.10 Deaktiviere jetzt jeglichen Schreibzugriff auf den Server und teste es.

```
# sed -i -e 's/anon_upload_enable=YES/#anon_upload_enable=YES/' \
    -e 's/write_enable=YES/#write_enable=YES/' /etc/vsftpd.conf; \
  /etc/init.d/vsftpd restart; \
  curl -T upload_file ftp://localhost/tmp/upload2
curl: (25) Failed FTP upload: 550
```

2.3.11 Leg den Benutzer tux an.

```
# deluser pinguin; rm -rf /home/pinguin
# PASS=`perl -e 'use Digest::MD5 qw(md5_base64);  \
    open U,"</dev/urandom"; \
    $p=$s=10x"x"; \
    read U,$p,10; \
    read U,$s,10; \
    $pass=md5_base64($p); \
    $salt=md5_base64($s); \
    print $pass," ", crypt($pass,$salt),"\n"'`;  \
  CRYPT=${PASS#* }; \
  PASS=${PASS% *}; \
  export CRYPT PASS; \
  useradd -p "$CRYPT" -c pinguin -m tux
```

2.3.12 Versuche, ob du dich auf dem Rechner deines Nachbarn als tux anmelden kannst.

Vollinhaltlich von der Workstation nebenan …

```
> curl -u tux:$PASS ftp://brasilia.aoe/
drwxr-xr-x    5 1825     100          4096 Jul 06 12:24 Desktop
```

2.3.13 Wenn das geht, versucht es zu deaktivieren! Wenn nicht, dann aktiviert es.

```
# sed -i -e 's/^local_enable=YES/#local_enable=YES/' /etc/vsftpd.conf; \
  /etc/init.d/vsftpd restart; \
  sleep 1; \
  curl -u tux:"$PASS" ftp://localhost/
Restarting FTP server: vsftpd.
```

```
curl: (67) Access denied: 530

# sed -i -e 's/^#local_enable=YES/local_enable=YES/' /etc/vsftpd.conf; \
  /etc/init.d/vsftpd restart; \
  sleep 1; \
  curl -u tux:"$PASS" ftp://localhost/
Restarting FTP server: vsftpd.
drwxr-xr-x    5 1825     100          4096 Jul 06 12:24 Desktop
```

2.3.14 14. Sieh dir die Log-Datei des FTP Servers an und versuche die Daten zu interpretieren (je eine Zeile ist ein Zugriff auf den Server). Wenn dir einige Daten dort nicht klar sind, versuche mithilfe der angegebenen Webseiten mehr Information darüber herauszufinden.

```
Wed Jul  6 14:07:05 2005 [pid 9595] [ftp] FAIL DOWNLOAD: Client
"127.0.0.1", "/tmp/upload_file", 0.00Kbyte/sec
Wed Jul  6 14:11:23 2005 [pid 9814] [ftp] FAIL UPLOAD: Client "127.0.0.1",
"/tmp/upload2", 0.00Kbyte/sec
Wed Jul  6 14:14:19 2005 [pid 9940] CONNECT: Client "127.0.0.1"
Wed Jul  6 14:14:19 2005 [pid 9939] [ftp] OK LOGIN: Client "127.0.0.1",
anon password "curl_by_daniel@haxx.se"
Wed Jul  6 14:14:19 2005 [pid 9941] [ftp] OK UPLOAD: Client "127.0.0.1",
"/tmp/upload3", 4 bytes, 1.08Kbyte/sec
Wed Jul  6 14:15:01 2005 [pid 9996] CONNECT: Client "127.0.0.1"
Wed Jul  6 14:15:01 2005 [pid 9995] [ftp] OK LOGIN: Client "127.0.0.1",
anon password "curl_by_daniel@haxx.se"
Wed Jul  6 14:25:57 2005 [pid 10665] CONNECT: Client "192.168.2.10"
Wed Jul  6 14:26:56 2005 [pid 10681] CONNECT: Client "192.168.2.99"
Wed Jul  6 14:31:28 2005 [pid 11052] [tux] OK LOGIN: Client "127.0.0.1"
```

Misserfolge beim Login scheinen nur als `CONNECT` auf, ansonsten sind aus dem vsftpd.log alle Transfers und Logins mit Zeit, Herkunft und User ersichtlich.

2.4 Übungen zum Postfix Mail Server

2.4.1 Installiere postfix!

```
# apt-get install postfix
...
Postfix was not set up.  Start with
  cp /usr/share/postfix/main.cf.debian /etc/postfix/main.cf
```

```
.  If you need to make changes, edit
/etc/postfix/main.cf (and others) as needed.  To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.
```

2.4.2 Konfiguriere die notwendigen Netzwerkeinstellungen (Hostname, Domain, ...) in der /etc/postfix/main.cf.

```
# cp /usr/share/postfix/main.cf.debian /etc/postfix/main.cf; \
  echo mydomain = 3.aoe >> /etc/postfix/main.cf; \
```

2.4.3 Starte nun den Server.

```
# /etc/init.d/postfix start
Starting mail transport agent: Postfix.
```

2.4.4 Lege die lokalen User gandalf und frodo (z.b. mit adduser) an. Gib beiden Usern mit passwd ein Paßwort.

```
# adduser --disabled-password --gecos hobbit frodo
Adding user `frodo'...
Adding new group `frodo' (1002).
Adding new user `frodo' (1002) with group `frodo'.
Creating home directory `/home/frodo'.
Copying files from `/etc/skel'
# adduser --disabled-password --gecos wizard gandalf
Adding user `gandalf'...
Adding new group `gandalf' (1003).
Adding new user `gandalf' (1003) with group `gandalf'.
Creating home directory `/home/gandalf'.
Copying files from `/etc/skel'
```

Den Sinn der Passwortvergabe kann ich an dieser Stelle nicht erkennen, zur Methodik siehe 2.2.2 und 2.3.11

2.4.5 Ändere den Alias für `root`, sodaß Mail statt an ihn an `gandalf` geht und verifiziere das, indem du root eine Mail schickst.

Siehe auch Sektion 2.2.3

```
# sed -ie 's/root:.*/root: gandalf/' /etc/aliases; newaliases
# mail -s 'Of all the confounded nuisances you are the worst, Sam!' root \
    < /dev/null
```

```
# grep nuisance /var/mail/gandalf
Subject: Of all the confounded nuisances you are the worst, Sam!
```

2.4.6 Schicke vom root Account aus per pine eine Email an frodo.

```
# pine -s ignore frodo < /dev/null
-su: pine: command not found
```

Auf einem anderen Rechner, ganz weit weg ...

```
# pine -s ignore frodo@myhost < /dev/null
Argument Error: unknown flag "s"
Possible Starting Arguments for Pine program:
...
```

Schlussfolgerung: Pine ist kein regulärer MUA.

```
# mail -s ignore frodo < /dev/null
Null message body; hope that's ok
```

2.4.7 Überprüfe (mit pine und über das Maillog), ob die Mail angekommen ist.

