Auf den Punkt gebracht

Leserbriefe

Haben Sie Anregungen, Statements oder Kommentare? Dann schreiben Sie an [redaktion@linux-magazin.de]. Die Redaktion behält es sich vor, die Zuschriften und Leserbriefe zu kürzen. Alle Beiträge werden mit Namen veröffentlicht, sofern nicht ausdrücklich Anonymität gewünscht wird.

Dyndns

07/04, S. 80: Erst mal Glückwünsche zur neuen Aufmachung der letzten Ausgaben; die sehen nicht mehr so verspielt und damit professioneller aus.
Ich habe zum Artikel von Marc André Selig noch einige Fragen: Falls ich das richtig verstehe, kann man sich mit seiner registrierten Domain bei Dyndns.org rgistrieren und dann mittels des DNS-Eintrages im Router (Abbildung 1 des Artikels) die aktuelle IP abfragen? Die Abfrage erfolgt dann von meiner Linux-Kiste intern an meinen Router, der wiederum die Abfrage an Dyndns.org weiterleitet?
Spielt der verwendete DSL-Provider hierbei noch eine Rolle beziehungsweise muss der noch was schalten? Ich würde mich über eine kurze Antwort freuen, da mich dieses Thema sehr interessiert.
Jochen Konrad, per E-Mail

Sie können mit dem dargestellten Werkzeug nur die aktuelle IP setzen. Die DNS-Datenbank liegt in diesem Fall bei Dyndns.org. Jedes Mal, wenn sich Ihre IP ändert (beispielsweise beim Aufbau einer Internetverbindung), schickt Ihr Router die neue IP an den Anbieter und aktualisiert die dortige Datenbank.
Die Abfrage einer IP erfolgt, von wem auch immer, an Dyndns.org. Wenn Sie selbst Ihre IP abfragen, wird die Anfrage von Ihrem Rechner je nach Konfiguration unter Umständen an Ihren Router oder Ihren Provider weitergeleitet, auf alle Fälle aber letztlich von Dyndns.org beantwortet, richtig. Gibt jemand anderes Ihren Hostnamen ein, fragt sein Computer beziehungsweise sein Provider ebenfalls den DNS-Server von Dyndns.org.
Der jeweilige DSL-Provider hat keinen Einfluss darauf. Hätte er das, würde er es wohl in vielen Fällen unterbinden, DSL-Provider sehen diese Praxis nämlich nicht gerne. Allerdings können sie auch nicht viel dagegen unternehmen. (Marc André Selig)

Spam-Header

09/04, S. 54: Ich betreibe privat einige Domains und hoste darunter ein paar kleinere Firmen und Organisationen. Ihr Artikel über Sponts (Spezialfilter) war recht interessant. Was ich bei der kleinen Box vermisse, ist ein Konzept, das den Header sauber analysiert, bevor der Body einer Mail untersucht wird. Das würde meiner Meinung nach Zeit und Ressourcen sparen.
Kennen Sie eine Methode, Spam zu simulieren ohne echten Spam auf sich zu ziehen? Ich würde irgendwie gerne wissen, was passiert, wenn wirklich viele Mails auf den Server einprasseln.
Axel Thobabe, per E-Mail

Da kann ich nur Radio Eriwan zitieren: Im Prinzip ja. In der Praxis jedoch ist das Problem, dass im SMTP-Protokoll (siehe Kasten „SMTP-Dialog“ im Artikel) zwischen Header und Body der Nachricht nicht unterschieden wird. Somit werden Header und Body komplett übertragen und können dann auch gleich komplett ausgewertet werden.
Die Box verwendet als letzte Filterstufe Spamassassin: Der kann natürlich sehr schön Header und Body getrennt und zusammen filtern. Mittlerweile, so habe ich vom Hersteller erfahren, lässt sich der Spamd auch über einen SSH-Zugang als Root frei konfigurieren.
Ein Weg zu künstlichem Spam: Man nehme ein Spam-Postfach, sammle den Müll einige Tage, schreibe das Ganze in eine (oder mehrere) Dateien, gebe vielleicht noch einigen „Ham“ dazu, füge oben geeignete »RCPT TO:«-, »MAIL FROM:«- und »DATA«-Zeilen ein und schicke alles über das lokale Netz (gegebenenfalls von mehreren Rechnern) mit 100 MBit/s an den Mailserver. Dann zeigt sich schnell, was passiert. (Tobias Eggendorfer)

