Anleitung zum Absichern von Debian
Kapitel 12 - Häufig gestellte Fragen / Frequently asked Questions (FAQ)

Dieses Kapitel führt Sie in ein paar der am häufigsten gestellten Fragen in der Security-Mailingliste von Debian ein. Sie sollten sie lesen, bevor Sie dort etwas posten, oder die Leute werden Ihnen »RTFM!« sagen.

12.1 Sicherheit im Debian Betriebssystem

12.1.1 Ist Debian sicherer als X?

Ein System ist so sicher, wie der Administrator fähig ist, es sicher zu machen. Debians Standardinstallation von Diensten zielt darauf ab, *sicher* zu sein. Sie ist aber nicht so paranoid wie andere Betriebssysteme, die Dienste *standardmäßig abgeschaltet*. In jedem Fall muss der Systemadministrator die Sicherheit des System den lokalen Sicherheitsmaßstäben anpassen.

Für eine Übersicht der Sicherheitslücken von vielen Betriebssystemen sollten Sie sich die `US-CERT-Statistik` ansehen oder sich selber Statistiken mit der `National Vulnerability Database` (früher ICAT) erstellen. Sind diese Daten nützlich? Es müssen verschiedene Faktoren berücksichtigt werden, wenn die Daten interpretiert werden sollen. Man sollte beachten, dass diese Daten nicht dazu verwendet werden können, um die Verwundbarkeit eines Betriebssystems mit der eines anderen zu vergleichen. [82] Bedenken Sie außerdem, dass sich einige registrierte Sicherheitslücken im Zusammenhang mit Debian nur auf den *Unstable*-Zweig, also den nicht offiziell veröffentlichten Zweig, beziehen.

12.1.1.1 Ist Debian sicherer als andere Linux-Distributionen (wie Red Hat, SuSE, ...)?

Der Unterschied zwischen den Linux-Distributionen ist nicht sehr groß mit Ausnahme der Basisinstallation und der Paketverwaltung. Die meisten Distributionen beinhalten zum Großteil die gleichen Anwendungen. Der Hauptunterschied besteht in den Versionen dieser Programme, die mit der stabilen Veröffentlichung der Distribution ausgeliefert werden. Zum Beispiel sind der Kernel, Bind, Apache, OpenSSH, Xorg, gcc, zlib, etc. in allen Linux-Distributionen vorhanden.

Ein Beispiel: Red Hat hatte Pech und wurde veröffentlicht, als foo 1.2.3 aktuell war. Später wurde darin eine Sicherheitslücke entdeckt. Dagegen hatte Debian das Glück, dass es mit foo 1.2.4 ausgeliefert wurde, in dem der Fehler schon behoben war. Das war der Fall beim großen Problem mit `rpc.statd` vor ein paar Jahren.

Es besteht eine weitgehende Zusammenarbeit zwischen den jeweiligen Sicherheitsteams der großen Linux-Distributionen. Bekannte Sicherheitsaktualisierungen werden selten (wenn nicht sogar nie) von den Anbietern der Distribution nicht eingespielt. Das Wissen um eine Sicherheitslücke wird niemals vor anderen Anbietern von Distributionen geheim gehalten, da die Ausbesserungen gewöhnlich vom Programmautor oder von `CERT` koordiniert werden. Das hat zur Folge, dass notwendige Sicherheitsaktualisierungen üblicherweise zur selben Zeit veröffentlicht werden. Damit ist die relative Sicherheit der verschiedenen Distributionen ziemlich ähnlich.

Einer großen Vorteile von Debian in Hinblick auf die Sicherheit ist die Leichtigkeit von Systemaktualisierungen mit `apt`. Hier sind ein paar andere Aspekte über die Sicherheit in Debian, die Sie berücksichtigen sollten:

- Debian bietet mehr Sicherheitswerkzeuge an als andere Distributionen. Vergleichen Sie dazu Sicherheitswerkzeuge in Debian, Kapitel 8.
- Debians Standardinstallation ist kleiner (weniger Funktionen) und daher sicherer. Andere Distributionen tendieren im Namen der Benutzerfreundlichkeit dazu, standardmäßig viele Dienst zu installieren, und manchmal sind diese nicht ordentlich konfiguriert (denken Sie an `Lion` oder `Ramen`). Debians Installation ist nicht so streng wie OpenBSD (dort laufen Daemonen standardmäßig nicht), aber es ist ein guter Kompromiss. [83]
- Debian stellt die besten Verfahren zur Sicherheit in Dokumenten wie diesem vor.

12.1.2 In Bugtraq gibt es viele Debian-Fehler. Heißt das, dass es sehr gefährdet ist?

Die Debian-Distribution enthält eine große und wachsende Zahl von Softwarepaketen, wahrscheinlich sogar mehr als mit vielen proprietären Betriebssystem geliefert wird. Je mehr Pakete installiert sind, desto größer ist die Möglichkeit von Sicherheitslücken in einem System.

Immer mehr Menschen untersuchen den Quellcode, um Fehler zu entdecken. Es gibt viele Anweisungen im Zusammenhang mit Audits des Quellcodes von großen Softwarekomponenten, die in Debian enthalten sind. Immer wenn ein solcher Audit Sicherheitslücken aufdeckt, werden sie ausgebessert und eine Anweisung wird an Listen wie Bugtraq geschickt.

Fehler, die in der Debian-Distribution vorhanden sind, betreffen normalerweise auch andere Anbieter und Distributionen. Prüfen Sie einfach den "Debian specific: yes/no"-Abschnitt am Anfang jeder Anweisung (DSA).

12.1.3 Hat Debian irgendein Zertifikat für Sicherheit?

Die kurze Antwort: Nein.

Die lange Antwort: Zertifikate kosten Geld (besonders ein *seriöses* Sicherheitszertifikat). Niemand hat die Ressourcen aufgebracht, um Debian GNU/Linux beispielsweise mit irgendeinem Level des `Common Criteria` zertifizieren zu lassen. Wenn Sie daran interessiert sind, eine GNU/Linux-Distribution mit Sicherheitszertifikaten zu haben, stellen Sie uns die Ressourcen zur Verfügung, um dies möglich zu machen.

Es gibt im Moment mindestens zwei Linux-Distributionen, die mit verschiedenen `EAL` Levels zertifiziert sind. Beachten Sie, dass einige CC-Tests im `Linux Testing Project` vorhanden sind, welche in Debian durch `ltp` angeboten wird.

