

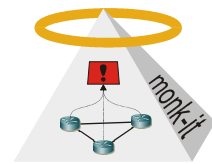


Diplomarbeit

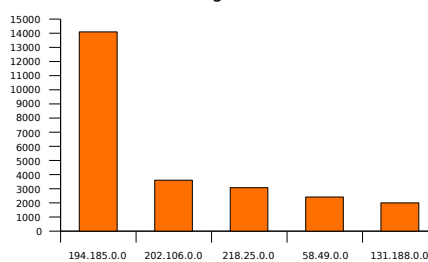
Entwicklung eines Korrelationswerkzeugs für sicherheitsrelevante Vorfälle mit zugehöriger Korrelationsengine

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. Durch bereits bestehende Überwachungssysteme wie beispielsweise Snort werden eine große Anzahl an Ereignissen in einem Netzwerk erkannt, welche allerdings oft Falschmeldungen ohne weitere Bedeutung darstellen. Um daraus relevante Sicherheitsvorfälle erkennen zu können, müssen mehrere Ereignisse durch vorbestimmte Regeln, so genannte Ereignisketten, in Verbindung gebracht werden. Dieser Vorgang wird als Ereigniskorrelation bezeichnet.



Anzahl erkannter Angriffe aus /16 Subnetzen



Aufgabenstellung:

In der Diplomarbeit soll eine Beschreibungsmöglichkeit für Ereignisse und Ereignisketten (z.B. mit XML) erarbeitet werden. Mit einer zu implementierenden Korrelationsengine sollen die gefundenen Ereignisketten in Echtzeit auf einkommende Ereignisse angewendet und auf Gültigkeit überprüft werden. Die gefundenen Informationen sollen zum einen visuell in das bereits bestehende webbasierte Verwaltungssystem für Sicherheitsvorfälle „PRISM“ integriert werden. Weiterhin soll die Engine aber auch unabhängig laufen und z.B. durch Email-Alarme auf Funde aufmerksam machen.



Table: topntarget Condition: (de)

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

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Angriffserkennung, Sicherheitsvorfall, Ereigniskorrelation

Ansprechpartner:

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

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

.....
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!