09/04, S. 54: Im Artikel ist vom „Sponts-Effekt“ die Rede. Meiner Erfahrung nach haben die meisten Spam-Mails gefälschte Absenderadressen. Es ist also anzunehmen, dass den meisten Spammern eine entsprechende Meldung nie zukommt. Hier zeigt sich ein grundsätzliches Problem von Spamfiltern, die Mails ablehnen. Die Spam-Mail wird in der Regel an einen Dritten – dem die gefälschte Absenderadresse gehört – weitergeleitet. Das erhöht tatsächlich das Aufkommen von Spam.
Die Meldung »user unknown« ist zudem eine gezielte Falschmeldung, die einem ehrlichen Absender die Fehlersuche erschwert. Im Zusammenhang mit Mailfilterung wird oft darauf hingewiesen, dass die Funktionalität „Mail verschicken“ nicht beeinträchtigt werden darf.
Frank Schwichtenberg, per E-Mail

Das kann ich so nicht nachvollziehen: Hier wird keine Fehlermeldungs-Mail verschickt, sondern direkt im SMTP-Dialog ein »user unknown« gesendet. Damit erfährt der versendende Mailserver, dass der Empfänger nicht existiert.
Der versendende Mailserver ist häufig unter Kontrolle der Spammer: Stellt dieser von seinem Rechner über eine Dial-in-

Leitung oder über einen Proxy zu, dann bekommt seine Mailsoftware die Fehlermeldung direkt zu Gesicht.
Kritisch könnte die Zustellung von Spam über ein Open Relay sein: Hier ist das Open Relay für die Verarbeitung der Fehlermeldung zuständig und könnte tatsächlich einen fehlerhaften Zustellversuch unternehmen.
Allerdings ist die Verwendung von Open Relays auf Seiten der Spammer rückläufig. Gängig dürfte mittlerweile die Verwendung von Würmern/Trojanern sein. Bei denen funktioniert das Verfahren jedoch problemlos. (Tobias Eggendorfer)

Rsync

09/04, S. 72: Der Artikel „Snapshot-Backups mit Rsync" beschreibt eine sehr elegante Lösung, die tatsächlich schon implementiert und veröffentlicht worden ist unter dem Namen Rsnapshot [http://www.rsnapshot.org]. Ich setze es auf Tipp eines Freundes seit einiger Zeit zum Mirroring ein.
Erwähnenswert ist an dieser Stelle ein »# du -sch $DATA_PATH/$SERVER/*«, das für das erste Verzeichnis die volle Größe, für alle folgenden nur noch den zusätzlichen Platzverbrauch sowie am Ende die Summe ausgibt.
Arvid Requate, per E-Mail

Evolution-Exchange

09/04, S. 74: Ich habe den Artikel über Evolution-Exchange mit Freude gelesen, habe dann aber leider feststellen müssen, dass unter der von Euch unter [4] angegebenen Quelle für Debian nur Pakete für die PPC-Architektur liegen. Es gibt aber zwei andere Quellen für i386-Sources:

```
deb http://adam.rosi-kessel.org/debian
 unstable main
```

über Apt oder unmittelbar auf [http://adam.rosi-kessel.org/debian/dists/unstable/main/binary-i386/gnome/] im Web.
Carsten Muck, per E-Mail

Unsichere Hoster

10/04, S. 56: Ich fand den Artikel „Reingehackt und aufgeschrieben" wirklich interessant. Aus meiner Sicht als ehemaliger Kunde entspricht die Reaktion der Admins in etwa der des Supports, nämlich nahezu inexistent.
Micha Espey, per E-Mail

10/04, S. 56: Nach dem ausführlichen Lesen des Berichts „Insel-Hüpfer" sollte doch auch mal auf mögliche Alternativen zu Confixx eingegangen werden. Denn dass Confixx Probleme mit der Sicherheit hat, wird ja immer wieder bestätigt. Mir fällt dabei spontan VAMSYS [http://vamsys.de] ein. Ich persönlich halte es für eine wirklich empfehlenswerte Alternative.
Christian Coenes, per E-Mail