12.1.4 Gibt es irgendein Abhärtungsprogramm für Debian?

Ja. `Bastille Linux`, das sich ursprünglich an anderen Linux-Distributionen (Red Hat und Mandrake) orientierte, es funktioniert derzeit auch mit Debian. Es sind Maßnahmen eingeleitet, um Änderungen am Originalprogramm auch in das Debian-Paket `bastille` einfließen zu lassen.

Manche Leute glauben jedoch, dass ein Absicherungsprogramm nicht die Notwendigkeit einer guten Administration ersetzt.

12.1.5 Ich möchte einen XYZ-Dienst laufen lassen. Welchen sollte ich benutzen?

Einer der größten Stärken von Debian ist die große Vielfalt von Paketen, die die gleichen Funktionen erfüllen (DNS-Server, Mail-Server, FTP-Server, Web-Server etc.). Das kann einen unerfahrenen Administrator verwirren, wenn er herausfinden will, welches Paket das richtige für ihn ist. Die beste Wahl hängt in der Balance zwischen Ihrem Bedürfnis nach Funktionalität und dem nach Sicherheit in der jeweiligen Situation ab. Im folgenden einige Fragen, die Sie sich stellen sollten, wenn Sie zwischen ähnlichen Paketen entscheiden müssen:

- Wird es noch vom Originalautor betreut? Wann war die letzte Veröffentlichung?

- Ist das Paket ausgereift? Die Versionsnummer sagt *nichts* darüber aus, wie ausgereift es ist. Versuchen Sie seine Geschichte nachzuvollziehen.
- Ist es von Fehlern durchsetzt? Gab es Sicherheits-Ankündigungen im Zusammenhang mit ihm?
- Stellt die Software die ganze Funktionalität zur Verfügung, die Sie benötigen? Bietet es mehr, als Sie wirklich brauchen?

12.1.6 Wie mache ich den Dienst XYZ unter Debian sicherer?

Sie werden in diesem Dokument Informationen über das Absichern von einigen Diensten (FTP, Bind) unter Debian GNU/Linux finden. Für Dienste die hier nicht abgedeckt werden, prüfen Sie die Programm-Dokumentation oder allgemeine Linux-Informationen. Die meisten Sicherheitshinweise für Unix-Systeme sind auch auf Debian anwendbar. So wird Dienst X unter Debian in den meisten Fällen wie in einer anderen Linux-Distribution (oder Un*x, was das betrifft) abgesichert.

12.1.7 Wie kann ich die Banner der Dienste entfernen?

Wenn Sie z.B. nicht wollen, dass Nutzer sich mit Ihrem POP3-Daemon verbinden und dadurch Informationen über Ihr System erlangen, sollten Sie das Banner, das der Dienst den Nutzern zeigt, entfernen (oder verändern). [84] Wie Sie das anstellen können. hängt von der Software ab, mit der Sie einen bestimmten Dienst betreiben. Für `postfix` stellen Sie beispielsweise das SMTP-Banner in `/etc/postfix/main.cf` ein:

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

Andere Software kann nicht so leicht verändert werden. `ssh` muss neu kompiliert werden, um die angezeigte Version zu ändern. Stellen Sie sicher, dass sie nicht den ersten Teil des Banners (`SSH-2.0`) entfernen, da Clients ihn verwenden, um die von Ihrem Paket unterstützten Protokolle zu identifizieren.

12.1.8 Sind alle Debian Pakete sicher?

Das Sicherheitsteam von Debian kann nicht alle Pakete aus Debian auf potenzielle Sicherheitslücken hin analysieren, da es einfach nicht genug Ressourcen gibt, um für das gesamte Projekt ein Quellcodeaudit durchzuführen. Allerdings profitiert Debian von den Quellcode-Prüfungen durch die Originalautoren.

Tatsächlich könnte ein Debian-Entwickler in einem Paket einen Trojaner verbreiten, und es gibt keine Möglichkeit das nachzuprüfen. Sogar wenn es in einen Zweig von Debian eingeführt werden würde, wäre es unmöglich, alle möglichen Situationen abzudecken, in denen der Trojaner ausgeführt werden würde. Das ist der Grund, warum Debian eine *"Keine Gewährleistung"*-Klausel in seiner Lizenz hat.

Allerdings können Debian-Benutzer insofern Vertrauen fassen, dass der stabile Quellcode eine breite Prüfung hinter sich hat. Die meisten Probleme würden dabei durch Benutzung entdeckt. Es ist zu empfehlen, ungetestete Software auf kritischen Systemen zu installieren, wenn Sie nicht die notwendige Code-Prüfung vornehmen können. In jedem Fall gewährleistet der Aufnahmeprozess in die Distribution (mit digitalen Signaturen), dass im Falle von in die Distribution eingeschleusten Sicherheitsproblemen das Problem letztendlich zum Entwickler zurückgeführt werden kann. Das Debian-Projekt hat diese Angelegenheiten nie auf die leichte Schulter genommen.

12.1.9 Warum sind einige Log- und Konfigurationsdateien für die Welt lesbar? Ist das nicht unsicher?

Natürlich können Sie die Standardrecht von Debian auf Ihrem System abändern. Der aktuelle Grundsatz in Bezug auf Log- und Konfigurationsdateien besagt, dass sie für die Welt lesbar sind, *es sei denn*, sie enthalten sensible Informationen.

Seien Sie vorsichtig, wenn Sie Änderungen vornehmen:

- Prozesse könnten nicht mehr in der Lage sein, in Log-Dateien zu schreiben, wenn Sie ihre Rechte einschränken.
- Einige Anwendungen könnten nicht mehr funktionieren, wenn sie ihre Konfigurationsdatei nicht mehr lesen können. Wenn Sie zum Beispiel das Recht, für die Welt lesbar zu sein, von `/etc/samba/smb.conf` entfernen, kann das Programm `smbclient` nicht funktionieren, wenn es von einem normalen Nutzer ausgeführt wird.

FIXME: Check if this is written in the Policy. Some packages (i.e. ftp daemons) seem to enforce different permissions.

