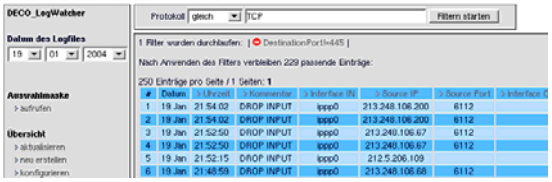
DECO_LogWatcher

Heutige Firewall-Systeme werden zunehmend komplexer und leistungsfähiger, als dies noch vor ein paar Jahren der Fall war. Hinzu kommen umfangreiche Logeinträge, die von Portscans, Attacken und anderen Abfragen aus dem Internet nur so wimmeln. Dementsprechend nimmt das Fehlerrisiko zu und Lücken können schlechter erkannt und vermieden werden. Die DECOIT GmbH setzt aus Gründen der Zuverlässigkeit, BSI-Empfehlungen und Lizenzkosten auf Open Source Software (OSS). In diesem Umfeld ist ein Monitoring noch schwieriger und komplexer, als dies bei kommerziellen Systemen ohnehin der Fall ist, da es keine zufrieden stellende Lösungen gib. Deshalb hat die DECOIT GmbH das eigene Monitoring-Tool DECO_LogWatcher auf Datenbankbasis entwickelt, welches auf OSS-Basis die Auswertung der entstandenen Logfiles effizient übernimmt.

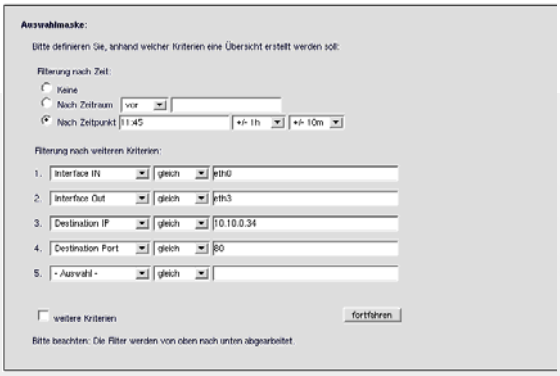
Der DECO_LogWatcher ist ein Web-basiertes Auswertungstool zur Fehlersuche und allgemeinen Kontrolle des Netzwerkverkehrs auf GNU/Linux-Systemen.

Durch sein Web-Interface ermöglicht er Administratoren eine vollkommen platt-form- und rechnerunabhängige Arbeit von jedem Rechner eines Netzwerks aus.

Auch die Verarbeitung von Logdaten eines ganzen Netzwerks ist dabei theoretisch möglich. Weiterhin können Filter nach Belieben verwendet werden. Die Grundoptionen beinhalten Rechnernamen, Kommentar, eingehendes/abgehendes Interface, Source IP, Source Port, Source Service, Destination IP/Port/Service und Protokoll. Erweiterte Optionen sind: MAC-Adresse, TOS, RES, PREC, DF-/SYN-/ACK-/PSH-/FIN-Flag, URGP, TYPE, CODE, TTL, Windows Size, Packet ID und SPI. Diese Optionen können zur Darstellung ausgewählt werden. Auch Erweiterungen stellen hier kein Problem dar, wenn nach weiteren Optionen gefiltert werden soll.



Die Konfiguration der Auswahlmasken zeigt die untere Abbildung. Hier kann die Filterung nach dem Zeitraum und weiteren Kriterien wie Interface, Destination etc. festgelegt werden.



Gefiltert werden grundsätzlich alle Informationen. Der DECO_LogWatcher übernimmt allerdings dabei die effiziente Aufarbeitung der Daten, sodass Fehlerquellen und Angriffsmuster sofort erkannt und eliminiert werden können.

Leistungsmerkmale:

- Einfache Überwachung eines einzelnen Hosts oder ganzen Netzwerks
- Automatische Aktualisierung der Log-Datenbank
- Dargestellte Logdaten lassen sich anhand von selbst definierten Filtern einschränken
- Filterung ist nach z.B. IP-Adressen, Port-Nummern, Interfaces, Protokollen, Paket-Flags und MAC-Adressen möglich
- Sämtliche in IP-Table-Logfiles enthaltene Daten lassen sich in die Filterung einbeziehen
- Zeitliche Eingrenzung durch das Setzen von Zeiträumen- und punkten ist möglich
- Filter lassen sich für den späteren Gebrauch speichern
- Filter sind beliebig kombinierbar
- Einfache Anpassung der Search-Engine an neue Parameter in den Logfiles
- Benutzerverwaltung, um jedem Benutzer ein individuelles Erscheinungsbild zu bieten
- Benutzerspezifische Konfiguration der GUI ist möglich

Systemanforderungen:

- Server: Linux System mit min. 1GHz CPU, 256 MByte RAM, Perl, Apache und Syslogd
- Client: PC mit min. 1 GHz CPU, 512 MByte RAM, Internet Explorer oder Mozilla

© DECOIT GmbH • Fahrenheitstraße 9 • D-28359 Bremen
Alle Rechte und technische Änderungen sind vorbehalten.
Die verwendeten Hard- und Softwarenamen sind Handelsnamen