SW-Soft hat für die aktuelle Confixx-Release immerhin ein Patch produziert. Das macht Confixx jetzt nicht prinzipiell zum Saubermann, aber immerhin hat der Hersteller reagiert. (fjl)

10/04, S. 56: Bei allem Respekt vor dem Stolz des Autors des Artikels: Ihr Vorgehen war verantwortungslos. Es gibt überhaupt keinen Grund, das Root-Passwort wiederzugeben, ein einfaches „Das Passwort war sicher" hätte definitiv ausgereicht. Ein korrektes Vorgehen bei dieser Publikation wäre meines Erachtens gewesen: Artikel redigieren und Dinge wie das Passwort entfernen. Den Provider informieren – eine Kopie des Artikels zustellen. Erst wenn die Löcher geschlossen sind, sollte der Artikel veröffentlicht werden.
Bei aller Achtung vor Ihrer Berichterstattung und Ihren sonst gelungenen Artikeln: So was darf nicht passieren. Nie mehr! Bitte!
Philip Hofstetter, per E-Mail

Damit ein solcher Artikel glaubhaft ist, muss er durch Details Authentizität beweisen. Das ist der einzige Grund für das Veröffentlichen der Passwörter. Aus dem gleichen Grund flechten auch andere Medien solche Details in ihre Artikel ein. Die betroffene Firma hat vorab den Artikel erhalten. Ziel des Beitrags war es sicher nicht, einen Provider an den Pranger zu stellen. Vielmehr wollten wir sowohl bei den Hostern als auch bei deren Kunden das Bewusstsein für Sicherheitsprobleme und sinnvolle Systemadministration schärfen. Das Publizieren auch kontroverser Sachverhalte gehört zur Aufgabe der freien Presse. (jk) ■

Errata

In der Ausgabe 09/04, S. 32, ist der Preis für den Suse Linux Desktop mit 630 Euro angegeben. In diesem Preis ist jedoch auch die Installation auf fünf Clients enthalten.

In der Ausgabe 10/04, S. 17, hat sich eine Namensverwechslung eingeschlichen: Die Datenbank von IBM heißt richtig „Cloudscape" und nicht „Cloudspace". Zu finden ist sie auf der Seite: [http://www-306.ibm.com/software/data/cloudscape/]

In der Meldung zu OpenFTPD in Ausgabe 10/04, S. 33, steht im letzten Absatz „ProFTPD 0.30.2". Richtig ist „OpenFTPD 0.30.2".

In den Infos zum Artikel „Tapetenwechsel" ab Seite 44 in Ausgabe 10/04 sind die URL-Verweise im Text ab Nummer [4] verrutscht: Statt [4] ist tatsächlich [5] gemeint, statt [5] die [6] und so weiter.

In der gleichen Ausgabe fehlt auf Seite 46 die Abbildung 2, auf die verwiesen wird. Sie finden sie hier rechts abgedruckt sowie im Web auf: [http://www.linux-magazin.de/Artikel/ausgabe/2004/10/Ablauf-Schema.png]

In der Ausgabe 10/04, S. 100, schrieben wir in der Projektekü-che: „Unter anderem geht es um die Entfernung jeder Dokumentation, die nicht unter der GFDL steht." In diesem Satz ist das Wort „nicht" zu viel.

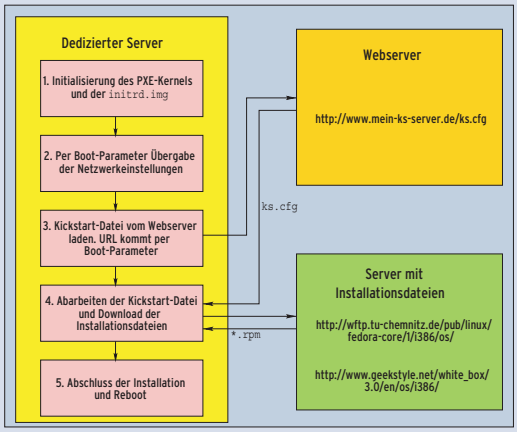

Abbildung: Diese Grafik illustriert die Installation von Fedora auf einem dedizierten Server. Sie fehlte in der Ausgabe 10/04.