`pine` ist aus verschiedenen Gründen (u. a. DFSG) nicht installiert, mailx-output folgt.

```
# grep frodo /var/log/mail.log
Jul  6 15:30:48 tipitapa postfix/local[4087]: B24FB179D8C:
to=<frodo@tipitapa.aoe>, orig_to=<frodo>, relay=local, delay=1, status=sent
(delivered to mailbox)
# mailx -f /var/spool/mail/frodo < /dev/null
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/spool/mail/frodo": 1 message 1 new
>N  1 root@tipitapa.aoe  Wed Jul  6 15:30   13/414   ignore
"/var/spool/mail/frodo" complete
```

2.4.8 Richte einen Alias `office` ein, der empfangene Mails an gandalf und frodo weiterleitet.

```
# echo office: frodo,gandalf >> /etc/aliases; newaliases
```

2.4.9 Schick eine Mail an `office` und schau dir das Maillog an!

```
# mutt -s "lazy lizards" office < /dev/null
# tail /var/log/mail.log
Jul  6 15:39:35 tipitapa postfix/pickup[4014]: 06DD8179D8C: uid=0 from=<root>
Jul  6 15:39:35 tipitapa postfix/cleanup[4134]: 06DD8179D8C:
  message-id=<20050706133934.GA4129@tivoli.oelzant.priv.at>
Jul  6 15:39:35 tipitapa postfix/qmgr[4015]: 06DD8179D8C:
  from=<root@tipitapa.aoe>, size=406, nrcpt=1 (queue active)
Jul  6 15:39:35 tipitapa postfix/local[4136]: 06DD8179D8C:
  to=<frodo@tipitapa.aoe>, orig_to=<office>, relay=local, delay=1,
  status=sent (delivered to mailbox)
Jul  6 15:39:35 tipitapa postfix/local[4136]: 06DD8179D8C:
  to=<gandalf@tipitapa.aoe>, orig_to=<office>, relay=local, delay=1,
  status=sent (delivered to mailbox)
Jul  6 15:39:35 tipitapa postfix/qmgr[4015]: 06DD8179D8C: removed
```

`postfix` schreibt für den Empfang des Mail nur host/from/msgid an, rcpt und delivery status lässt sich aber über die queue ids leicht verfolgen.

2.4.10 Schick eine Mail an einen nicht existierenden User des Rechners deines Nachbarn und interpretiere die Fehler-Mail, die du zurückbekommst.

```
Date: Wed, 6 Jul 2005 15:47:40 +0200
From: Mail Delivery Subsystem <MAILER-DAEMON>
Subject: Returned mail: see transcript for details
To: aoe@private.oelzant.priv.at

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.5K --]

The original message was received at Wed, 6 Jul 2005 15:47:40 +0200
from aoe@localhost [127.0.0.1]

   ----- The following addresses had permanent fatal errors -----
<asdf@tipitapa3.aoe>
    (reason: 550 <asdf@tipitapa3.aoe>: Recipient address rejected: User
unknown in local recipient table)
...
```

Oder von postfix-seite:

```
From: Mail Delivery System <MAILER-DAEMON@tipitapa3.aoe>
```

```
Subject: Undelivered Mail Returned to Sender
To: root@tipitapa3.aoe

[-- Attachment #1: Notification --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.5K --]

This is the Postfix program at host tipitapa3.aoe.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                        The Postfix program

<asdfgh@oelzant.priv.at>: host comitan.oelzant.priv.at[62.178.208.184]
said:
    550 5.1.1 <asdfgh@oelzant.priv.at>... User unknown (in reply to RCPT TO
command)
...
```

2.4.11 Schreibe in main.cf folgenden Abschnitt dazu, um dem Server Zugriff auf die access Datei zu ermöglichen und restarte den postfix danach:

```
smtpd_recipient_restrictions = permit_mynetworks, reject_invalid_hostname, reject_unknown
                               reject_unknown_sender_domain, reject_unknown_recipient_dom
                               check_recipient_access hash:/etc/postfix/access,
 check_relay_domains
```

2.4.12 Teste es durch eine einfache Access-Regel, die alle Mails an gandalf zurückweist.

```
# echo gandalf@ REJECT > /etc/postfix/access;
  postmap /etc/postfix/access ; \
  /etc/init.d/postfix restart
```

Ergebnis:

```
   ----- The following addresses had permanent fatal errors -----
<gandalf@tipitapa3.aoe>
    (reason: 554 <gandalf@tipitapa3.aoe>: Recipient address rejected:
```

```
Access denied)
```

2.4.13 Schreibe eine Access-Regel für den User `frodo` so, daß die Meldung „Bin Ring zerstören!“ zurückgeliefert und die Mail nicht an frodo zugestellt wird.

```
# echo frodo@ DEFER_IF_PERMIT 'Bin Ring zerstoeren!'> /etc/postfix/access; \
  postmap /etc/postfix/access ; \
  /etc/init.d/postfix restart
```

2.4.14 Teste, ob alles ok ist, indem du frodo eine Mail schickst.

```
$ mutt -s asdasd frodo@tipitapa3.aoe < /dev/null
$ mailq -v
MSP Queue status...
/var/spool/mqueue-client is empty
                Total requests: 0
MTA Queue status...
                /var/spool/mqueue (1 request)
-----Q-ID----- --Size-- -Priority- ---Q-Time---
--------Sender/Recipient--------
j66ESu0r016764        0     120517 Jul  6 16:28
<aoe@private.oelzant.priv.at>
                 (Deferred: 450 <frodo@tipitapa3.aoe>: Recipient address
rejected: Bin Ring zerstoeren!)
                                                <frodo@tipitapa3.aoe>
                 (Deferred: 450 <frodo@tipitapa3.aoe>: Recipient address
rejected: Bin Ring zerstoeren!)
                Total requests: 1
```

2.4.15 Welche verschiedenen Einträge kannst du in der Logdatei erkennen?

```
Jul  6 16:28:50 tipitapa postfix/master[5021]: daemon started -- version
 2.2.3, configuration /etc/postfix
Jul  6 16:28:55 tipitapa postfix/smtpd[5025]: warning: dict_nis_init: NIS
 domain name not set - NIS lookups disabled
Jul  6 16:28:55 tipitapa postfix/smtpd[5025]: connect from brasilia.aoe[192.168.2.99]
Jul  6 16:28:55 tipitapa postfix/smtpd[5025]: warning: support for
  restriction "check_relay_domains" will be removed from Postfix; use
  "reject_unauth_destination" instead
Jul  6 16:28:55 tipitapa postfix/smtpd[5025]: NOQUEUE: reject: RCPT from
  brasilia.aoe[192.168.2.99]: 450 <frodo@tipitapa3.aoe>: Recipient address
  rejected: Bin Ring zerstren!; from=<aoe@oelzant.priv.at>
```

```
  to=<frodo@tipitapa3.aoe> proto=ESMTP
  helo=<chello062178208184.1.15.univie.teleweb.at>
Jul  6 16:28:55 tipitapa postfix/smtpd[5025]: disconnect from
  brasilia.aoe[192.168.2.99]
Jul  6 16:30:24 tipitapa postfix/smtpd[5025]: connect from
  brasilia.aoe[192.168.2.99]
Jul  6 16:30:24 tipitapa postfix/smtpd[5025]: NOQUEUE: reject: RCPT from
  brasilia.aoe[192.168.2.99]: 450 <frodo@tipitapa3.aoe>: Recipient address
  rejected: Bin Ring zerstren!; from=<aoe@oelzant.priv.at>
  to=<frodo@tipitapa3.aoe> proto=ESMTP
  helo=<chello062178208184.1.15.univie.teleweb.at>
Jul  6 16:30:24 tipitapa postfix/smtpd[5025]: disconnect from
  brasilia.aoe[192.168.2.99]
```

Warnungen/Hinweise, Queue Messages, (dis)connects und NOQUEUE (reject). Verfolgung von Mails siehe oben 2.4.9 über Queue IDs.

