

24 Aufbau eines Ethical-Hacking-Labors mit Capture-the-Flag-Umgebung

Tuesday 5 November 2024 10:30 (1h 30m)

Zur Sicherstellung eines hohen Praxisbezugs der Lehre im Fachgebiet IT-Sicherheit wurde an der Hochschule Schmalkalden das IT-Sicherheitslabor um einen Ethical-Hacking-Teil erweitert. In diesem Labor befinden sich reale Softwaresysteme, an welchen Sicherheitsanalysen durchgeführt werden können. Diese Systeme werden in einer streng isolierten Umgebung betrieben, um einen Angriff auf Produktivsysteme aus dem Labor heraus zu verhindern.

Der Laborteil besteht aus Kali-Linux-Rechnern, welche zur Analyse von SUASploitable-Rechnern genutzt werden können. Bei letzteren handelt es sich um automatisch, zufällig generierte, verwundbare Softwaresysteme. Alle Rechner werden virtualisiert in der isolierten Umgebung betrieben. Die Studenten können direkt auf die Kali-Linux-Rechner zugreifen und sollen mittels diesen Sicherheitslücken in den SUASploitable-Rechnern auffinden und dokumentieren. Im Anschluss sollen gefundene Sicherheitslücken bewertet und behoben werden.

Die Studenten können in den SUASploitable-Maschinen Flags (vergleichbar mit Passwörtern) finden. Anhand dieser kann beim Laborsystem erfragt werden, ob eine Sicherheitslücke gefunden wurde und den Fund ggf. für sich reklamieren. Im Capture-the-Flag-System erhalten die Studenten einen Überblick über gefundene Flags und können so ihren Lernstand einsehen.

Insgesamt kann im Ethical-Hacking-Laborteil praxisnah erlernt werden, wie Softwaresysteme auf Sicherheitslücken überprüft werden. Die Isolation verhindert eine missbräuchliche Nutzung der Analysewerkzeuge. Das entwickelte System ist unter einer Open-Source-Lizenz verfügbar und kann so durch andere Institutionen mitgenutzt werden.

Primary author: TEFKE, Tobias (Hochschule Schmalkalden)

Co-author: Prof. STAUDEMEYER, Ralf C. (Hochschule Schmalkalden)

Presenter: TEFKE, Tobias (Hochschule Schmalkalden)

Session Classification: Showcases im Obergeschoss

Track Classification: Lernplattformen und digitale Tools