Check_Security

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Bruce Nikkel
Experte: Dr. Igor Metz

Das Icinga2 Security Monitoring für Linux-Systeme ist eine Plugin-Sammlung für das Monitoring Tool Icinga, bestehend aus insgesamt 23 verschiedenen Plugins aus den Themengebieten Webservermonitoring, System- und Benutzermonitoring, sowie Containerhost- und Netzwerkmonitoring. Der Schwerpunkt des Monitorings liegt in den Bereichen Best-Practice Konfigurationen und Log Auswertung.

Ausgangslage

Heutzutage kommen Linux Systeme vor allem im Serverumfeld vermehrt zum Einsatz. Insbesondere in den Bereichen Webhosting und Netzwerkinfrastruktur, sowie für Container-Systeme wird des Öfteren auf Linux gesetzt. Ebenso gehört im Serverumfeld das automatisierte Ausspionieren von Serversystemen, durch böswillige Akteure auf der Suche nach Sicherheitslücken, zur Tagesordnung. Diese Akteure agieren mit dem Ziel, sensitive Daten von infiltrierten Systemen zu stehlen, oder sogar die Systeme komplett zu übernehmen. Daher ist es im Serverumfeld unerlässlich, entsprechende Gegenmassnahmen anzuwenden.

Zielsetzung

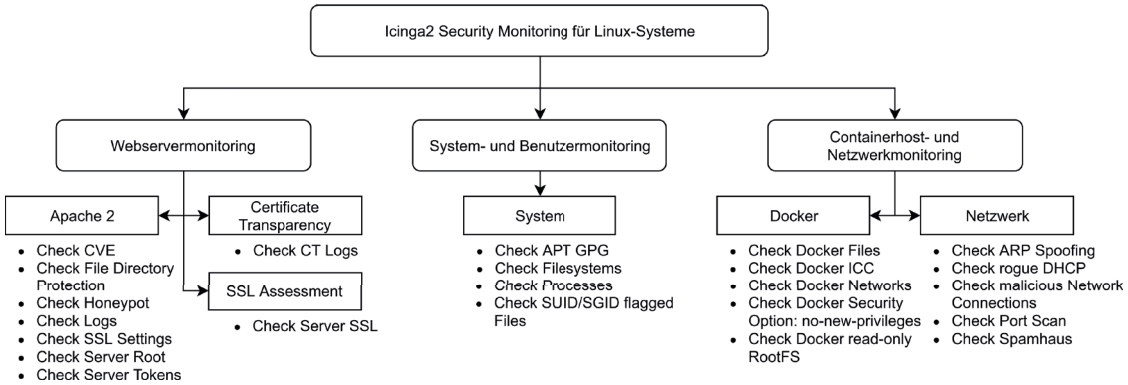
Ziel dieser Arbeit ist die Entwicklung einer solchen Gegenmassnahme in Form einer Echtzeit-Systemüberwachung für die Bereiche in denen Linux vermehrt zum Einsatz kommt. Das Monitoring baut auf dem open-source Überwachungstool Icinga2 auf und besteht aus einer Sammlung von eigenständigen Plugins für Icinga.

Ergebnis

Während drei Entwicklungsrunden sind insgesamt 23 Icinga / Nagios Plugins entstanden, die alle einzeln und unabhängig voneinander als Check in ein Monitoring integriert werden können. Zusätzlich wurden drei Klassen geschrieben die übergreifende Funktionalitäten für mehrere Checks zur Verfügung stellen. Alle Checks und Klassen wurden in Python 3 geschrieben und sind unter der WTFPL Lizenz frei Verfügbar. So wurde beispielsweise für das Webservermonitoring ein Check umgesetzt, welcher über die Qualys SSL Labs API ein SSL Assessment für Webserver durchführt. Es werden alle Webserver unter einer bestimmten Domain getestet und das erhaltene Ergebnis wird überwacht. So wird der Webserver immer nach aktuellen Kriterien bewertet und es ist ersichtlich, ob sich die Bewertung noch im angestrebten Rahmen befindet. Im Bereich Netzwerkinfrastruktur wurde ein Check zur Erkennung von Rogue DHCP Servern erstellt, welcher einen DHCP Discover Broadcast versendet und nach einer festgelegten Zeit prüft, ob nur Antworten von erwarteten DHCP Servern eingetroffen sind.

Raphael Gerber

Louis Justus Siegrist



Liste der umgesetzten Monitoring Checks