2.5 Übungen zum Bind DNS Server

2.5.1 Installiere das `bind` Paket.

```
# apt-get install bind
Reading Package Lists... Done
Building Dependency Tree... Done
Sorry, bind is already the newest version.
0 packages upgraded, 0 newly installed, 0 to remove and 18  not upgraded.
```

2.5.2 Kopiere die Datei `named.conf` nach `/etc` und `named.ca`, `named.local`, `matrix.rev` und `matrix.hosts` nach `/var/named`.

```
# (cd /var/named; curl -s -O \
    http://www.mat.univie.ac.at/~martin/lehre/ss05/pp/dns/matrix.rev)
# (cd /var/named; curl -s -O \
    http://www.mat.univie.ac.at/~martin/lehre/ss05/pp/dns/matrix.hosts)
```

named.conf und localhost setup ist bereits vorhanden ;)

```
zone "matrix" {
        type master;
        file "/var/named/matrix.hosts";
};
zone "23.10.10.in-addr.arpa" {
        type master;
        file "/var/named/matrix.rev";
};
```

Abbildung 2.1: named.conf

2.5.3 Konfiguriere `/etc/named.conf` so, daß dein Rechner Masterserver für die matrix Zone (die sich in der Datei `/var/named/matrix.hosts` befindet) ist. Mach dasselbe für den Reverse Lookup (verwende dazu das Netz 10.10.23.*).

2.5.4 Ändere die Defaultinformationen in /var/named/matrix.hosts und /var/named/matrix.rev auf sinnvolle Werte. Konkret soll später z.B. ein Rechner in der matrix Zone die IP 10.10.23.42 und den Namen test.matrix. haben.

```
# sed -i -e "s/ns.domain/‘hostname‘/" \
    -e "s/domain-admin.domain/hostmaster.‘hostname‘/" \
    /var/named/matrix.hosts /var/named/matrix.rev
# echo test 1D IN A         10.10.23.42 >> /var/named/matrix.hosts
# echo 42      IN PTR test.matrix. >> /var/named/matrix.rev
```

2.5.5 Starte den named.

```
# ndc restart
new pid is 17515
```

2.5.6 Ändere die /etc/resolv.conf: Trage deine Test-Domain matrix in den search Pfad ein (lösche dabei das pclab heraus!) und die Server-IP (10.10.a.b) bei nameserver ein (auch hier den vorhandenen Eintrag entfernen!).

Wieso? host/nslookup haben ohnehin ns parameter ...

```
# sed -i -e ’s/pclab/matrix/’ \
    -e "s/^nameserver.*/nameserver ‘hostname -i‘/" /etc/resolv.conf
```

2.5.7 Versuche, 127.0.0.1 mit host in einen Namen aufzulösen. Welcher Name ist dieser IP zugeordnet?

```
# host 127.0.0.1
1.0.0.127.in-addr.arpa domain name pointer localhost.
# nslookup -q=ptr 1.0.0.127.in-addr.arpa
Server:         127.0.0.1
Address:        127.0.0.1#53

1.0.0.127.in-addr.arpa  name = localhost.
```

2.5.8 Versuche, den Hostnamen und die IP Adresse deines zriXXYYY Rechners aufzulösen. Geht das? Warum (nicht)?

Der Rechner ist seit Aufgabe 2.5.6 sein eigener DNS, hat kein zri.* .mat konfiguriert, hierarchisch vergebener Name ist das auch keiner („wir“ sind schließlich in einem privaten Netz ...), daher kann der Name nicht aufgelöst werden.

2.5.9 Trage nun folgende Rechner in den Nameserver sowohl als Lookup als auch als Reverse Lookup ein:

10.10.23.1 heißt gw

```
# echo gw 1D IN A 10.10.23.1 >> /var/named/matrix.hosts
# echo 1 IN PTR gw.matrix. >> /var/named/matrix.rev
```

gw soll auch als gateway und router erreichbar sein

```
# for i in gateway router; do
    echo $i IN CNAME gw >> /var/named/matrix.hosts ; \
  done
```

10.10.23.2 heißt zion

```
# echo zion 1D IN A 10.10.23.2 >> /var/named/matrix.hosts
# echo 2 IN PTR zion.matrix. >> /var/named/matrix.rev
```

zion soll auch als email, ftp, www und ns erreichbar sein

```
# for i in email ftp www ns ; do
    echo $i IN CNAME zion >> /var/named/matrix.hosts ; \
  done
```

10.10.23.3 heißt neo

```
# echo neo 1D IN A 10.10.23.3 >> /var/named/matrix.hosts
# echo 3 IN PTR neo.matrix. >> /var/named/matrix.rev
```

10.10.23.10 heißt smith und agentsmith.

```
# for i in smith agentsmith ; do
    echo $i IN A 10.10.23.10 >> /var/named/matrix.hosts ; \
    echo 10 IN PTR $i.matrix. >> /var/named/matrix.rev; \
  done
```

Die Mails von neo sollen an Rechner architekt.matrix. (auch eintragen mit selbst gewählter IP) gehen

```
# echo architekt 1D IN A 10.10.23.33 >> /var/named/matrix.hosts
# echo neo 1D IN MX 666 architekt >> /var/named/matrix.hosts
# echo 33 IN PTR architekt.matrix. >> /var/named/matrix.rev
```

2.5.10 Mails an die gesamte Matrix sollen im Allgemeinen an den Rechner zion gehen.

```
# echo @ 1D IN MX 0 zion >> /var/named/matrix.hosts
```

2.5.11 10.10.23.99 heißt orakel

```
# echo orakel 1D IN A 10.10.23.99 >> /var/named/matrix.hosts
# echo 99 IN PTR orakel.matrix. >> /var/named/matrix.rev
```

2.6 Teste die Einträge deiner Domain mit dem host Utility. Schreibe im speziellen Abfragen, die folgendes herausfinden:

```
# ndc reload
```

2.6.1 Den Namen von 10.10.23.99

```
# host 10.10.23.99
99.23.10.10.in-addr.arpa domain name pointer orakel.matrix.
```

Die IP von agentsmith

```
# host agentsmith.matrix
agentsmith.matrix has address 10.10.23.10
```

Ob es sich bei agentsmith um einen CNAME handelt

Eine Anforderung, dass agentsmith ein CNAME sein sollte, war auch bei mehrmaligem Lesen von Aufgabe 2.5.9 nicht ersichtlich, und gemäss RFC wurden zwei A/PTR eingetragen. (Interpretation siehe auch *http://archives.neohapsis.com/archives/postfix/2002-08/2177.html* [1]

```
# host -t cname agentsmith.matrix
#
```

Zum Ausgleich ein echter `CNAME`:

```
# host -t cname ns.matrix
ns.matrix is an alias for zion.matrix.
```

Welcher Rechner für Emails an neo zuständig ist.

```
# host -t mx neo.matrix
neo.matrix mail is handled by 666 architekt.matrix.
```

2.6.2 Teste einige Einträge auch mit dem dig Tool und interpretiere die Ausgabe.

Das utility `dig` produziert ebenso wie `host -l -v -t any ...` hübschen zonzefile-kompatiblen output, zeigt request und response an und listet die einträge säuberlich auf. z. B.

```
# dig neo.matrix

; <<>> DiG 9.2.4 <<>> neo.matrix
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1307
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;neo.matrix.                    IN      A

;; ANSWER SECTION:
neo.matrix.             86400   IN      A       10.10.23.3

;; AUTHORITY SECTION:
matrix.                 86400   IN      NS      comitan.aoe.
```

---

[1] The consensus on the BIND users list / newsgroup is that multiple PTRs are legal, but almost always unnecessary, and more likely to cause problems than to solve them in actual practice.

```
;; ADDITIONAL SECTION:
comitan.aoe.            86400   IN      A       192.168.2.1

;; Query time: 35 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jul  6 17:31:18 2005
;; MSG SIZE  rcvd: 85
```

Hier sind bei entsprechender Vergrösserung deutlich die Fühler des Insekts zu sehen, leider reicht die Objektivapertur nicht aus, um auch die Facettenaugen erkennen zu können.

