

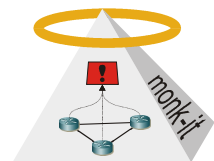


Studienarbeit

Entwicklung einer effizienten Filterung und Datenweiterleitung im Monitoring-Framework Vermont

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 fuer Multi-Gigabit Netze implementiert. Das Ziel ist es, eine intelligente, selbstorganisierende Monitoringumgebung zu schaffen, die Analysen (z.B. Angriffserkennung) vereinfacht.



In diesem Zusammenhang wurde das Programm Vermont als Monitoringapplikation entwickelt, welche Daten in Datenströme, sogenannte Netflows, aggregiert und diese dann im IPFIX Format an weitere Module für anschließende Auswertung weiterleitet. Eine TCP/IP Verbindung wird dann anhand der IP-Headerdaten in zwei Datensätzen repräsentiert: Eine für den Hinweg, eine für den Rückweg. Möglichkeiten der Auswertung werden beispielsweise durch Detektionsalgorithmen für die Portscannererkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.

Aufgabenstellung:

Im Rahmen des Projekts wird eine verteilte Analyseumgebung für die Erkennung von Angriffen implementiert. Mehrere durch Vermont realisierte Sensorknoten sollen Daten von Netzwerken empfangen, diese filtern und möglichst effizient an nachgeschaltete Analyseknöten weiterleiten. Schwerpunkt dieser Arbeit ist es, Vermont so zu erweitern, dass eine hochperformante Filterung und Weiterleitung dieser Daten möglich wird. Dabei sollen komplette Netzwerkpakete inklusive Payload mit Hilfe des Protokolls PSAMP über das Netzwerk versendet werden, um danach von einer weiteren Instanz von Vermont auf den Analyseknöten empfangen, aufbereitet und einem nachgeschalteten IDS (wie z.B. Snort) übergeben zu werden.

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, IPFIX, Flows, Vermont, Snort

Ansprechpartner:

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

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