Das Linux-Systemhaus

[**Linux**] [**Software**] [**Unternehmen**]

in-put LinuxNews 08/2011

Vorbemerkung:
Sie erhalten hiermit die achte Ausgabe der "in-put LinuxNews". Mit diesem monatlich erscheinenden Newsletter wollen wir Sie über Neuigkeiten rund um Linux, sowie über neue und hilfreiche Programme informieren. Desweiteren stellen wir in jeder Ausgabe ein Tool aus der Linux-Werkzeugkiste vor, das dem Linux-Anwender das Leben erleichtern wird.
Für Fragen und Kommentare freuen wir uns über Ihr Feedback an die Adresse **feedback@in-put.de**

Neuigkeiten:

1. Linux-Kernel 3.0 freigegeben [**Weitere Informationen**]
2. Red Hat Enterprise Linux 5.7 freigegeben [**Weitere Informationen**]
3. Linux-Verband und Lisog verschmelzen [**Weitere Informationen**]
4. Samba 3.6.0 bringt volle SMB2-Unterstützung [**Weitere Informationen]**

Der Griff in die Linux-Werkzeugkiste: tcpdump
Wer als Administrator dem Netzwerk auf die Finger schauen will, kommt auf der Kommandozeile selten um tcpdump herum. Die Anhänger der grafischen Oberfläche greifen zu Wireshark, welches dieselbe libpcap Bibliothek wie tcpdump verwendet.

tcpdump ist ein Netzwerksniffer, welcher sich mit einem vorgegebenen Netzwerkport verbindet und die Details zu allen Datenpaketen anzeigt. Erfahrungsgemäß ist der Output sehr umfangreich, daher wollen wir uns einige Filtermöglichkeiten näher anschauen.

Startet man tcpdump ohne einen Parameter, überwacht es automatisch die erste Netzwerkschnittstelle, zumeist eth0. Soll eine andere Schnittstelle überwacht werden, muss man dies tcpdump mit dem Parameter "-i" mitteilen:

```
tcpdump -i eth1
```

Damit tcpdump die Namensauflösung unterläßt, IP-Adresse ausgibt und statt Portnamen die Portnummern, verwendet man den Parameter "-n":

```
tcpdump -n -i eth1
```

Möchte man überprüfen, ob der PC mit der IP-Adresse 192.168.1.100 tatsächlich keine Emails via POP3 abholen kann, startet man tcpdump auf dem Emailserver mit den folgenden Parametern:

```
tcpdump -i eth1 host 192.168.1.100 and port 110
```

Ist man sich nicht sicher, ob es POP3 oder IMAP ist, variiert man den Befehl:

```
tcpdump -i eth1 host 192.168.1.100 and "(port 110 or port 143)"
```

Da ein "and" stärker bindet als ein "or", fasst man die beiden Ports innerhalb der Klammer zusammen. Die Anführungszeichen sind erforderlich, da andernfalls die Shell eine Fehlermeldung ausgeben würde.

Weitere Informationen zu *tcpdump* findet man in den man pages (*man tcpdump*) oder schicken Sie uns eine Email an **feedback@in-put.de**

Programm des Monats: Emails verschlüsseln und signieren mit Djigzo

Emails werden zumeist im Klartext verschickt. Das bedeutet, dass jeder der Zugriff auf den Datenstrom hat, den Inhalt der Emails lesen kann. Dies ist inzwischen für die meisten Unternehmen, Institutionen und Organisationen inakzeptabel - Emails müssen vertraulich sein und verschlüsselt werden.

Djigzo ist ein zentraler Mail Transfer Agent (MTA), der nach dem "store and forward" Prinzip arbeitet: Eingehende Emails, gleichgültig ob von intern oder extern, werden nur so lange gespeichert, bis sie ver-/entschlüsselt wurden und an die Bestimmungsadresse weitergeleitet werden können.

Wesentliche Features von Djigzo sind unter anderem:

- Kann als Appliance vor dem Emailserver (MS Exchange, Lotus Domino, etc.) eingesetzt oder auf dem Emailserver installiert werden, wenn es sich um eine Linux-Distribution handelt.
- Keine Änderungen und Anpassungen an den Email-Clients für die Verschlüsselung erforderlich.
- Informiert den Absender über eine erfolgreiche Verschlüsselung.
- Webinterface für die Administration.
- Data Leak Prevention: Ausgehende Emails können nach Keywords und mit regulären Ausdrücken durchsucht und der Versand verhindert werden.
- Open Source Software, lizenziert nach AGPLv3.

Weitere Informationen zu Djigzo erhalten Sie unter **http://www.djigzo.de/**

Aktuelle Schulungstermine:

24. - 26. August 2011 **Nagios: Linux-Systemmonitoring**
07. - 08. September 2011 **VPN mit Linux - OpenSWAN/StrongSwan**
12. - 16. September 2011 **Programmieren mit PHP**
19. - 21. September 2011 **Samba-Server**
27. - 30. September 2011 **Linux-Systemadministration**
18. - 20. Oktober 2011 **Nagios: Linux-Systemmonitoring**
25. - 26. Oktober 2011 **OpenLDAP-Server**

Weitere Informationen und Termine unter **http://www.in-put.de/linux/schulungen.html**

Schlusssatz:
Sie erhalten unseren Newsletter, weil es in der Vergangenheit oder aktuell einen Kontakt oder Geschäftsvorgang zwischen Ihnen und der in-put GbR gab oder gibt. Sollten Sie an unseren Dienstleistungen und Produkten generell nicht mehr interessiert sein, so bedauern wir dies.
Bitte klicken Sie auf den unten angegebenen Link, um sich von unserem Newsletter abzumelden.

in-put powered by Linux since 1996

in-put GbR · Moltkestrasse 49 · D -76133 Karlsruhe
Tel./Fax: +49 (0) 7 21 / 6 80 32 88 -0 / -3
Kontakt-Formular Email: **kontakt@in-put.de**