2.6.3 Was kann man mit dem nslookup Tool machen?

Im wesentlichen das gleiche wie mit host, die Syntax ist alelrdings eine andere und der Zonefile-artige Output ist (afaik) nicht verfügbar. z. B.

```
# nslookup  -q=any matrix.
Server:         127.0.0.1
Address:        127.0.0.1#53

matrix  nameserver = comitan.aoe.
matrix
        origin = comitan.aoe
        mail addr = hostmaster.comitan.aoe
        serial = 2004040703
        refresh = 28800
        retry = 14400
        expire = 3600000
        minimum = 86400
matrix  mail exchanger = 0 zion.matrix.
```

2.7 Übungen zum NFS Server

2.7.1 Wie findet man heraus, ob NFS schon installiert ist?

```
# rpcinfo -p|grep -E "nfs|mount"
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100005    1   udp    605  mountd
    100005    1   tcp    608  mountd
    100005    2   udp    605  mountd
```

```
    100005    2   tcp    608  mountd
    100005    3   udp    605  mountd
    100005    3   tcp    608  mountd
```

2.7.2 Starte den NFS Server!

```
# /etc/init.d/portmap restart;/etc/init.d/nfs-kernel-server restart
Stopping portmap daemon: portmap.
Starting portmap daemon: portmap.
Stopping NFS kernel daemon: mountd nfsd.
Unexporting directories for NFS kernel daemon...done.
Exporting directories for NFS kernel daemon...done.
Starting NFS kernel daemon: nfsd mountd.
```

2.7.3 Vergewissere dich einerseits durch Ansehen der Serverkonfiguration, andererseits durch einen showmount Befehl, daß der Server noch keine Verzeichnisse exportiert.

```
# showmount -e
Export list for comitan.aoe:
```

2.7.4 Erstelle ein Verzeichnis /mytmp, das du ohne Optionenliste an alle im PC Labor freigibst.

```
# mkdir /mytmp
# chmod 1777 /mytmp
# echo "/mytmp 10.10.23.0/24()" >> /etc/exports; exportfs -r; \
    showmount -e|grep mytmp
exportfs: /etc/exports [31]: No 'sync' or 'async' option specified for
export "10.10.23.0/24:/mytmp".
  Assuming default behaviour ('sync').
  NOTE: this default has changed from previous versions
/mytmp                  10.10.23.0/24
```

2.7.5 Finde einerseits heraus, ob das Verzeichnis generell read-write oder read-only ist, andererseits, ob root darin beliebig schreiben darf oder nicht! (kurz gesagt: Welche Defaultwerte gelten für einen Export, wenn man keine Optionen angibt?)

```
[root@df root]# mount brasilia:/mytmp /mnt/mytmp
[root@df root]# cd /mnt/mytmp
[root@df mytmp]# touch asd
touch: cannot touch `asd': Permission denied
```

```
> touch /mnt/mytmp/asd
touch: cannot touch ‘/mnt/mytmp/asd’: Permission denied
```

Default ist also `ro,root_squash,sync`

2.7.6 Erstelle ein Verzeichnis /myspace und /mp3s und lege einige Dateien hinein.

```
# apt-get install mldonkey
# mlnet
# telnet localhost 4000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Welcome on mldonkey command-line

Use ? for help

MLdonkey command-line:
> s mp3
> vr
...
1011 sources, total available 18.99G
> d 1 2 3 ...
```

2.7.7 Gib `/myspace` an das gesamte PCLabor zum Lese- und Schreibzugriff frei.

```
# sed -i -e 's#^/mytmp.*#/mytmp 192.168.2.0/24(rw,root_squash,sync)#' \
  /etc/exports
# echo "/mp3s 192.168.2.0/24(ro,no_root_squash,sync)" >> /etc/exports
# exportfs -r
```

2.7.8 Versuche, /myspace deines Nachbarn auf deinem Rechner nach /mnt/tmp zu mounten und eine Datei hineinzukopieren (Verzeichnisrechte beachten!)

Verzeichnisrechte siehe Aufgabe 2.7.4.

```
> touch /mnt/mytmp/asdf
# touch asd
# ls -ldn asd
-rw-r--r--  1 65534 65534 0 Jul  6 18:19 asd
```

Facit: squashed access heist remapping auf anon user (nobody o. ä.)

2.7.9 Gib /mp3s ausschließlich an deinen Nachbarn nur zum Lesezugriff frei.

siehe Aufgabe 2.7.7

2.7.10 Darf dein Nachbar als root trotzdem darauf schreiben?

```
# mount brasilia:/mp3s /mnt/mytmp
# ls -l /mnt/mytmp
total 0
-rw-r--r--  1 postgres postgres 0 Jul  6 18:19 asd
-rw-r--r--  1 aoe      aoe      0 Jul  6 18:20 asdf
# touch /mnt/mytmp/sdfsdf
touch: cannot touch '/mnt/mytmp/sdfsdf': Permission denied
```

Nein, natürlich nicht, ro gilt auch (und besonders, bei root_squash) für root. nur ein Verzeichnis mit permissions a-w, aber rw,no_toot_squash exportiert könnte von remote root überschreiben werden.

2.7.11 Füge in der /etc/exports die Option root_squash beim /myspace Eintrag hinzu. Kannst du jetzt als root (nach exportfs -r!) noch Dateien in /myspace anlegen?

Siehe vorherige Frage, das hatte ich vorher eigentlich auch schon :)

Mit root_squash nur squashed auf nobody, weil das dir (bei mir) tmp-berechtigungen hat; nicht jedoch, wenn die permissions Schreibzugriff fuer `others` nicht zulassen.

Mit no_toot_squash könnte root natürlich tatsächlich uid-0-Dateien anlegen/bearbeiten (sieht bei den nfsroots natuerlich so aus).

2.8 Übungen zum NIS Server

2.8.1 Installiere den YP Server und starte ihn.

```
# apt-get install nis
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  nis
0 upgraded, 1 newly installed, 0 to remove and 40 not upgraded.
Need to get 256kB of archives.
After unpacking 897kB of additional disk space will be used.
Get:1 http://ftp.at.debian.org unstable/main nis 3.13-3 [256kB]
```

```
Fetched 256kB in 1s (149kB/s)
Preconfiguring packages ...
Selecting previously deselected package nis.
(Reading database ... 180514 files and directories currently installed.)
Unpacking nis (from .../nis_3.13-3_powerpc.deb) ...
Setting up nis (3.13-3) ...
Configuring nis
---------------

You now need to choose a NIS domainname for your system. If you want this
machine to just be a client, enter the NIS domainname of your network.
Otherwise
choose an appropriate NIS domainname.

Enter your NIS domain aoedomain



Your system needs more configuration.

Your system has not yet been completely configured as a NIS client - you
need to
setup /etc/nsswitch.conf and/or /etc/passwd and /etc/group. Please read
/usr/share/doc/nis/nis.debian.howto.gz to find out how.

Setting NIS domainname to: aoedomain
Starting NIS services: ypbind
```

