Erik Brändli

Technologie ITSecx

Erik Brändli

Hüseyin Bozkurt

TcpDump

Traffic-Analysierer

Contents

[Changelog 1](#_Toc422320640)

[tcpdump 2](#_Toc422320641)

[Hersteller (Das Tcpdump-Team) 2](#_Toc422320642)

[Produktdaten 2](#_Toc422320643)

[Globale Anwendung 3](#_Toc422320644)

[Entscheidungsgrundlagen 3](#_Toc422320645)

# Changelog

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Datum* | *Name* | *Unterschrift* |
| Erstellt | 17.06.15 | Erik Brändli |  |
| Geprüft | 18.06.15 | Hüseyin Bozkurt |  |
| Freigegeben |  |  |  |

# tcpdump

## Hersteller (Das Tcpdump-Team)

### Produktdaten

Aktuelle Version 4.7.4  
Betriebssysteme: Unix & Linux Abkömmlinge

Tcpdump ist eine Software zur Überwachung und Auswertung von Netzwerkverkehr. Sie wurde von Van Jacobson, Craig Leres und Steven McCanne geschrieben, wird aber mittlerweile von vielen anderen weiterentwickelt. Tcpdump arbeitet im Textmodus und wird über die Kommandozeile gesteuert.Das Programm liest Daten in Form von Paketen, die über das Netzwerk gesendet werden, und stellt diese auf dem Bildschirm dar oder speichert sie in Dateien. Durch die Umstellung eines Netzwerkadapters in den Promiscuous Mode ist es darüber hinaus möglich, Pakete, die nicht für diesen Netzwerkadapter bestimmt sind, zu empfangen und auszuwerten.

Zusätzlich ermöglicht tcpdump die Auswertung von vorher in Dateien gespeicherten Paketen. Mittels Parametern, die bei Programmstart auf der Kommandozeile angegeben werden müssen, steuert der Benutzer das Verhalten von tcpdump und übergibt Filter an das Programm, nach denen die Pakete ausgewertet werden.

## Globale Anwendung

Tcpdump ist eine Software zur Überwachung und Auswertung von Netzwerkverkehr. Sie wurde von Van Jacobson, Craig Leres und Steven McCanne geschrieben, wird aber mittlerweile von vielen anderen weiterentwickelt. Tcpdump arbeitet im Textmodus und wird über die Kommandozeile gesteuert.

Haupteinsatzgebiete von tcpdump sind:

* Fehlersuche in Programmen, die über das Netzwerk kommunizieren.
* Fehlersuche im Netzwerkaufbau selbst.
* Aufzeichnung und Darstellung der Kommunikation anderer Benutzer und Computer. Benutzern, die Zugriff auf Router oder Gateways innerhalb eines Netzwerkes haben, wird es hiermit ermöglicht, die Kommunikation zwischen verschiedenen Teilnehmern des Netzwerkes zu überwachen und mitzuschneiden. Da einige Protokolle ihre Übertragung unverschlüsselt abwickeln, ist es auf diese Weise möglich, Passwörter und Benutzerdaten aus dem Netzwerk zu erhalten.

## Entscheidungsgrundlagen

Gute Einsicht in die Daten von unzählig vielen Protokollen.

Live Ansicht und nachträgliche Offline Analysen