12.1.10 Warum hat /root/ (oder NutzerX) die Rechte 755?

Tatsächlich kann die gleiche Frage auch für jeden anderen Nutzer gestellt werden. Da Debians Standardinstallation *keine* Dateien unter diesem Verzeichnis abgelegt, sind keine sensiblen Informationen vorhanden, die geschützt werden müssten. Wenn Sie denken, dass diese Rechte für Ihr System zu locker sind, können Sie sie auf 750 einschränken. Für Nutzer sollten Sie Begrenzung des Zugangs zu Informationen anderer Nutzer, Abschnitt 4.11.13.1 lesen.

Dieser `Thread` der Sicherheitsmailingliste von Debian hat weitere Ausführungen zu diesem Thema.

12.1.11 Nach der Installation von grsec oder einer Firewall bekomme ich viele Nachrichten auf der Konsole. Wie entferne ich sie?

Wenn Sie Nachrichten auf der Konsole empfangen und `/etc/syslog.conf` so eingerichtet haben, dass sie in Dateien oder auf ein spezielles TTY umgeleitet werden, sehen Sie vielleicht Nachrichten, die direkt an die Konsole geschickt werden.

Der Standardloglevel der Konsole ist bei jeden Kernel sieben, was bedeutet, dass alle Nachrichten mit einer niedrigeren Priorität auf der Konsole erscheinen werden. Für gewöhnlich haben Firewalls (die LOG-Regel) und einige andere Sicherheitswerkzeuge eine niedrigere Log-Priorität. Daher werden ihre Logs direkt an die Konsole geschickt.

Um die Nachrichten, die an die Konsole geschickt werden, nicht verringern, können Sie `dmesg` (Option `-n`, vergleichen Sie `dmesg(8)`) verwenden, das den Ringspeicher des Kernel untersucht und *steuert*. Damit das nach dem nächsten Neustart in Ordnung ist, ändern Sie in `/etc/init.d/klogd`

```
KLOGD=""
```

zu

```
KLOGD="-c 4"
```

ab.

Verwenden Sie eine niedrigere Nummer für `-c`, wenn Sie immer noch unerwünschte Nachrichten sehen. Eine Beschreibung der verschiedenen Loglevels befindet sich in `/usr/include/sys/syslog.h`:

```
#define LOG_EMERG       0       /* system is unusable */
#define LOG_ALERT       1       /* action must be taken immediately */
#define LOG_CRIT        2       /* critical conditions */
#define LOG_ERR         3       /* error conditions */
#define LOG_WARNING     4       /* warning conditions */
#define LOG_NOTICE      5       /* normal but significant condition */
#define LOG_INFO        6       /* informational */
#define LOG_DEBUG       7       /* debug-level messages */
```

12.1.12 Benutzer und Gruppen des Betriebssystems

12.1.12.1 Sind alle Systemnutzer notwendig?

Ja und nein. Debian wird mit einigen vordefinierten Nutzern (User-ID (UID) < 99, beschrieben in der `Debian Policy` oder in `/usr/share/doc/base-passwd/README`) geliefert. Dadurch wird die Installation einiger Dienste erleichtert, für die es notwendig ist, unter einem passenden Nutzer/UID zu laufen. Wenn Sie nicht vorhaben, neue Dienste zu installieren, können Sie die Nutzer entfernen, denen keine Dateien auf Ihrem System gehören und die keine Dienste laufen lassen. Unabhängig davon ist das Standardverhalten in Debian, dass UIDs von 0 bis 99 reserviert sind und UIDs von 100 bis 999 von Paketen bei der Installation erstellt werden und gelöscht werden, wenn das Pakete vollständig gelöscht wird (purge) wird.

Benutzer, denen keine Dateien gehören, finden Sie leicht mit dem folgenden Kommando[85] (führen Sie es als Root aus, da ein normaler Benutzer nicht genügend Zugriffsrechte haben könnte, um einige sensible Verzeichnisse zu durchsuchen):

```
cut -f 1 -d : /etc/passwd | \
while read i; do find / -user "$i" | grep -q . || echo "$i"; done
```

Diese Nutzer kommen aus dem Paket `base-passwd`. Sie finden Informationen über die Behandlung dieser Nutzer unter Debian in der Dokumentation des Pakets. Es folgt nun eine Liste der Standardnutzer (mit einer entsprechenden Gruppe):

- root: Root ist (typischerweise) der Superuser.
- daemon: Einige unprivilegierte Daemonen, die Dateien auf die Festplatte schreiben müssen, laufen als daemon.daemon (z.B. `portmap`, `atd`, wahrscheinlich noch andere). Daemonen, die keine eigenen Dateien besitzen müssen, können stattdessen als nobody.nogroup laufen. Komplexere oder sicherheitsbewusste Daemonen laufen als eigenständige Nutzer. Der Nutzer daemon ist auch praktisch für lokal installierte Daemons.
- bin: aus historischen Gründen beibehalten.
- sys: das gleiche wie bei bin. Jedoch gehören /dev/vcs* und `/var/spool/cups` der Gruppe sys.
- sync: Die Shell des Nutzers sync ist `/bin/sync`. Wenn das Passwort auf etwas leicht zu ratendes gesetzt wurde (zum Beispiel »«), kann jeder das System von der Konsole aus synchronisieren lassen, auch wenn er kein Konto hat.
- games: Viele Spiele sind SETGID »games«, damit sie ihre Highscore-Dateien schreiben können. Dies wird in der Richtlinie erklärt.
- man: Das Programm man läuft (manchmal) als Benutzer »man«, damit es Cat-Seiten nach `/var/cache/man` schreiben kann.
- lp: wird von Druck-Daemonen benutzt
- mail: Mailboxen unter `/var/mail` gehören der Gruppe »mail«, wie in der Policy erklärt wird. Der Benutzer und die Gruppe werden auch von verschiedene MTAs zu anderen Zwecken benutzt.
- news: Verschiedene News-Server und ähnliche Programme (zum Beispiel `suck`) benutzen den Nutzer und die Gruppe news auf unterschiedliche Weise. Dateien im news-Spool gehören häufig dem Nutzer und der Gruppe news. Programme wie `inews`, die man benutzen kann, um News zu posten, sind normalerweise SETGID news.
- uucp: Der Nutzer uucp und die Gruppe uucp werden vom UUCP-Subsystem benutzt. Ihnen gehören Spool- und Konfigurationsdateien. Nutzer in der Gruppe uucp können uucico aufrufen.
- proxy: Wie Daemon wird dieser Nutzer und diese Gruppe von manchen Daemonen (insbesondere Proxy-Daemonen) verwendet, die keine spezielle User-ID haben, aber eigene Dateien besitzen müssen. Zum Beispiel wird die Gruppe proxy von `pdnsd` benutzt, und `squid` läuft als Nutzer proxy.
- majordom: `Majordomo` hat auf Debian-Systemen aus historischen Gründen eine statisch zugewiesene UID. Auf neuen Systemen wird sie nicht installiert.

