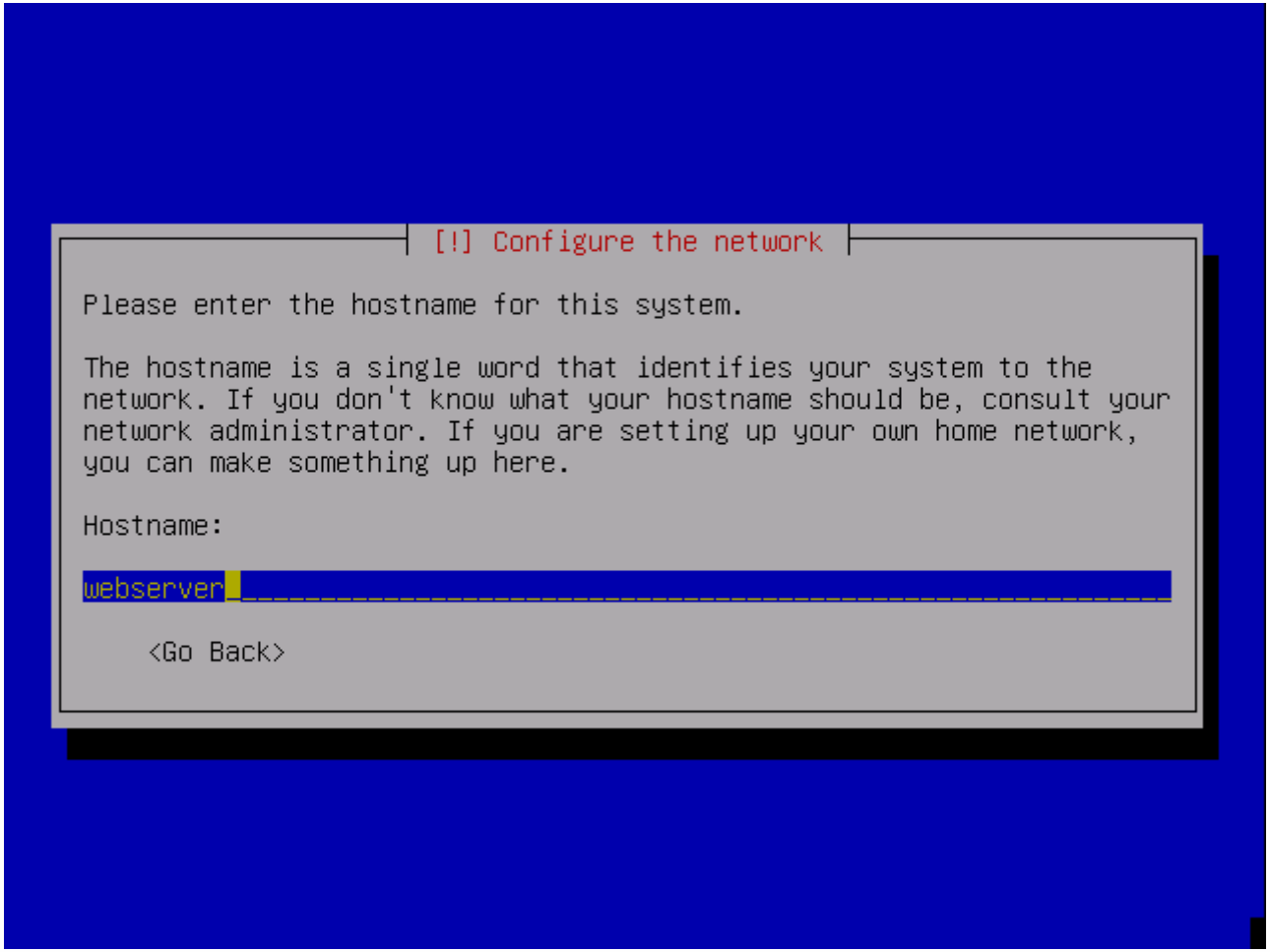
Härtung eines Debian-Systems

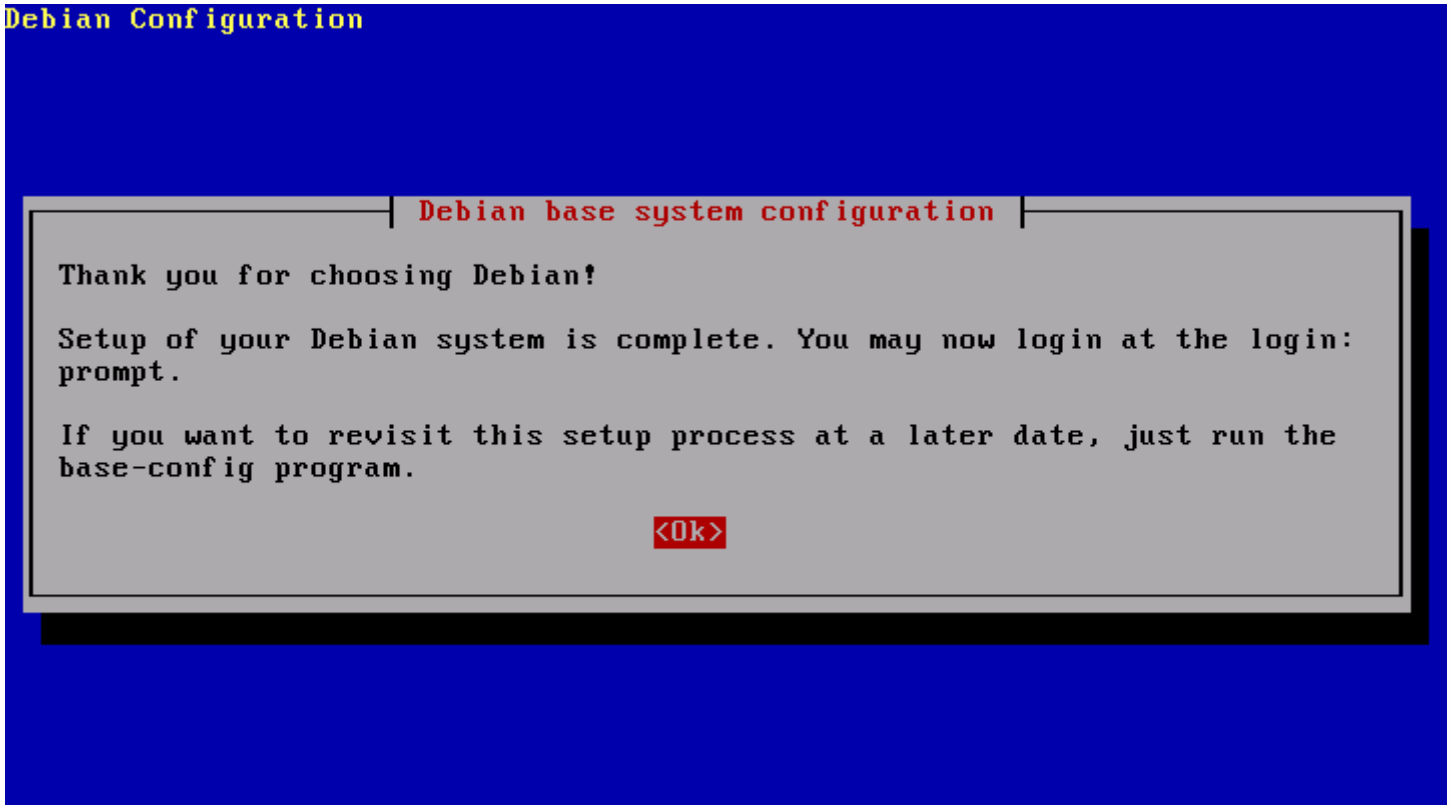
Grundsystem härten

Install CD

Servernamen festlegen



Installation abgeschlossen



Grundsystem härten

Überflüssige Dienste deinstallieren

```
# aptitude purge lpr
# aptitude purge portmap
```

