

CMDB based Policy Verifier

IT Security / Betreuer: Hansjürg Wenger
Experte: Andreas Dürsteler

Die Sicherheit in einem Netzwerk spielt zunehmend eine wichtigere Rolle. Eine Unachtsamkeit kann reichen und sensitive Daten gelangen aus einem Firmennetzwerk in falsche Hände. Die Höhe der Sicherheit legen heute die Firewalls und Servers mit ihren Konfigurationen fest. Doch sind diese genügend sicher konfiguriert? Mit dem CMDB based Policy Verifier wurde ein unabhängiges System entwickelt, welches die Sicherheit auf Basis einer CMDB und mit Hilfe von definierten Policies überprüft. Durchgeführt werden diese Überprüfungen mit dem bekannten Open Source Utility Nmap.

Ausgangslage

Mit der Entwicklung des Policy Verifiers soll ein System erstellt werden, welches die Einhaltung von Policies verifizieren kann. Dabei ist das Netzwerkumfeld in einer CMDB abgespeichert, und die Policies werden an Hand dieser Informationen erstellt. Im Rahmen einer Analyse wird festgelegt, wie die CMDB auszusehen hat und wie die Policies definiert werden. Der Policy Verifier soll in der Lage sein, die Überprüfungen automatisch oder manuell von mehreren Punkten in einem Netzwerk auszuführen und die Resultate entsprechend darzustellen.

Aufbau

Die CMDB enthält Informationen über die im Netzwerk vorhandenen Geräte sowie deren Dienste. Zusätzlich sind architekturbezogene Angaben wie Subnetze, VLANs und Zonenbezeichnungen

enthalten. Mit diesen Informationen werden die Policies definiert. Eine Policy gibt die erlaubten oder verbotenen Dienste zwischen einem Sender und einem Empfänger an. Technisch ausgedrückt regelt diese den Zugriff auf einen Scope. Dieser Scope kann eine einzelne IP-Adresse sein oder sogar aus mehreren Subnetzen bestehen. Weiter kann der Scope von einer oder mehreren Prüfsonden aus, sogenannte Proben, verifiziert werden. Mittels Rules werden die erlaubten oder verbotenen Dienste in der Policy hinterlegt. Das Open Source Utility Nmap ermöglicht schliesslich das Scannen dieser Dienste von den Proben und führt auf, ob diese vom Scope auch angeboten werden.

Testumgebung

Der entwickelte Policy Verifier wurde anschliessend in einer dafür aufgebauten Testumgebung ein-

gesetzt. Der Management-Server stellt dabei den eigentlichen Policy Verifier dar. Die Proben ermöglichen die Verifikation von mehreren Punkten im Netzwerk. In der Testumgebung wurden vier verschiedene Zonen mit jeweils einer Probe erstellt und durch eine Firewall getrennt. Auch der Management-Server kann als Probe eingesetzt werden. Die erlaubte Kommunikation konnte in Policies festgehalten und mit dem Policy Verifier auf dessen Einhaltung hin geprüft werden.

Policy Verifier

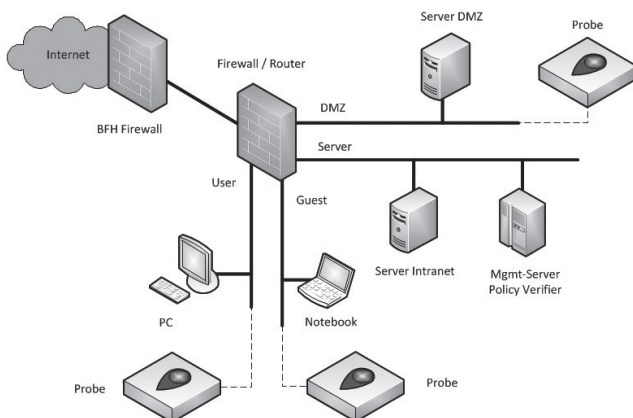
Neben der Überprüfung von Policies, ermöglicht der Policy Verifier auch die Durchführung eines Konsistenz-Checks zwischen der statischen CMDB und dem dynamischen Netzwerkumfeld. Ganze Netzwerkumgebungen und die dazugehörigen Policies können grafisch über eine Webseite erstellt und abgebildet werden. Änderungen in Konfigurationen, wie beispielsweise das Aufschalten oder Deaktivieren eines neuen Dienstes auf einem Server werden über den Policy Verifier automatisch oder auch durch manuell gestartete Scans sichtbar. In Reports können Details zu diesen Scans eingesehen werden. Zusätzlich bietet der Policy Verifier die Möglichkeit weitere Netzwerkutilities über diese Webseite zu nutzen.



Marco Gfeller



Giuliano Pescio



Testumgebung