Security Operation Center Lab

Diplomandin

Alexandra Diener

Problemstellung: Für das kommende Semester bietet die OST ein neues Cyber Defense Modul an. Da die meisten Unternehmen auf Microsoft Windows und Active Directory basieren, soll mit dieser Arbeit eine On-Demand Lernplattform für Studierende entwickelt werden, damit diese den Aufbau eines Security Operation Center (SOC) erlernen und praktisch anwenden können.

Ziel der Arbeit: Diese Arbeit soll ein Basis SOC Framework bereitstellen, welches im zukünftigen Cyber Defense Modul verwendet wird. Der Fokus ist hierbei ein SOC für Ausbildungszwecke bereit zu stellen, welches in ein virtuelles On-Demand Windows Active Directory eingebunden ist. Die Infrastruktur wird dabei über das Hacking-Lab der OST pro Student oder Studentengruppe in der Azure Cloud deployed. Sekundäres Ziel dieser Arbeit ist es, diverse Übungsszenarien zu konzipieren, welche die Studenten darin befähigen ein SOC einzurichten, zu nutzen und entsprechende Erfahrungen damit zu sammeln.

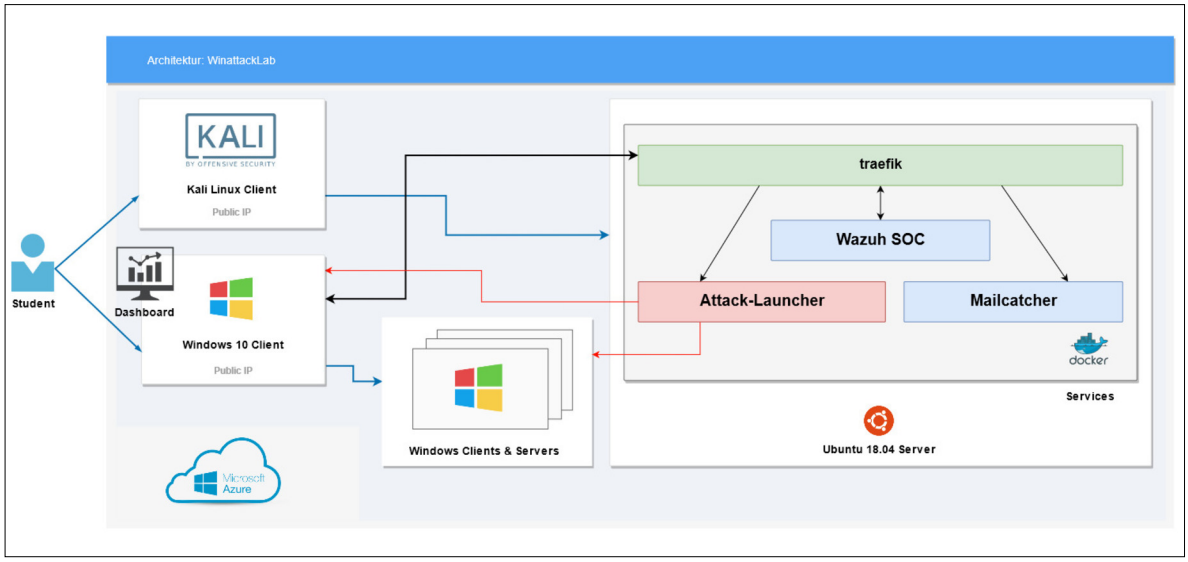
Ergebnis: Primäres Resultat dieser Arbeit ist die erfolgreiche Erweiterung des On-Demand Active Directory Netzwerkes um ein SOC und einem virtuellen Attack Launcher Service. Als SOC Lösung wurde die Open Source Software Wazuh evaluiert. Für die Simulation der Hacker Angriffe wurde auf Basis von Docker ein eigener «Attack-Launcher» Service entwickelt. Diesen nutzen die Studenten um vordefinierte Attacken auf die Infrastruktur zu lancieren und entsprechende Alerts im SOC auszulösen. Ausserdem kann das virtuelle SOC Framework mit ihren diversen Services pro Student oder Studentengruppe über das Hacking-Lab der OST in der Azure Cloud deployed werden.

Schlussendlich sind auch diverse Übungsszenarien entstanden, wie beispielsweise das Einrichten von Log Forwardern, die Verbesserung der Log Qualität mittels Active Directory, Group Policy und Verbesserung der Erkennungsrate mittels externen Indicators of Compromise (IOCs).

Open Source Security Operation Center Wazuh Logo
https://wazuh.com/uploads/2020/03/pageImage_home.png

Terraform und Microsoft Azure für das Deployment der Infrastruktur WinattackLab
https://hashicorp.github.io/workshops/

Architektur Übersicht vom WInattackLab
Mit draw.io erstellt, Firmen und Technologien Logos inkl.



Examinator
Ivan Bütler

Experte
Thomas Röthlisberger, Swisscom (Schweiz) AG, Wallisellen, ZH

Themengebiet
Networks, Security & Cloud Infrastructure