Überflüssige Compiler, Libaries und Programme deinstallieren

```
# aptitude purge gcc-3.3 bin86 cpp-3.3 bison flex \
  gnu-efi libc6-dev libgc1 m4 make
# aptitude purge bc dc info gdb ed ppp \
  pppconfig pppoe pppoeconf
```

Rootlogin per Passwort mittels SSH unterbinden

- in /etc/ssh/sshd_config folgendes setzen:

  PermitRootLogin without-password
- ssh-Server neustarten
- ermöglicht trotzdem RootLogin mit Key (z.B. für Backups)

Port des ssh-Servers ändern

- bei begrenztem Benutzerkreis (und falls eine Begrenzung der Quellnetze nicht sinnvoll ist) sollte dies in Erwägung gezogen werden
- Herhinderung massiver Brute Force Angriffe, da diese auf Port 22 abzielen

PAM restriktiver gestalten

- Pluggable Authentifikation Modules
- cracklib-Erweiterung für PAM installieren

aptitude install libpam-cracklib wenglish

Änderungen in /etc/pam.d/common-password

```
 # new password.

-password   required   pam_unix.so nullok obscure min=4 max=8 md5
+#password   required   pam_unix.so nullok obscure min=4 max=8 md5

 # Alternate strength checking for password. Note that this

 #
-# password required      pam_cracklib.so retry=3 minlen=6 difok=3
-# password required      pam_unix.so use_authtok nullok md5
+password required        pam_cracklib.so retry=3 minlen=6 difok=3
+password required        pam_unix.so use_authtok nullok obscure min=6 max=20 md5
```

Änderungen in /etc/pam.d/su

```
 # (Replaces the `SU_WHEEL_ONLY' option from login.defs)
-# auth       required   pam_wheel.so
+auth       required   pam_wheel.so

 # be allowed to use su at all.
-# auth       required   pam_wheel.so deny group=nosu
+auth       required   pam_wheel.so deny group=nosu
```

Ergebnis

- Passwortlänge zwischen 6 und 20 Zeichen erzwungen
- Überprüfung, ob Passwort in Wörterbüchern vorkommt
- nur Benutzer der Gruppe „root“ dürfen sich mit „su“ in den BOfH-Mode versetzen

Ausgewählte Benutzer in Gruppe „root“ aufnehmen

```
# adduser tmtadm root
Adding user `tmtadm' to group `root'...
Done.
```

Postfix als MTA

- Konfigurationssyntax einfacher als sendmail, dadurch weniger Fehler an der Konfiguration
- viele Filtermöglichkeiten

Postfix installieren

aptitude install postfix

- „Internet site“ als System wählen
- Mailadresse angeben, wohin Mails für root geschickt werden sollen (meist hostmaster@deinedomain.de)
- FQDN als Mailer Name angeben (siehe Text)

Postfix nur für lokalen Versand

```
# sed -i s/inet_interfaces\ =\ all/inet_interfaces\ =\ 127.0.0.1/ \
    /etc/postfix/main.cf
# /etc/init.d/postfix restart
```

Lokalen Zeitserver installieren

- eine genaue Uhrzeit ist wichtig, um Einträge in den Logfile genau zuordnen zu können

aptitude install ntp-server

Möglichkeiten den Kernel härten & weitere Zugriffskontrollen zu implementieren

SELinux

(http://mitre.org/tech/selinux/)

- in Debian standardmäßig enthalten (Kernel und Userland-Tools)
- Out of the Box - Betrieb
- Projekt der NSA (vernutlich nicht so schnell eingestellt)
- gut dokumentiert
- sehr umfangreich

SELinux

(http://mitre.org/tech/selinux/)

- Komplexe Konfiguration
- keine automatische Erstellung von Zugriffsregeln
- Zugriffskonfiguration von Grund auf nötig
- in Produktivbetrieb sehr aufwendig