2.8.2 Initialisiere einen Master Server.

```
# sed -e 's/^\(NISSERVER=\).*/\1master/' /etc/default/nis
# /etc/init.d/nis restart
Starting NIS services: ypserv yppasswdd ypxfrd ypbind
```

2.8.3 Bearbeite die /var/yp/securenets so, daß nur die Einträge für 127.0.0.1, deinen eigenen Rechner und den deines Nachbarn eingetragen sind. Restarte den ypserv.

```
# sed -ie 's/^0.0.0.0/255.255.255.0 192.168.2.0/' /etc/ypserv.securenets
# /etc/init.d/nis restart
Starting NIS services: ypserv yppasswdd ypxfrd ypbind [binding to YP server
.......... backgrounded]
```

2.8.4 Trage den Rechner deines Nachbarn als YP Server in /etc/yp.conf und /var/yp/ypservers ein.

```
# echo -e "domain aoedomain server 192.168.3.44\nypserver 192.168.3.44" \
   > /etc/yp.conf
# echo aoedomain > /etc/defaultdomain
```

2.8.5 Überprüfe mit den yp Tools, ob du z.b. die passwd oder group Map deines Nachbarn lesen kannst (auch wenn diese vermutlich noch leer sind).

```
# ypcat passwd
frodo:x:1002:1002:hobbit,,,:/home/frodo:/bin/bash
gandalf:x:1003:1003:wizard,,,:/home/gandalf:/bin/bash
```

2.8.6 Lege einen User mit einer User-ID ≥ MINUID (die du in /var/yp/Makefile findest) an (mittels der Option -u bei adduser oder useradd).

Siehe Aufgabe 2.4.4, UID_MIN in `login.defs` und MINUID in `/var/yp/Makefile` stimmen ferner bereits überein.

2.8.7 Überprüfe, ob du den User deines Nachbarn per YP sehen kannst.

Siehe Übung 2.8.5 zum Thema `ypcat`

2.8.8 Starte den `yppasswdd`.

Dieser daemon wird bei Debian GNU/Linux automatisch gestartet, siehe z. B. `nis restart` in Aufgabe 2.8.3

2.8.9 Versuche, das Paßwort des auf dem Nachbarrechner angelegten Users per YP zu ändern.

Das geht, wenn `nsswitch.conf` ok ist (nis einträge, nona), rpc.yppasswdd am Server läuft und der Client den Server per IP-Adresse kennt (. . .)

```
gandalf@master:~$ yppasswd
Changing NIS account information for gandalf on tipitapa.
Please enter old password:
Changing NIS password for gandalf on tipitapa.
Please enter new password:
Please retype new password:

The NIS password has been changed on tipitapa.
```

```
[gandalf@client mnt]$ yppasswd
...
The NIS password has been changed on tipitapa.
[root@df mnt]# yppasswd  gandalf
Changing NIS account information for gandalf on tipitapa.
Please enter root password:
Changing NIS password for gandalf on tipitapa.
Please enter new password:
Please retype new password:

The NIS password has been changed on tipitapa.
```

```
[root@client mnt]# yppasswd  gandalf
Changing NIS account information for gandalf on tipitapa.
Please enter root password:
Changing NIS password for gandalf on tipitapa.
Please enter new password:
Please retype new password:

The NIS password has been changed on tipitapa.
```

2.8.10 Versuche, für diesen Benutzer Finger Information einzugeben.

Abhängig vom `YPCHANGEOK` setting („`chsh`“, „`chfn`“, „`chsh,chfn`“) ist das möglich oder nicht. Die Variable ist bei Debian GNU/Linux in `/etc/default/nis` gesetzt und wird von `/etc/init.d/nis` in `-e` Variablen umgebaut, die `$YPPWDDIR` auf der commandline mitbekommt.

2.9 Übungen zum Squid Proxy Server

2.9.1 Installiere das Squid Paket.

```
# apt-get install squid
...
FATAL: Could not determine fully qualified hostname.
  Please set 'visible_hostname'
...
/var/lib/dpkg/info/squid.postinst: line 114:  7337 Aborted /usr/sbin/squid -z
...
# echo visible_hostname tipitapa.aoe >> /etc/squid/squid.conf
```

2.9.2 Setze den Port des Squid Servers auf 8080.

```
# grep http_port /etc/squid/squid.conf
```

```
#  TAG: http_port
#       internal address:port in http_port. This way Squid will only be
# http_port 3128
#               cache_peer hostname type http_port icp_port
#               http_port
# echo http_port 8080 >> /etc/squid/squid.conf
```

2.9.3 Starte den Proxyserver.

```
# /etc/init.d/squid restart
Restarting proxy server: Creating squid spool directory structure
2005/07/06 20:40:40| Creating Swap Directories
squid.
# netstat -an|grep 8080
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
```

2.9.4 Konfiguriere den Proxyserver in deinem Webbrowser.

```
# http_proxy=http://localhost:8080/ lynx -dump www.apple.com > /dev/null
# http_proxy=http://localhost:8080/ lynx -dump www.apple.com > /dev/null
```

2.9.5 Gehe auf eine beliebige Webseite und finde heraus, ob der Proxy tatsächlich verwendet wird.

```
# cat /var/log/squid/access.log
1120675607.563    897 127.0.0.1 TCP_MISS/200 13541 GET
  http://www.apple.com/ - DIRECT/17.254.0.91 text/html
1120675624.223      1 127.0.0.1 TCP_HIT/200 13539 GET http://www.apple.com/
  - NONE/- text/html
```

2.9.6 Funktioniert der Zugriff auch von einem anderen Rechner aus? Probier es mit deinem Nachbarn aus!

```
1120675801.708      6 192.168.2.10 TCP_DENIED/403 1391 GET
  http://www.apple.com/ - NONE/- text/html
```

Nein, die Default-konfiguration verweigert korrekterweise den Zugang von Aussen.

2.9.7 Wenn es nicht funktioniert, versuche in der Konfiguration herauszufinden, wie man den Zugang für weitere Rechner außer localhost ermöglicht und konfiguriere den Squid entsprechend!

```
# sed -ie '1s/.*/acl neighbour src 192.168.2.10\n\
```

```
    http_access allow neighbour\n&/' /etc/squid/squid.conf; \
  killall -HUP squid
# tail -1 /var/log/squid/access.log
1120676255.814      9 192.168.2.10 TCP_HIT/200 13540 GET
  http://www.apple.com/ - NONE/- text/html
```

2.10 Übungen zum Samba Server

2.10.1 Installiere das Samba-Server-Paket (samba-common und samba-client sind bereits installiert).

```
# apt-get install samba
Reading Package Lists... Done
Building Dependency Tree... Done
Suggested packages:
  samba-doc
The following NEW packages will be installed:
  samba
0 upgraded, 1 newly installed, 0 to remove and 40 not upgraded.
Need to get 0B/2736kB of archives.
After unpacking 6820kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously deselected package samba.
(Reading database ... 180485 files and directories currently installed.)
Unpacking samba (from .../samba_3.0.14a-5_powerpc.deb) ...
Setting up samba (3.0.14a-5) ...
Starting Samba daemons: nmbd.
```

2.10.2 Starte den Samba-Server und sieh dir die Start-Konfiguration an. Versuche, mittels `smbclient` auf den Server zuzugreifen und dir die verfügbaren Freigaben anzeigen zu lassen. (Du benötigst dazu noch keinen Username/Password, bestätige beim Passwort-Prompt einfach mit ENTER.) Du kannst sowohl DNS- als auch NetBIOS-Hostnamen verwenden.

