

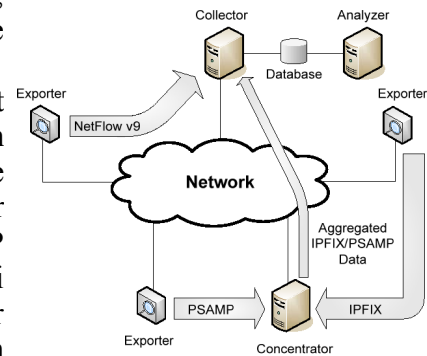
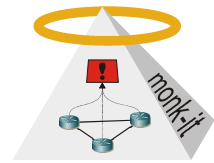
Studienarbeit

Entwicklung von Anomaliedetektionsalgorithmen für Netflowdaten

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 Portscanerkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.



Aufgabenstellung:

In der Studienarbeit sollen mehrere Auswertungsmodule für Netflowdaten implementiert werden. In einem ersten Schritt sollen Detektoren für horizontale (über mehrere Systeme) und vertikale (mehrere Ports auf einem System) Portscans, und verschiedene statistische Auswertungen entwickelt werden. Diese werden in einem zweiten Schritt auf Effektivität überprüft.

 **Korrelationsmanager** Top Quellnetze

Table: topntarget Condition: (de)

#	ZielIP	Zielhostname
0	131.188.12.138	ircneu.rrze.uni-erlangen.de
1	131.188.3.221	ntp1-rz.rrze.uni-erlangen.de

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, Portscan, 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

Dich interessiert zwar der Bereich Netzwerksicherheit, aber dieser Vorschlag entspricht nicht deiner Vorstellung? Schau einfach bei uns vorbei und wir können dann sicherlich gemeinsam ein geeignetes Thema finden!