Grsecurity

(http://www.grsecurity.net/)

- leicht zu installieren
- Rollenbasierte Zugriffskontrollen
- Randomisierung der Mechanismen bezüglich Prozesse und Netzwerkfunktionen

Grsecurity

(http://www.grsecurity.net/)

- Verbesserung der chroot Funktion, Logging und Schutz vor Race Conditions in temp. Verzeichnissen
- Kernelpatch und Userland Tools
- automatisches Erstellen von minimalen Zugriffsregeln (gradm)

Grsecurity

(http://www.grsecurity.net/)

- eigen(es) Kernel(-paket) erzeugen (kein Sicherheits Support durch Debian)
- Zugriffskontrollsystem relativ schlecht dokumentiert
- weniger Funktionen für Zugriffskontrolle als SELinux

Optionale Monitoring-Möglichkeiten

Backports.org in source.list

(Quelle http://www.backports.org/instructions.html)

“**deb http://www.backports.org/debian/ sarge-backports main**”

to your /etc/apt/sources.list, and these lines

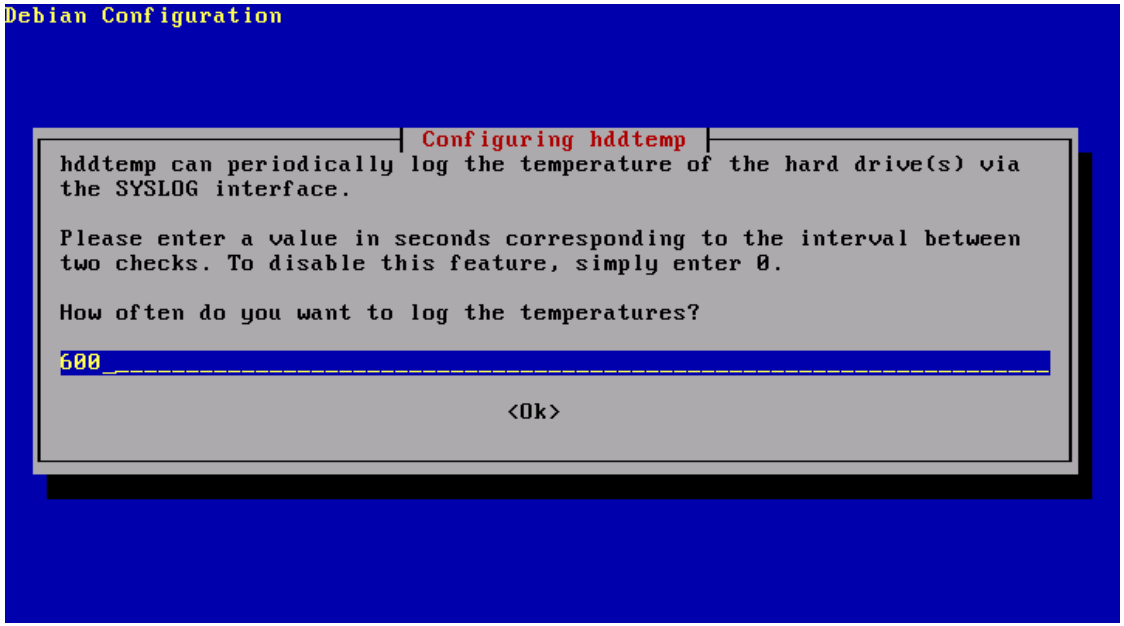
“**Package: *
Pin: release a=sarge-backports
Pin-Priority: 200**”

to your /etc/apt/preferences. That will deactivate all packages from bpo.

aptitude update

Installation Systemmonitoring

```
# apt-get -t sarge-backports install hddtemp \
    smartmontools
```



Zeit für Logfileeintäge einstellen

Festplattenfehler per Mail

- In /etc/smartd.conf folgendes ändern:

  “DEVICESCAN -m root -M exec /usr/share/smartmontools/smartd-runner”

  in

  “DEVICESCAN -m <mailaddr> -I 194 -I 231 -I 9 -M exec
  /usr/share/smartmontools/smartd-runner”

- Smartmontools starten:

  # sed -i s/#start_smartd/start_smartd/ /etc/default/smartmontools

  # /etc/init.d/smartmontools start

Evtl. lm-sensors installieren

- Abhängig von der Sensorenunterstützung
- Pakete: libsensors3 lm-sensors + kernelmodule

Festplattenkapazität per snmp prüfen

aptitude install snmpd

- ACHTUNG! Diesen Dienst durch eine Firewall schützen und nur vertrauenswürdigen Netzen öffnen!

Bitte etwas mehr Infos & Änderung Community

```
# sed -i s/com2sec\ paranoid\ \ default\ \ \ \ \ \ \ \ \
   public/#com2sec\ paranoid\ \ default\ \ \ \ \ \ \ \ \
   public/ /etc/snmp/snmpd.conf
# sed -i s/#com2sec\ readonly\ \ default\ \ \ \ \ \ \ \ \
   public/com2sec\ readonly\ \ default\ \ \ \ \ \ \ \ \
   <community>/ /etc/snmp/snmpd.conf
```

Partitionen konfigurieren

- in /etc/snmp/snmpd.conf „disk checks“-Sektion suchen
- Partitionen hinzufügen
- Syntax:

  disk PATH [MIN=DEFDISKMINIMUMSPACE]

/etc/init.d/snmpd restart

Apache2 und PHP installieren & härten

A(2)MP installieren

```
# aptitude install libapache2-mod-php4 \
  libapache2-mod-security php4-gd php4-mysql \
  mysql-server-4.1 phpmyadmin
# /usr/bin/mysqladmin -u root password 'enter-
  your-good-new-password-here‘
# exit
$ su –
# rm /root/.bash_history
```

PHP4 härten

„# sed -i s/disable_functions\ =/disable_functions\ =\
shell_exec,system,exec,passthru,show_source,proc_op
en,popen,highlight_file,phpinfo/
/etc/php4/apache2/php.ini“

„# sed -i s/expose_php\ =\ On/expose_php\ =\ Off/
/etc/php4/apache2/php.ini”

Apache2 einrichten

```
# a2dismod userdir
# a2enmod mod-security && a2enmod rewrite \  &&
   a2enmod ssl && a2enmod suexec
# echo "<Directory /var/www/*/>" > \
   /etc/apache2/conf.d/make_htaccess_work_for_vhosts \
   && echo "AllowOverride AuthConfig" >> \
   /etc/apache2/conf.d/make_htaccess_work_for_vhosts \
   && echo "</Directory>" >> \
   /etc/apache2/conf.d/make_htaccess_work_for_vhosts
# mkdir /var/log/apache2/vhosts/access_logs/
# mkdir /var/log/apache2/vhosts/error_logs/
```

Apache2 einrichten

```
# echo "Alias /phpmyadmin /usr/share/phpmyadmin" > \
    /etc/apache2/conf.d/make_phpmyadmin_for_all
# echo "<IfModule prefork.c>" > \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "StartServers          5" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "MinSpareServers       5" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "MaxSpareServers      10" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "MaxClients          150" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "MaxRequestsPerChild  0" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf && echo \
    "</IfModule>" >> \
    /etc/apache2/conf.d/server_poolzize_regulation.conf
```