`-N` unterdrückt den pw-prompt

```
# smbclient -L tipitapa -N
Anonymous login successful
Domain=[DEBIAN_FANS] OS=[Unix] Server=[Samba 3.0.14a-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
```

```
        IPC$            IPC       IPC Service (tipitapa server (Samba
3.0.14a-Debian))
        ADMIN$          IPC       IPC Service (tipitapa server (Samba
3.0.14a-Debian))
        lp              Printer   Generic dot-matrix printer entry
Anonymous login successful
Domain=[DEBIAN_FANS] OS=[Unix] Server=[Samba 3.0.14a-Debian]

        Server               Comment
        ---------            -------
        TIPITAPA             tipitapa server (Samba 3.0.14a-Debian)

        Workgroup            Master
        ---------            -------
        DEBIAN_FANS
```

2.10.3 Sieh dir die Einträge in den Logfiles zu deinen gerade getätigten Zugriffen an.

Ein (leeres) logfile für den Source Host wird in /var/log/samba angelegt, ein Eintrag wird in /var/log/syslog erstellt:

```
Jul  6 21:12:02 tipitapa smbd[7649]: connect from 127.0.0.1 (127.0.0.1)
Jul  6 21:14:10 tipitapa smbd[7659]: connect from 192.168.2.10 (192.168.2.10)
```

2.10.4 Verwende die Man-Pages und Internetressourcen (Samba Projektseite, Google o.ä.) dazu herauszufinden, was der Parameter "`os level`" (smb.conf) beeinflusst bzw. welche Eigenart des SMB-Protokolls dahinter steckt.

```
# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
;   os level = 20
```

Dieser esoterische Parameter entscheidet bei Hahnenkämpfen, welcher Gockel gewinnt.

Aus dem "Official Samba-3 HOWTO and Reference Guide" [2]:

4.4. Samba ADS Domain Control

The `os level` must be set at or above a value of 32. A Domain Controller must be the Domain Master Browser, must be set in user mode security, must support Microsoft-compatible encrypted passwords, and must provide the network logon service (domain logons). Encrypted passwords must be

---

[2] *http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf*

enabled. For more details on how to do this, refer to[1191] Account Information Databases.

2.10.5 Lege eine Public-Freigabe an, auf die jeder Lesezugriff hat. Versuche, auf diese Freigabe mit smbclient zuzugreifen und eine Datei von der Freigabe auf deinen Rechner zu kopieren. Achte darauf, dass dazu auch die lokalen UNIX-Rechte passen müssen.

```
# mkdir /mnt/stuff
# echo whatever > /mnt/stuff/newfile
# echo '[myexport]
    comment=various stuff
    path=/mnt/stuff
    public=yes
    writable=no' >> /etc/samba/smb.conf ; \
  killall -HUP smbd

$ smbclient //tipitapa/myexport -N -c ls
Anonymous login successful
Domain=[DEBIAN_FANS] OS=[Unix] Server=[Samba 3.0.14a-Debian]
  .                                   D        0  Wed Jul  6 21:32:22 2005
  ..                                  D        0  Wed Jul  6 21:32:05 2005
  newfile                                      9  Wed Jul  6 21:32:22 2005

                49569 blocks of size 262144. 1113 blocks available

# smbclient //tipitapa/myexport -N -c "get newfile -"
Anonymous login successful
Domain=[DEBIAN_FANS] OS=[Unix] Server=[Samba 3.0.14a-Debian]
whatever
getting file \newfile of size 9 as - (0.3 kb/s) (average 0.3 kb/s)
```

Bitte den Inhalt der Datei “`whatever`” zu beachten.

2.10.6 Mounte eine Freigabe deines eigenen Servers z.B. unter /mnt/tmp.

```
# apt-get install smbfs # fuer smbmount
# mkdir /mnt/mytmp
# mount //tipitapa/myexport /mnt/mytmp -o password=
Anonymous login successful
```

Siehe auch die inoffiziellen symlink-Patches [3].

---

[3] *http://lists.samba.org/archive/samba/2000-July/019850.html*

2.10.7 Passe die Freigabe der Home-Verzeichnisse deinen Vorstellungen nach an und starte den Samba-Server neu. Lege dir einen normalen UNIX-Benutzer an und aktiviere diesen mit smbpasswd für Samba. Mounte dann sein Home-Verzeichnis in das Verzeichnis /mnt/mydir (das du vorher noch anlegen mußt) und lege einige Dateien und Verzeichnisse an.

```
# sed -ie 's/^.*encrypt passwords = false/encrypt passwords = true/' \
    /etc/samba/smb.conf
# smbpasswd -a gandalf
# smbpasswd gandalf
New SMB password:
Retype new SMB password:
# /etc/init.d/samba restart
# mv /mnt/mytmp /mnt/mydir
# mount //tipitapa/gandalf /mnt/mydir -o username=gandalf,password=wizard
# sed -ie '/homes/,/writables/s/writable = no/writable = yes/' \
    /etc/samba/smb.conf
# ls -la /mnt/mydir/
total 28
drwxr-xr-x   1 root    root    4096 Jul  6 22:02 .
drwxr-xr-x  12 root    root    4096 Jul  6 21:46 ..
-rw-r--r--   1 gandalf gandalf  266 Jul  6 15:26 .alias
# mkdir /mnt/mytmp/asd
# echo Hello World > /mnt/mytmp/asd
# cat /mnt/mytmp/asd/hello
Hello World
```

2.10.8 Mounte eine Freigabe deines Nachbarn unter /mnt/nachbar (auch anlegen). Lasse dir dazu von deinem Nachbarn einen User inkl. Password anlegen.

Siehe vorige Aufgabe

2.10.9 Funktioniert der Zugriff auf deinen Server von einem unter Windows gebooteten PC-Labor Rechner aus?

Keine Ahnung, sowas habe ich nicht

Kapitel 3

“Seminararbeit” inn (NNTP Server) mit Anbindung an ein Webforum

3.1 Motivation

Da es lange her ist, seit ich den letzten innd installiert habe und ich eine sinnvolle Anwendung dafür habe (Umbau von vbnntpd), erscheint mir Rich $alz’s InterNetNews daemon am sinnvollsten eingehender zu bearbeiten. Debian GNU/Linux hat allerdings `inn` Pakete, ich verkürze mir die Installation dementsprechend mit dpkg-source.

Nach einigen Versuchen stellte sich heraus, dass `inn` Version 2 notwendig war, da hier erweiterte Authentifizierungsmöglichkleiten über externe Programme möglich waren, die für die Zukunft notwendig sein werden, Konfiguration siehe unten.

Natürlich wäre es sportlicher, wieder einmal unter `AIX 4.3` zu kompilieren, aber ich weiss, dass ich nicht der einzige bin, der dort Spaß mit dem Linker hat (dynlibs unter AIX sind . . . anders).

