

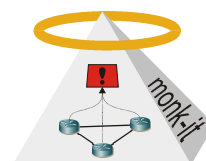


Diplomarbeit

Adaptive verteilte Firewallkonfiguration basierend auf Linux-Netfilter

Beschreibung:

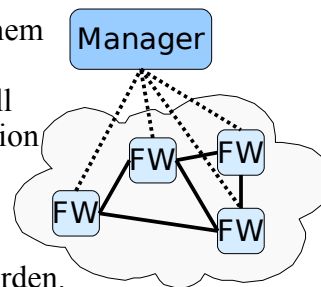
Mit der Anzahl der Internetnutzer und der angebotenen Dienstleistungen steigen auch Anzahl, Rate und Qualität von Angriffen. Viren und Würmer erreichen besorgniserregende Ausmaße. Es wird vom BSI ein Forschungsprojekt namens „monk-it“ finanziert, welches unter anderem ein effizientes und verteiltes Netzwerküberwachungssystem für Multi-Gigabit Netze implementiert. Das Ziel ist es, eine intelligente, selbstorganisierende Monitoringumgebung zu schaffen, die Analysen (z.B. Angriffserkennung) vereinfacht.



Durch bereits bestehende Überwachungssysteme wie unter anderem dem Intrusion Detection System Snort können sicherheitsrelevante Vorfälle in einem Netzwerk erkannt werden. Um die Anzahl der Angriffe ohne Administrationsaufwand einzuschränken, ist es sinnvoll, Firewalls dynamisch anhand der von Intrusion Detection Systemen einkommenden Ereignisse zu rekonfigurieren und so sich böswillig verhaltende Hosts aus dem Netzwerk auszuschließen.

Aufgabenstellung:

In der Diplomarbeit soll eine verteilte Architektur bestehend aus einem zentralen Konfigurationsmanager und mehreren rekonfigurierbaren Firewall-Clients entworfen werden. Der Konfigurationsmanager soll dabei sicherheitsrelevante Ereignisse im IDMEF-Format von Intrusion Detection Systemen empfangen und anhand einer zu definierenden Regelsprache entscheiden, ob und welche Firewalls böswillige Hosts aus dem Netzwerk ausschließen sollen. Dabei sollen die Firewall-Clients mit Hilfe des Netconf Protokolls instrumentiert werden. Im Rahmen dieser Arbeit soll dabei als zugrunde liegende Firewall-API Linux Netfilter verwendet werden.



Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Sicherheit sind wünschenswert.

Stichworte:

Angriffserkennung, Firewall, Rekonfiguration, Netfilter

Ansprechpartner:

Tobias Limmer
tobias.limmer@informatik.uni-erlangen.de
Raum 06.158

und Dr. Falko Dressler
dressler@informatik.uni-erlangen.de
Raum 06.157