Apache2 einrichten

/etc/apache2/conf.d/mod_security.conf:

```
<IfModule mod_security.c>
SecFilterEngine On
SecFilterCheckURLEncoding On
SecFilterCheckCookieFormat On
SecFilterCheckUnicodeEncoding Off
SecFilterForceByteRange 0 255
SecAuditEngine RelevantOnly
SecAuditLog /var/log/apache2/modsec_audit_log
SecFilterScanPOST On
SecFilterDefaultAction "deny,log,status:403"
SecFilterSelective HTTP_Content-Type \
"!(^$|^application/x-www-form-urlencoded$|^application/x-www-form-urlencoded|^multipart/form-
    data$|^multipart/form-data|^charset=iso-8859-1$|^charset=iso-8859-15$|^application/x-vermeer-
    urlencoded$|^application/x-vermeer-urlencoded|^multipart/mixed$|^multipart/mixed;)"
SecFilter "[Tt][Oo]\:"
SecFilter "[Ff][Rr][Oo][Mm]\:"
SecFilter "[Cc][Cc]\:"
</IfModule>
```

Apache2 härten

```
# echo "# Restrict banner information" > \
    /etc/apache2/conf.d/disable_banner && echo \
    "ServerTokens Prod" >> \
    /etc/apache2/conf.d/disable_banner
# addgroup vhoster
```

Vhost Konfiguration

```
<VirtualHost *>
        ServerName www.foo.bar
        ServerAlias foo.bar
        ServerAdmin webmaster@foo.bar
        DocumentRoot /var/www/www.foo.bar/public_html
        ScriptAlias /cgi-bin/ /var/www/www.foo.bar/cgi-bin/
        Alias /stats "/var/www/www.foo.bar/stats/"
         <IfModule mod_php4.c>
              AddType application/x-httpd-php .php .phtml .php3 .php4
              AddType application/x-httpd-php-source .phps
       </IfModule>
        ServerSignature Off
        <Directory /var/www/www.foo.bar/public_html/>
              Options FollowSymLinks
              AllowOverride AuthConfig
        </Directory>
```

Vhost Konfiguration

```
<Directory "/var/www/www.foo.bar/cgi-bin">
        AllowOverride None
        Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
</Directory>
SuexecUserGroup fooadm vhoster
LogLevel warn
CustomLog /var/log/apache2/vhosts/access_logs/www.foo.bar-access.log
combined
ErrorLog /var/log/apache2/vhosts/error_logs/www.foo.bar-error.log
```

Vhost Konfiguration

```
## some kind of php chroot (where php-code can be read from)
php_admin_value open_basedir
“/usr/share/php:/etc/phpmyadmin/:/usr/share/
phpmyadmin/:/var/www/www.foo.bar/“
## defining upload dir
php_admin_value upload_tmp_dir /var/www/www.foo.bar/tmp
## defining session dir
php_admin_value session.save_path /var/www/www.foo.bar/session
## disbale globals register (highly recommended)
php_admin_value register_globals off
## escaping bad chars
php_admin_value magic_quotes_gpc "1"
## don't include urls into php-code
php_admin_value allow_url_fopen no
```

Vhost Konfiguration

```
        ## uncomment, if safe_mode needs deactivated for this vhost, but
      remember, its a high security risk!
        #php_admin_value safe_mode "0"
        ## uncomment, if register_globals needs activated for this vhost, but re
member, its a high security risk!
        #php_admin_value register_globals "1"
        ## restrict exec dir (if exec is needed) (where programms can be started
 from)
        ## symlink the binaries to this dir!
        ## only working if safe_mode="1"
        php_admin_value safe_mode_exec_dir /var/www/www.foo.bar/bin
        ## disable crosssite scripting
        RewriteEngine on
        RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
        RewriteRule .* - [F]
</VirtualHost>
```

Vhost Konfiguration

(sinnvollerweise durch Script)