3.2 Installation

```
# apt-get source inn2
Building dependency tree... Done
Need to get 1911kB of source archives.
Get:1 http://ftp.at.debian.org unstable/main inn2 2.4.2-3 (dsc) [741B]
Get:2 http://ftp.at.debian.org unstable/main inn2 2.4.2-3 (tar) [1864kB]
Get:3 http://ftp.at.debian.org unstable/main inn2 2.4.2-3 (diff) [46.4kB]
Fetched 1911kB in 24s (76.5kB/s)
dpkg-source: extracting inn2 in inn2-2.4.2
dpkg-source: unpacking inn2_2.4.2.orig.tar.gz
```

```
dpkg-source: applying ./inn2_2.4.2-3.diff.gz
# cd inn2-2.4.2/
# dpkg-buildpackage
dpkg-buildpackage: source package is inn2
dpkg-buildpackage: source version is 2.4.2-3
dpkg-buildpackage: source changed by Marco d'Itri <md@linux.it>
dpkg-buildpackage: host architecture powerpc
dpkg-checkbuilddeps: Unmet build dependencies: libdb4.3-dev
dpkg-buildpackage: Build dependencies/conflicts unsatisfied; aborting.
dpkg-buildpackage: (Use -d flag to override.)
```

um alle dependencies zu erfüllen, brauche ich also noch `libdb4.3-dev`

```
# apt-get install libdb4.3-dev
...
# dpkg-buildpackage
dpkg-buildpackage: source package is inn2
...
(cd build-tree/inn-2.4.2; /usr/bin/make  )
make[1]: Entering directory `/usr/src/inn2-2.4.2'
(cd build-tree/inn-2.4.2; /usr/bin/make install \
DESTDIR=/usr/src/inn2-2.4.2/debian/inn2  )
make[2]: Entering directory `/usr/src/inn2-2.4.2/build-tree/inn-2.4.2'
...
cd include   && /usr/bin/make all
cd lib       && /usr/bin/make all
cd storage   && /usr/bin/make library
cd history   && /usr/bin/make all
cd innd      && /usr/bin/make all
cd nnrpd     && /usr/bin/make all
cd innfeed   && /usr/bin/make all
cd control   && /usr/bin/make all
cd expire    && /usr/bin/make all
cd frontends && /usr/bin/make all
cd backends  && /usr/bin/make all
cd authprogs && /usr/bin/make all
cd scripts   && /usr/bin/make all
cd storage   && /usr/bin/make programs
cd doc     && /usr/bin/make all
cd samples && /usr/bin/make all
cd site    && /usr/bin/make all
...
make[2]: Leaving directory `/usr/src/inn2-2.4.2/build-tree/inn-2.4.2'
make[1]: Leaving directory `/usr/src/inn2-2.4.2'
```

```
...
dh_installdeb -a
dh_shlibdeps -a --exclude=ckpasswd
dh_gencontrol -a
dpkg-gencontrol: warning: unknown substitution variable ${PERLAPI}
dpkg-gencontrol: warning: unknown substitution variable ${misc:Depends}
dpkg-gencontrol: warning: unknown substitution variable ${misc:Depends}
dh_gencontrol -a -- \
    -VPERLAPI=$(perl -MConfig -e 'print "perlapi-$Config{version}"')
dpkg-gencontrol: warning: unknown substitution variable ${misc:Depends}
dpkg-gencontrol: warning: unknown substitution variable ${misc:Depends}
dh_md5sums -a
dh_builddeb -a
dpkg-deb: building package `inn2' in `../inn2_2.4.2-3_powerpc.deb'.
dpkg-deb: building package `inn2-ssl' in `../inn2-ssl_2.4.2-3_powerpc.deb'.
dpkg-deb: building package `inn2-inews' in `../inn2-inews_2.4.2-3_powerpc.deb'.
dpkg-deb: building package `inn2-dev' in `../inn2-dev_2.4.2-3_powerpc.deb'.
 dpkg-genchanges
dpkg-genchanges: not including original source code in upload
dpkg-buildpackage: binary and diff upload (original source NOT
included)
signfile ../inn2_2.4.2-3_powerpc.changes
sh: pgp: command not found
# dpkg -i ../inn2*.deb
(Reading database ... 180364 files and directories currently installed.)
Preparing to replace inn2-dev 2.4.2-3 (using
.../inn2-dev_2.4.2-3_powerpc.deb) ...
Unpacking replacement inn2-dev ...
Selecting previously deselected package inn2-inews.
Unpacking inn2-inews (from .../inn2-inews_2.4.2-3_powerpc.deb) ...
Selecting previously deselected package inn2-ssl.
Unpacking inn2-ssl (from .../inn2-ssl_2.4.2-3_powerpc.deb) ...
Selecting previously deselected package inn2.
Unpacking inn2 (from ../inn2_2.4.2-3_powerpc.deb) ...
Setting up inn2-dev (2.4.2-3) ...
Setting up inn2-inews (2.4.2-3) ...
Setting up inn2 (2.4.2-3) ...
Starting news server: done.

Setting up inn2-ssl (2.4.2-3) ...
```

3.3 Konfiguration

`/usr/share/doc/inn2/INSTALL.gz` ist das offizielle Dokument dafür.

Die Konfigurationsdateien legt Debian GNU/Linux in `/etc/news` ab. Da der `pathhost` Wert in `/etc/news/inn.conf` auf „`unknown` steht, muss diser noch konfiguriert werden. (eigener Name im `path` header). `inews` beschwert sich mangels `server: localhost` Eintrag noch, dass es keine Artikel posten kann:

```
# sed -ie ’s/^pathhost.*/pathhost: ’‘hostname‘’/’ /etc/news/inn.conf
# sed -ie ’s/^#server:.*/server: localhost/’ /etc/news/inn.conf
$ lynx -dump nntp://localhost/|grep nntp
   1. nntp://localhost/control
   2. nntp://localhost/control.cancel
   3. nntp://localhost/control.checkgroups
   4. nntp://localhost/control.newgroup
   5. nntp://localhost/control.rmgroup
   6. nntp://localhost/junk
   7. nntp://localhost/local.general
   8. nntp://localhost/local.test
$ echo dummy | inews -n local.test -f alexander@oelzant.priv.at -t "test ignore"
$ lynx -dump nntp://localhost/local.test | grep ignore
     * [2]"test ignore" - alexander@oelzant.priv.at
```

Um auch Zugang von aussen zu erlauben, ist es dann notwendig, `/etc/news/reader.conf` anzupassen. Es sollen alle lesen, aber nur authentifizierte BenutzerInnen schreiben können. In `/usr/share/doc/inn2/perl-hook.gz` wird ein Mechanismus beschrieben, der `perl` ähnlich wie bei Apache `mod_perl` direkt ausführt, auch andere Executables könnten aber über `auth:` aufgerufen werden. In einer `auth{}` Gruppe kann dann `perl_auth: /path/to/script` als Authenticator verwendet werden.

```
# echo 'auth "readers" {
hosts: "*"
default: "<read-only>"
}
access "read-only" {
users: "<read-only>"
read: "*"
}
auth "users" {
hosts: "*"
perl_auth: "/usr/lib/news/auth.dir/asdf.pl"
default: "<users>"
}
```

```
access "read-write" {
users: "<users>"
newsgroups: "*"
access: RPA
}' >> /etc/news/readers.conf
```

/usr/lib/news/auth.dir/asdf.pl:

```
#!/usr/bin/perl
# aoe 2005

require '/usr/lib/news/innshellvars.pl';
use vars qw(%attributes %authcodes %users);
use strict;
use warnings;

# does not do anything useful for now, but nnrpd needs it
sub auth_init {
}

sub authenticate {
        my %response = (
                        "ok"   => [281,'authenticated'],
                        "fail" => [502,'authentication unsuccessful']
                       );
# this will be modified to use db access in the near future

        if ($attributes{"username"} eq "aoe" &&
    $attributes{"password"} eq "pass") {
                return(@{$response{'ok'}});
        } else {
                return(@{$response{'fail'}});
        }
}
```