- postgres: `Postgresql`-Datenbanken gehören diesem Nutzer und dieser Gruppe. Alle Dateien in `/var/lib/postgresql` gehören diesem Nutzer, um anständige Sicherheit zu gewährleisten.
- www-data: Einige Web-Server laufen als www-data. Web-Inhalte sollten *nicht* diesem Nutzer gehören, andernfalls wäre ein kompromittierter Web-Server in der Lage, eine Web-Seite zu überschreiben. Daten, die der Web-Server schreibt, einschließlich Log-Dateien, gehören www-data.
- backup: So können Backup-/Wiederherstellungszuständigkeiten lokal an irgendjemanden ohne volle Root-Zugriff delegiert werden.
- operator: operator ist historisch (und praktisch) das einzige 'Nutzer'-Konto, in das man sich entfernt einloggen kann, und das nicht von NIS/NFS abhängt.
- list: Mailinglisten-Archive und Daten gehören diesem Nutzer und dieser Gruppe. Manche Mailinglisten-Programme laufen auch unter diesem Nutzer.
- irc: Wird von irc-Daemonen benutzt. Ein statisch zugewiesener Nutzer wird nur wegen eines Fehlers in `ircd` benötigt, das beim Start SETUID() auf sich selbst für eine bestimmte UID ausführt.
- gnats.
- nobody, nogroup: Daemonen die keine eigenen Dateien haben laufen als Nutzer nobody und Gruppe nogroup. Demzufolge sollten keine Dateien auf dem gesamten System diesem Nutzer oder dieser Gruppe gehören.

Andere Gruppe, die keinen dazugehörigen Benutzer haben:

- adm: Die Gruppe adm wird zu Zwecken der Überwachung benutzt. Mitglieder dieser Gruppe können viele Dateien in `/var/log` lesen und die xconsole benutzen. `/var/log` war früher einmal `/usr/adm` (und später `/var/adm`), daher der Name dieser Gruppe.
- tty: TTY-Geräte gehören dieser Gruppe. Die Befehle write und wall benutzen dies, um auf die TTYs anderer Leute zu schreiben.
- disk: Roh-Zugriff auf Festplatten. Größtenteils äquivalent zum Root-Zugriff.
- kmem: /dev/kmem und ähnliche Dateien sind von dieser Gruppe lesbar. Dies ist größtenteils ein Relikt aus BSD. Aber jedes Programm, dass Lese-Zugriff auf den Systemspeicher braucht, kann so SETGID kmem gemacht werden.
- dialout: Voller und direkter Zugriff auf serielle Schnittstellen. Mitglieder dieser Gruppen können Modems rekonfigurieren, sich irgendwo einwählen, usw.
- dip: Der Name der Gruppe steht für »Dial-up IP«. Mitglied der Gruppe dip zu sein erlaubt Ihnen Programme wie `ppp`, `dip`, `wvdial` usw. zu benutzen, um eine Verbindung herzustellen. Die Nutzer in dieser Gruppe können das Modem nicht konfigurieren. Sie können lediglich Programme aufrufen, die es benutzen.
- fax: Erlaubt es den Mitgliedern, Fax-Software zu benutzen, um Faxe zu senden und zu empfangen.
- voice: Voicemail, nützlich für Systeme, die Modems als Anrufbeantworter benutzen.
- cdrom: Diese Gruppe kann dazu benutzt werden, einer bestimmen Menge von Nutzern Zugriff auf CD-ROM-Laufwerke zu geben.
- floppy: Diese Gruppe kann dazu benutzt werden, einer bestimmen Menge von Nutzern Zugriff auf Diskettenlaufwerke zu geben.
- tape: Diese Gruppe kann dazu benutzt werden, einer bestimmen Menge von Nutzern Zugriff auf Bandlaufwerke zu geben.
- sudo: Mitglieder dieser Gruppe müssen ihr Passwort nicht eingeben, wenn sie `sudo` benutzen. Siehe `/usr/share/doc/sudo/OPTIONS`.

- audio: Diese Gruppe kann dazu benutzt werden, einer bestimmen Menge von Nutzern Zugriff auf jedes Audiogerät zu geben.
- src: Dieser Gruppe gehören die Quellcodes, einschließlich der Dateien in `/usr/src`. Sie kann benutzt werden, um einem bestimmten Nutzern die Möglichkeit zu bieten, Quellcode des Systems zu verwalten.
- shadow: `/etc/shadow` ist von dieser Gruppe lesbar. Einige Programme, die auf diese Datei zugreifen müssen, sind SETGID shadow.
- utmp: Diese Gruppe kann nach `/var/run/utmp` und ähnlichen Dateien schreiben. Programme, die darin schreiben können müssen, sind SETGID utmp.
- video: Diese Gruppe kann dazu benutzt werden, einer bestimmen Menge von Nutzern Zugriff auf ein Videogerät zu geben.
- staff: Erlaubt Nutzern lokale Modifikationen am System vorzunehmen (`/usr/local`, `/home`), ohne dass sie Root-Privilegien bräuchten. Vergleichen Sie sie mit »adm«, die sich mehr auf Überwachung/Sicherheit bezieht.
- users: Während Debian-Systeme standardmäßig das System einer privaten Nutzergruppe (jeder Nutzer hat seine eigene Gruppe) benutzen, ziehen es manche vor, ein traditionelleres Gruppen-System zu verwenden. In diesem System ist jeder Nutzer Mitglied dieser Gruppe.

12.1.12.2 Ich entfernte einen Systembenutzer! Wie kann ich dies rückgängig machen?

Wenn Sie einen Systembenutzer entfernt und kein Backup Ihrer `password`- und `group`-Dateien haben, können Sie versuchen, diesen mittels `update-passwd` (vergleichen Sie `update-passwd(8)`) wiederherzustellen.