- /var/www/www.foo.bar/public_html (fooadm:vhoster) anlegen
- /var/www/www.foo.bar/cgi-bin (fooadm:vhoster) anlegen
- /var/www/www.foo.bar/stats (root:root) anlegen
- /var/www/www.foo.bar/tmp (www-data:vhoster) anlegen
- /var/www/www.foo.bar/session (www-data:vhoster) anlegen
- /var/www/www.foo.bar/bin (root:root) anlegen

adduser fooadm vhoster

Vsftpd Server

Vsftpd klar machen

```
# aptitude install vsftpd
# sed -i
    s/anonymous_enable=YES/#anonymous_enable=YES/
    /etc/vsftpd.conf
# echo "/bin/false" >> /etc/shells
# echo "banner_file=/etc/vsftpd_banner.conf" >> \
    /etc/vsftpd.conf
# echo "local_enable=YES" >> /etc/vsftpd.conf
# echo "chroot_local_user=YES" >> /etc/vsftpd.conf
```

Vsftpd klar machen

```
# echo "chroot_list_enable=YES" >> /etc/vsftpd.conf
# echo "chroot_list_file=/etc/vsftpd.chroot_list" >> \
   /etc/vsftpd.conf
# echo "write_enable=YES" >> /etc/vsftpd.conf
# echo "local_umask=022" >> /etc/vsftpd.conf
# echo "log_ftp_protocol=YES" >> /etc/vsftpd.conf
# echo "dual_log_enable=YES" >> /etc/vsftpd.conf
# echo "anonymous_enable=NO" >> /etc/vsftpd.conf
# echo "tmtadm" > /etc/vsftpd.chroot_list
# echo "Welcome to foobar\!" > /etc/vsftpd_banner.conf
```

SSL/TLS Support für vsftpd (optional)

```
# echo "ssl_enable=YES" >> /etc/vsftpd.conf
# echo "ssl_tlsv1=YES" >> /etc/vsftpd.conf
# echo "ssl_sslv3=YES" >> /etc/vsftpd.conf
# echo "force_local_data_ssl=NO" >> /etc/vsftpd.conf
# echo "force_local_logins_ssl=NO" >> /etc/vsftpd.conf
```

- Zertifikat unter /etc/ssl/certs/vsftpd.pem ablegen

```
# /etc/init.d/vsftpd restart
```

Vsftpd Server

Firewall installieren/konfigurieren

- Default Policy: Deny/Reject
- ICMP für alle erlauben
- für unseren Webserver TCP Port 80, 443 global auf
- Optional für FTP Port TCP 20, 21 global auf
- Optional für vertrauenswürdige Hosts UDP Port 161 für snmp Monitoring öffnen
- als iptables Frontend bietet sich shorewall an

Quota einrichten

System für Quota klar machen

- In /etc/fstab für die Partition mit den Vhost DocumentRoot hinter „defaults“ „,usrquota“ anfügen

mount –o remount /dev/<vhosts>

cd <part_root_vhosts> && touch quota.user && \
  chmod 600 quota.user

User-Quota setzen

(wieder mal am Besten im/als Script)

```
# QUOTAPART=/dev/<vhost_part> ADMLOGIN=fooadm \
    SOFTQUOTA=55 HARDLIMIT=50 \
    quotatool -b $QUOTAPART -u $ADMLOGIN \
    -q $SOFTLIMIT MB -l $HARDLIMIT MB -v
```

Weiterführende Quellen

- Securing Debian Manual - http://www.debian.org/doc/manuals/securing-debian-howto

Informationen bezüglich Sicherheitslücken und weiterführende Informationen

Woher bekomme ich Informationen zu aktuellen Sicherheitslücken?

- http://www.debian.org/security/
- Mailingliste debian-security-announce
- Mailingliste debian-security
- Mailingliste Full-Disclosure (http://lists.grok.org.uk/full-disclosure-charter.html)
- Mailingliste Bugtraq (http://www.securityfocus.com/archive/1/description)
- Mailingliste Vulnwatch (http://www.vulnwatch.org/)
- Mailingliste US-Cert (http://www.us-cert.gov/nav/t01/)

Weiterführende Informationen zum Härten von Debian

- Securing Debian Manual - http://www.debian.org/doc/manuals/securing-debian-howto
- Michael D. Bauer: Sichere Server mit Linux, Köln 2003, ISBN 3-89721-139-4

To be continued….