3.3.1 SSL Konfiguration

Gem\"ass {\tt /usr/share/doc/inn2-ssl/README.Debian} muss
{\tt /usr/lib/news/bin/nnrpd-ssl} (leider ist dort der falsche Pfad
angegeben) mit Option {\tt -S} von inetd oder sonstwie aufgerufen werden,
dazu braucht es ein x509-Zertifikat. Da f\"ur den Zielserver noch keines
existiert, wird eines erstellt. Zum Schluss wird noch das {\tt
nnrpd}-binary durch einen Symlink auf {\tt nnrpd-ssl} ersetzt, da es
offenbar keine andere M\"oglichkeit gibt, {\tt innd} einen {\tt

```
STARTTLS}-f\"ahigen reader daemon unterzujubeln.

\begin{verbatim}
# mkdir /etc/news/ca
# cd /etc/news/ca
# chmod 600 .
# openssl genrsa -out ca.key 1024
# echo -e "AT\n\nWien\nFSINF CA\n\ntigerente.htu.tuwien.ac.at\n"\
"rootca@tigerente\n\n" \
    | openssl req -new -key ca.key -out ca.csr 2>/dev/null
# mkdir ca.db.certs
# cat /dev/null > ca.db.index
# cat /dev/null > ca.db.index.attr
# echo 01 > ca.db.serial
# echo > ca.config '
extension =
[ ca ]
default_ca              = CA_own
[ CA_own ]
dir                     = .
certs                   = $dir
new_certs_dir           = $dir/ca.db.certs
database                = $dir/ca.db.index
serial                  = $dir/ca.db.serial
RANDFILE                = $dir/ca.db.rand
certificate             = $dir/ca.crt
private_key             = $dir/ca.key
default_days            = 10000
default_crl_days        = 30
default_md              = md5
preserve                = no
policy                  = policy_anything
x509_extensions = usr_cert
[ policy_anything ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
[ usr_cert ]
'
# openssl x509 -req -days 3650 -in ca.csr -signkey ca.key -out ca.crt
```

```
Signature ok
subject=/C=AT/ST=Some-State/L=Wien/O=FSINF
CA/CN=tigerente.htu.tuwien.ac.at/emailAddress=rootca@tigerente
Getting Private key
# openssl genrsa -out /etc/news/nnrpd-key.pem 1024
# echo -e "AT\n\nWien\nTigerente\n\ntigerente.htu.tuwien.ac.at\n"\
"usenet@tigerente.htu.tuwien.ac.at\n\n" \
     | openssl req -new -key /etc/news/nnrpd-key.pem -out nnrpd-cert.csr \
     2>/dev/null
# yes | openssl ca -config ca.config -days 10000 -in nnrpd-cert.csr \
    -cert ca.crt -keyfile ca.key -out /etc/news/nnrpd-cert.pem
Using configuration from ca.config
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'AT'
stateOrProvinceName   :PRINTABLE:'Some-State'
localityName          :PRINTABLE:'Wien'
organizationName      :PRINTABLE:'Tigerente'
commonName            :PRINTABLE:'tigerente.htu.tuwien.ac.at'
emailAddress          :IA5STRING:'usenet@tigerente.htu.tuwien.ac.at'
Certificate is to be certified until Nov 23 13:16:19 2032 GMT (10000 days)
Sign the certificate? [y/n]:

1 out of 1 certificate requests certified, commit? [y/n]Write out database
with 1 new entries
Data Base Updated
# cp ca.crt /etc/news/nnrpd-ca-cert.pem
# chown news:news /etc/news/nnrpd-key.pem
# chmod 600 /etc/news/nnrpd-key.pem
# chown news:news /etc/news/nnrpd-cert.pem
# chmod 600 /etc/news/nnrpd-cert.pem
# echo nntps   stream  tcp nowait news.news /usr/lib/news/bin/nnrpd-ssl \
    nnrpd -S >> /etc/inetd.conf
# killall -HUP inetd
$ openssl s_client -host localhost -port 563 \
    -CAfile /etc/news/nnrpd-ca-cert.pem 2>&1 | grep Verify
    Verify return code: 0 (ok)
# mv /usr/lib/news/bin/nnrpd /usr/lib/news/bin/nnrpd.old
# ln -s nnrpd-ssl /usr/lib/news/bin/nnrpd
```

3.4 Befüllen des Newsspool aus der Datenbank

Um die Datenbank erst einmal in den Spool zu bekommen, muss `artcutoff` in `inn.conf` von 10 (Tagen) auf (z. B.) 10000 gesetzt werden (offenbar auch noch in `expire.ctl`, `incoming.conf` und `storage.conf`). `maxartsize` hat für die Attachments weiter unten Bedeutung.

Das vorhandene script produziert so etwas wie active und newsgroup files, feinere Granularität und `actsync` kommen bei Bedarf.

Mit ein paar Modifikationen können nun die Artikel in den spool eingespielt werden; das script ist zwar noch immer buggy und inn meint alle paar tausend postings, dass die history kaputt wäre ...[1]

```
# ctlinnd go go go
ctlinnd: Wrong reason
# tail -2 /var/log/news/news.err
Jul  9 01:49:28 tigerente innd: SERVER throttle File exists writing SMstore
  file -- throttling
Jul  9 01:49:28 tigerente innd: SERVER cant store article: File exists

# /etc/init.d/inn2 stop
# su -c "/usr/lib/news/bin/makedbz -s 218670 -o" news
# /etc/init.d/inn2 start
```

oder, etwas weniger interaktiv (`vbnntp/vbnntpd.10` fẗtert hier per nntp artikel an localhost:119, die älter als timestamp $lastold sind) ...

```
lastold=1;
while [ $lastold -lt ‘date +%s‘ ]; do
  /etc/init.d/inn2 stop;
su -c "/usr/lib/news/bin/makedbz -s 218670 -o" news;
/etc/init.d/inn2 start;
newlog=‘su -c "cd /home/aoe; /home/aoe/vbnntp/vbnntpd.10 -f "$lastold" \
  aoe | tail‘;
lastold=${newlog#*-};
lastold=${lastold%%-*};
echo  $lastold;
sleep 1;
done
```

Da die Attachments noch Probleme machen, werden diese geloescht und neu eingespielt.

---

[1] *http://entropy.brneurosci.org/linuxsetup32.html* Installing and Maintaining an INN News Server

```
news:~$ < ~aoe/attach.txt xargs -i /usr/lib/news/bin/ctlinnd cancel "{}"
# /etc/init.d/inn2 stop
news:~$ /usr/lib/news/bin/makehistory
# /etc/init.d/inn2 start
aoe:~$ vbnntp/vbnntpd.10 -f "attach>0 ORDER BY dateline"
```

3.5 Nachgedanken Posten, endgültige Authentifizierungsmechanismen usw

Diese und einige andere Features müssen erst einmal warten, aber mittels eines conjob, der `su -c ’cd /home/aoe; /home/aoe/vbnntp/vbnntpd.10 -f ‘date +%s -d ¨10 min ago¨‘’` oder ähnliches macht, kann nun regelmässig der Foreninhalt konvertiert werden; auch ein daemon mit der gleichen Funktionalität wäre denkbar.

`vbnntp`[2] entstand vor drei Jahren aus Frust über das Informatik-Forum, das leider zu diesem Zeitpunkt gegenüber news ziemlich beliebt geworden war, ruhte nach der übereilten Umstellung auf eine 3.x Beta-Version der Forensoftware und ist hiermit zu neuem Leben erwacht.

---

[2] *http://tigerente.htu.tuwien.ac.at/ãoe/vbnntp/*