12.1.12.3 Was ist der Unterschied zwischen den Gruppen adm und staff?

Die Gruppe 'adm' besteht üblicherweise aus Administratoren. Die Rechte dieser Gruppe erlauben es ihnen, Log-Dateien zu lesen, ohne `su` benutzen zu müssen. Die Gruppe 'staff' ist gewöhnlich für Kundendienst- und Junioradministratoren bestimmt und gibt ihnen die Möglichkeit, Dinge in `/usr/local` zu erledigen und Verzeichnisse in `/home` anzulegen.

12.1.13 Warum gibt es eine neue Gruppe, wenn ich einen neuen Nutzer anlege? (Oder warum gibt Debian jedem Nutzer eine eigene Gruppe?)

Das Standardverhalten von Debian ist, dass jeder Nutzer seine eigene, persönliche Gruppe hat. Das traditionelle UN*X-Modell weist alle Benutzer der Gruppe *users* zu. Zusätzliche Gruppe werden erstellt, um den Zugang zu gemeinsam genutzten Dateien, die mit verschiedenen Projektverzeichnissen verbunden sind, einzuschränken. Die Dateiverwaltung wurde schwierig, wenn ein einzelner Nutzer an verschiedenen Projekten arbeitete, da, wenn jemand eine Datei erstellte, diese mit der primären Gruppe des Erstellers (z.B. 'users') verbunden war.

Das Modell von Debian löst dieses Problem, indem es jedem Nutzer seine eigene Gruppe zuweist. So wird mit einer korrekten Umask (0002) und mit dem SETGID-Bit für ein Projektverzeichnis den Dateien, die in diesem Verzeichnis erstellt werden, automatisch die richtige Gruppe zugewiesen. Das erleichtert die Arbeit von Menschen, die an verschiedenen Projekten arbeiten, da sie nicht die Gruppe oder Umasks ändern müssen, wenn sie mit gemeinsam genutzten Dateien arbeiten.

Sie können allerdings dieses Verhalten verändern, indem Sie `/etc/adduser.conf` modifizieren. Ändern Sie die Variable *USERGROUPS* auf 'no' ab. Dadurch wird keine neue Gruppe erstellt, wenn ein neuer Nutzer angelegt wird. Sie sollten auch *USERS_GID* die GID der Gruppe zuweisen, der alle Nutzer angehören.

12.1.14 Fragen über Dienste und offene Ports

12.1.14.1 Warum werden Dienste während der Installation aktiviert?

Das ist der Annäherung an das Problem, auf der einen Seite sicherheitsbewusst und auf der anderen Seite benutzerfreundlich zu sein. Anders als OpenBSD, das alle Dienste abschaltet, bis sie vom Administrator aktiviert werden, aktiviert Debian GNU/Linux alle installierten Dienste, bis sie abgeschaltet werden (siehe dazu Daemons abschalten, Abschnitt 3.6.1). Immerhin haben Sie den Dienst installiert, oder?

Es gab viele Diskussionen auf Debian-Mailinglisten (sowohl auf debian-devel als auch auf debian-security) darüber, welches die bessere Vorgehensweise für eine Standardinstallation ist. Jedoch gab es bisher (10. März 2002) keinen Konsens.

12.1.14.2 Kann ich `inetd` entfernen?

`Inetd` ist nicht leicht zu entfernen, da `netbase` von dem Paket abhängt, das es enthält (`netkit-inetd`). Wenn Sie es entfernen wollen, können Sie es entweder abschalten (siehe Daemons abschalten, Abschnitt 3.6.1) oder das Paket entfernen, indem Sie das Paket `equivs` benutzen.

12.1.14.3 Warum muss ich Port 111 offen haben?

Port 111 ist sunrpcs Portmapper und wird standardmäßig bei der Grundinstallationen eines Debian-Systems eingerichtet, da es keine Möglichkeit gibt herauszubekommen, wann ein Programm eines Nutzers RPC gebrauchen könnte, um korrekt zu arbeiten. Jedenfalls wird es meistens von NFS benutzt. Wenn Sie kein NFS benutzen, entfernen Sie es, wie in Sichern von RPC-Diensten, Abschnitt 5.13 erklärt.

In Versionen des Pakets `portmap` später als 5-5 können Sie sogar den Portmapper installieren, aber ihn nur auf dem Localhost lauschen lassen (dazu müssen Sie `/etc/default/portmap` verändern).

12.1.14.4 Wozu ist der `identd` (Port 113) da?

Der Dienst Identd ist ein Authentisierungdienst, der den Besitzer einer bestimmten TCP/IP-Verbindung zu einem entfernten Server, der die Verbindung annimmt, identifiziert. Wenn ein Benutzer sich mit einem entfernten Host verbindet, schickt `inetd` auf dem entfernten Host üblicherweise eine Anfrage an Port 113 zurück, um Informationen über den Besitzer herauszufinden. Er wird häufig von Mail-, FTP- und IRC-Servern eingesetzt. Er kann auch dazu verwendet werden, um einen Nutzer Ihres lokalen Systems, der ein entferntes System angreift, aufzuspüren.

Es gab ausführliche Diskussionen über die Sicherheit von `identd` (siehe in den `Archiven der Mailingliste`. Im Allgemeinen ist `identd` auf Multi-User-Systemen nützlicher als auch einer Workstation mit nur einem Benutzer. Wenn Sie keine Verwendung von ihn haben, sollten Sie ihn abschalten, damit Sie keinen Dienst für die Außenwelt offen lassen. Wenn Sie sich entscheiden, den identd-Port mit einer Firewall zu blockieren, benutzen Sie *bitte* die Regel 'reject' und nicht die Regel 'deny', da andernfalls eine Verbindung zu einem Server, die `identd` verwendet, bis zu einer Zeitüberschreitung hängen bleiben wird (lesen Sie dazu `reject or deny issues`).

12.1.14.5 Ich habe Dienste, die die Ports 1 und 6 verwenden. Welche sind das und wie kann ich sie entfernen?

Sie führen den Befehl `netstat -an` aus und erhalten Folgendes:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
-
raw        0      0 0.0.0.0:6               0.0.0.0:*               7
-
```

Sie sehen *nicht* Prozesse, die auf dem TCP/UDP-Port 1 und 6 lauschen. Tatsächlich sehen Sie einen Prozess, der auf einem *Raw*-Socket für Protokoll 1 (ICMP) und 6 (TCP) lauscht. Ein solches Verhalten ist für Trojaner und einige Systeme zur Eindringlingserkennung wie `iplogger` und `portsentry` üblich. Wenn Sie diese Pakete besitzen, löschen Sie sie einfach. Falls nicht, versuchen Sie mit netcats Option `-p` (Prozess) herauszufinden, welcher Prozess diese Lauscher betreibt.

12.1.14.6 Ich habe festgestellt, dass ich den folgenden Port (XYZ) offen habe. Kann ich ihn schließen?

Ja, natürlich. Die Ports, die Sie offen lassen, hängen von Ihrem individuellen Regelwerk bezüglich öffentlich zugänglicher Dienste ab. Prüfen Sie, ob sie von `inetd` (siehe Abschalten von `inetd` oder seinen Diensten, Abschnitt 3.6.2) oder von anderen installierten Paketen geöffnet werden, und leiten Sie passende Maßnahmen ein (d.h. konfigurieren Sie inetd, entfernen Sie das Paket, verhindern Sie, dass der Dienst beim Booten gestartet wird).

12.1.14.7 Hilft das Löschen von Diensten aus `/etc/services`, um meinen Rechner abzusichern.

Nein, `/etc/services` stellt nur eine Verbindung zwischen virtuellem Namen und Portnummer her. Das Entfernen von Namen aus dieser Datei verhindert (üblicherweise) nicht, dass ein Dienst gestartet wird. Manche Daemonen starten vielleicht nicht, wenn `/etc/services` verändert wurde, aber das ist nicht die Norm. Um einen Dienst richtig abzuschalten, sehen Sie sich Daemons abschalten, Abschnitt 3.6.1 an.

12.1.15 Allgemeine Sicherheitsfragen

12.1.15.1 Ich habe mein Passwort vergessen und kann auf das System nicht mehr zugreifen!

Die nötigen Schritte, um wieder Zugriff erhalten, hängen davon ab, ob Sie die vorgeschlagene Prozedur zum Absichern von `lilo` und BIOS durchgeführt haben oder nicht.

Wenn Sie beides eingeschränkt haben, müssen Sie im BIOS erlauben, von anderen Medien als der Festplatte zu booten, bevor Sie weitermachen können. Wenn Sie auch Ihr BIOS-Passwort vergessen haben, müssen Sie Ihr BIOS zurücksetzen. Dazu öffnen Sie das PC-Gehäuse und entfernen die BIOS-Batterie.

Sobald Sie das Booten von CD-ROM oder Diskette eingeschaltet haben, sollten Sie Folgendes ausprobieren:

- Booten Sie von eine Rettungsdiskette und starten den Kernel.
- Wechseln Sie mit Alt+F2 auf eine virtuelle Konsole.
- Mounten Sie die Partition, auf der sich Ihr /root befindet.
- Editieren Sie (auf der Rettungsdiskette von Debian 2.2 befindet sich `ae`, Debian 3.0 enthält `nano-tiny`, der `vi` ähnelt) die Datei `/etc/shadow` und ändern Sie die Zeile:

  ```
  root:asdfjl290341274075:XXXX:X:XXXX:X::: (X=irgendeine Ziffer)
  ```

  in:

  ```
  root::XXXX:X:XXXX:X:::
  ```

Dies entfernt das vergessene Root-Passwort, das sich im ersten durch Doppelpunkte abgetrennten Feld nach dem Nutzernamen befand. Speichern Sie die Datei ab, starten Sie das System neu und melden Sie sich als Root mit einem leeren Passwort an. Dies wird funktionieren, außer wenn Sie Ihr System etwas sicherer eingestellt haben, d.h. wenn Sie nicht erlauben, dass Nutzer leere Passwörter haben, oder dass Root sich auf einer Konsole einloggen kann.

Falls Sie derartige Maßnahmen getroffen haben, müssen Sie im Single-User-Modus starten. Wenn Sie LILO eingeschränkt haben, müssen `lilo` erneut ausführen, nachdem Sie das Root-Passwort zurückgesetzt haben. Das ist

ziemlich verzwickt, da Ihre `/etc/lilo.conf` verändert werden muss, da das Root-Dateisystem (/) eine RAM-Disk und keine echte Festplatte ist.

Sobald LILO nicht mehr eingeschränkt ist, versuchen Sie Folgendes:

- Drücken Sie Alt, Shift oder Steuerung (Control), kurz bevor das BIOS seine Arbeit beendet hat, und Sie sollten nun einen LILO-Prompt erhalten.
- Geben Sie am Prompt `linux single`, `linux init=/bin/sh` oder `linux 1` ein.
- Sie erhalten einen Shell-Prompt im Single-User-Modus (Sie werden nach dem Passwort gefragt, aber das kennen Sie jetzt ja)
- Binden Sie die Root-Partition (/) im Schreib/Lese-Modus neu ein, indem Sie den Befehl mount verwenden:

```
mount -o remount,rw /
```

- Ändern Sie das Superuser-Passwort mit `passwd` (da Sie der Superuser sind, werden Sie nicht nach dem alten Passwort gefragt).

12.1.16 Wie muss ich vorgehen, wenn ich meinen Nutzern einen Dienst anbieten möchte, ihnen aber kein Shell-Konto geben will?

Wenn Sie zum Beispiel einen POP-Dienst anbieten wollen, müssen Sie nicht für jeden zugreifenden Benutzer ein Konto anlegen. Am besten setzen Sie hierzu eine Authentifizierung, die auf Verzeichnisses basiert, durch einen externen Dienst (wie Radius, LDAP oder eine SQL-Datenbank) ein. Installieren Sie einfach die gewünschte PAM-Bibliothek (`libpam-radius-auth`, `libpam-ldap`, `libpam-pgsql` oder `libpam-mysql`), lesen Sie die Dokumentation (Einsteiger sehen bitte unter Nutzerauthentifizierung: PAM, Abschnitt 4.11.1 nach) und konfigurieren Sie den PAM-nutzenden Dienst, so dass er Ihren Backend benutzt. Bearbeiten Sie dazu die dem Dienst entsprechenden Dateien unter `/etc/pam.d/` und ändern die folgenden Zeile von

```
auth    required        pam_unix_auth.so shadow nullok use_first_pass
```

beispielsweise für ldap zu:

```
auth    required        pam_ldap.so
```

Im Fall von LDAP-Verzeichnissen liefern manche Dienste LDAP-Schemata mit, die Sie Ihrem Verzeichnis hinzufügen können, um eine LDAP-Authentifizierung zu benutzen. Wenn Sie relationale Datenbanken benutzen, gibt es einen nützlichen Trick: Benutzen Sie die Klausel *where*, wenn Sie die PAM-Module konfigurieren. Wenn Sie beispielsweise eine Datenbank mit der folgenden Tabelle haben:

```
(user_id,user_name,realname,shell,password,uid,gid,homedir,sys,pop,imap,ftp)
```

Wenn Sie die Attribute der Dienste zu Boolean-Feldern machen, können Sie sie verwenden, um den Zugang zu den verschiedenen Diensten zu erlauben oder zu verbieten. Sie müssen dazu nur die geeigneten Zeilen in folgende Dateien einfügen:

- `/etc/pam.d/imap`:`where=imap=1`.
- `/etc/pam.d/qpopper`:`where=pop=1`.
- `/etc/nss-mysql*.conf`:`users.where_clause = user.sys = 1;`.
- `/etc/proftpd.conf`:`SQLWhereClause "ftp=1"`.

12.2 Mein System ist angreifbar! (Sind Sie sich sicher?)

12.2.1 Der Scanner X zur Einschätzung der Verwundbarkeit sagt, dass mein Debian-System verwundbar wäre?

Viele Scanner zur Einschätzung der Verwundbarkeit liefern falsche Positivmeldungen, wenn sie auf Debian-Systemen verwendet werden. Das liegt daran, dass sie nur die Version eines Softwarepakets überprüfen, um herauszufinden, ob es verwundbar ist. Sie prüfen nicht, ob tatsächlich eine Sicherheitslücke vorhanden ist. Da Debian nicht die Version einer Software ändert, wenn ein Paket repariert wird (häufig werden Ausbesserungen an neueren Veröffentlichungen zurückportiert), neigen einige Werkzeuge dazu zu denken, dass ein aktualisiertes Debian-System verwundbar ist, auch wenn das nicht der Fall ist.

Wenn Sie denken, dass Ihr System auf dem aktuellen Stand der Sicherheitsaktualisierungen ist, sollten Sie die Querverweise zu den Datenbanken mit Sicherheitslücken, in denen die DSAs veröffentlicht sind (vergleichen Sie dazu Debian-Sicherheits-Ankündigungen, Abschnitt 7.2), verwenden, um falsche Positive auszusondern, wenn das Programm, das Sie verwenden, CVE-Referenzen enthält.

12.2.2 Ich habe in meinen Logfiles einen Angriff gesehen: Ist mein System kompromittiert?

Ein Hinweis auf einen Angriff heißt nicht notwendigerweise, dass Ihr System gehackt wurde. Leiten Sie die üblichen Schritte ein, um festzustellen, ob das System kompromittiert wurde (siehe Nach einer Kompromittierung (Reaktion auf einem Vorfall), Kapitel 11). Selbst wenn Ihr System hinsichtlich des protokollierten Angriffs nicht verwundbar ist, könnte ein entschlossener Angreifer neben der von Ihnen entdeckten Sicherheitslücke auch eine andere ausgenutzt haben.

12.2.3 Ich habe in meinen Logs merkwürdige »MARK«-Einträge gefunden. Wurde ich gehackt?

Sie können die folgenden Zeilen in Ihren System-Logs finden:

```
Dec 30 07:33:36 debian -- MARK --
Dec 30 07:53:36 debian -- MARK --
Dec 30 08:13:36 debian -- MARK --
```

Dies stellt keinen Hinweis auf eine Kompromittierung dar, obwohl Nutzer, die von einer Debian-Release wechseln, es vielleicht merkwürdig finden. Wenn Ihr System keine große Last (oder nicht viele aktive Dienste) hat, können diese Zeilen in alle Logs auftauchen. Dies ist ein Hinweis, dass Ihr `syslogd`-Daemon richtig läuft. Aus `syslogd(8)`:

```
-m interval
       Der Syslogd protokolliert regelmäßig einen
       Zeitstempel. Der voreingestellte Abstand zwischen zwei --
       MARK -- Zeilen ist 20 Minuten. Er kann mit dieser Option
       geändert werden. Setzen Sie den Abstand auf Null, um
       die Zeitstempel komplett abzuschalten.
```

12.2.4 Ich habe Nutzer gefunden, die laut meinen Logfiles 'su' benutzen: Bin ich kompromittiert?

Sie könnten in Ihren Logdateien Zeilen wie die folgenden finden:

```
Apr  1 09:25:01 server su[30315]: + ??? root-nobody
Apr  1 09:25:01 server PAM_unix[30315]: (su) session opened for user nobody by (uid=0)
```

Seien Sie nicht zu besorgt. Prüfen Sie, ob dies durch einen `Cron`-Job hervorgerufen wird (normalerweise `/etc/cron.daily/find` oder `logrotate`):

```
$ grep 25 /etc/crontab
25 9    * * *   root    test -e /usr/sbin/anacron || run-parts --report
/etc/cron.daily
$ grep nobody /etc/cron.daily/*
find:cd / && updatedb --localuser=nobody 2>/dev/null
```

12.2.5 Ich habe 'possible SYN flooding' in meinen Logs entdeckt: Werde ich angegriffen?

Sie sehen Einträge wie diese in Ihren Logs:

```
May 1 12:35:25 linux kernel: possible SYN flooding on port X. Sending cookies.
May 1 12:36:25 linux kernel: possible SYN flooding on port X. Sending cookies.
May 1 12:37:25 linux kernel: possible SYN flooding on port X. Sending cookies.
May 1 13:43:11 linux kernel: possible SYN flooding on port X. Sending cookies.
```

Überprüfen Sie mit `netstat`, ob es eine große Anzahl von Verbindungen zum Server gibt. Zum Beispiel:

```
linux:~# netstat -ant | grep SYN_RECV | wc -l
   9000
```

Dies ist ein Anzeichen, dass ein Denial-of-Service-Angriff (DoS) auf den Port X Ihres Systems (am wahrscheinlichsten gegen einen öffentlichen Dienst wie Ihr Web- oder Mailserver). Sie sollten TCP-Syncookies in Ihrem Kernel einschalten, siehe Konfiguration von Syncookies, Abschnitt 4.18.2. Beachten Sie, dass ein DoS-Angriff Ihr Netzwerk überfluten kann, auch wenn Sie verhindern können, dass er Ihr System zum Absturz bringt. [86] Der einzige effektive Weg, diesen Angriff abzuwehren, ist, mit Ihrem Netzprovider in Verbindung zu treten.

12.2.6 Ich habe seltsame Root-Sessions in meinen Logs entdeckt: Wurde ich gehackt?

Sie sehen folgende Art von Einträgen in der Datei `/var/log/auth.log`:

```
May 2 11:55:02 linux PAM_unix[1477]: (cron) session closed for user root
May 2 11:55:02 linux PAM_unix[1476]: (cron) session closed for user root
May 2 12:00:01 linux PAM_unix[1536]: (cron) session opened for user root by
(UID=0)
May 2 12:00:02 linux PAM_unix[1536]: (cron) session closed for user root
```

Sie kommen von einem ausgeführten `Cron`-Job (in unserem Beispiel alle fünf Minuten). Um herauszufinden, welches Programm für diese Jobs verantwortlich ist, überprüfen Sie die Einträge in `/etc/crontab`, `/etc/cron.d`, `/etc/crond.daily` und Roots `crontab` in `/var/spool/cron/crontabs`.

12.2.7 Ich bin Opfer eines Einbruchs, was soll ich jetzt tun?

Es gibt mehrere Schritte, die Sie bei einem Einbruch durchführen sollten:

- Prüfen Sie, ob Ihr System auf dem aktuellen Stand der Sicherheitsaktualisierungen für veröffentlichte Verwundbarkeiten ist. Wenn Ihr System verwundbar ist, hat die die Möglichkeit, dass Ihr System tatsächlich gehackt wurde, erhöht. Die Wahrscheinlichkeit steigt weiter an, wenn die Sicherheitslücke schon eine Zeit lang bekannt ist, da üblicherweise mehr Tätigkeit mit älteren Verwundbarkeiten besteht. Hier ist ein Link zu `SANS Top 20 Security Vulnerabilities`.
- Lesen Sie dieses Dokument, besonders den Abschnitt Nach einer Kompromittierung (Reaktion auf einem Vorfall), Kapitel 11.
- Fragen Sie nach Hilfe. Sie können die Mailingliste debian-security benutzen und um Rat fragen, wie Sie Ihr System wiederherstellen oder patchen.
- Benachrichtigen Sie Ihren lokalen `CERT` (wenn einer existiert, ansonsten sollten Sie sich vielleicht direkt mit CERT in Verbindung setzen). Das könnte Ihnen helfen (vielleicht aber auch nicht), aber wenigstens wird CERT über laufende Angriffe informiert. Diese Information ist sehr wertvoll, um herauszufinden, welche Werkzeuge und Angriffsarten von der *Blackhat*-Community verwendet werden.

12.2.8 Wie verfolge ich einen Angriff zurück?

Sie können einen Angriff zu seinem Ursprung zurückverfolgen, indem Sie die Logs (wenn sie nicht geändert wurden) mit Hilfe eines Systems zur Eindringlingserkennung (siehe Aufsetzen einer Eindringlingserkennung, Abschnitt 10.3), `traceroute`, `whois` oder ähnlicher Werkzeuge (einschließlich forensischer Analyse) durchsehen. Wie Sie auf diese Informationen reagieren und was *Sie* als Angriff betrachten, hängt ausschließlich von Ihren Sicherheitsrichtlinien ab. Ist ein einfacher Scan ein Angriff? Ist die Prüfung auf eine Verwundbarkeit ein Angriff?

12.2.9 Das Programm X in Debian ist angreifbar – was soll ich tun?

Nehmen Sie sich zuerst einen Augenblick Zeit, um zu schauen, ob die Sicherheitslücke in öffentlichen Sicherheitsmailinglisten (wie Bugtraq) oder anderen Foren bekannt gemacht wurde. Das Sicherheitsteam von Debian ist hinsichtlich dieser Listen auf dem Laufenden, daher könnte ihm dieses Problem bereits bekannt sein. Leiten Sie keine weiteren Maßnahmen ein, wenn Sie schon eine Bekanntmachung auf `http://security.debian.org` sehen.

Wenn anscheinend keine Informationen veröffentlicht wurden, schicken Sie bitte eine E-Mail zu den betroffenen Paketen mit einer detaillierten Beschreibung der Verwundbarkeit (Code, der dies bestätigt, ist auch in Ordnung) an `team@security.debian.org`. Dort erreichen Sie das Sicherheitsteam von Debian.

12.2.10 Laut der Versionsnummer eines Paketes läuft bei mir immer noch eine angreifbare Version!

Statt auf neue Veröffentlichung zu aktualisieren, portiert Debian sicherheitsrelevante Korrekturen zu der Version zurück, die in der Stable-Veröffentlichung enthalten ist. Der Grund dafür ist, dass sicher gegangen werden soll, dass die Stable-Veröffentlichung so wenig wie möglich verändert wird. Damit wird verhindert, dass sich Dinge als Folge einer Sicherheitskorrektur unerwartet ändern oder kaputt gehen. Ob Sie eine sichere Version eines Paketes benutzen, stellen Sie fest, indem Sie das Changelog des Paketes durchsehen, oder indem Sie die exakte Versionsnummer (ursprüngliche Version -slash- Debian-Release) mit der Nummer aus der Debian-Sicherheits-Ankündigung (DSA) vergleichen.

12.2.11 Spezielle Software

12.2.11.1 `Proftpd` ist für einen Denial-of-Service-Angriff anfällig.

Fügen Sie Ihrer Konfigurationsdatei `DenyFilter \*.*/` hinzu. Mehr Informationen entnehmen Sie `http://www.proftpd.org/bugs.html`.

12.2.11.2 Nach der Installation von `portsentry` sind viele Ports offen.

Dies ist nur die Art und Weise, wie `portsentry` arbeitet. Es öffnet etwas zwanzig ungenutzte Ports und versucht so, Port-Scans zu entdecken.

12.3 Fragen zum Sicherheitsteam von Debian

Diese Informationen stammen aus dem `Debian Sicherheits-FAQ`.

Version: 3.11, Sat, 17 Jan 2015 16:19:18 +0000

Javier Fernández-Sanguino Peña `jfs@debian.org`
Autoren, Abschnitt 1.1
