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

Tobias Tefke[1] **Ralf C. Staudemeyer**[1]

[1]Fakultät Informatik

Ausgangslage

- Neue Lehrveranstaltung: “Security Hacking” (seit Sommersemester 2023)
- Studenten lernen, Softwaresysteme auf Sicherheitslücken zu überprüfen
- Finden und Bewerten von potenziellen Schwachstellen
- Beheben von Schwachstellen (bevor Angreifer diese ausnutzen)
- hoher Praxisbezug durch realitätsnahe Simulation
- Anwendung von Analysewerkzeugen (nur innerhalb der Laborumgebung)
- Einsehen des Lernfortschritts durch den Studenten

Problemlösung

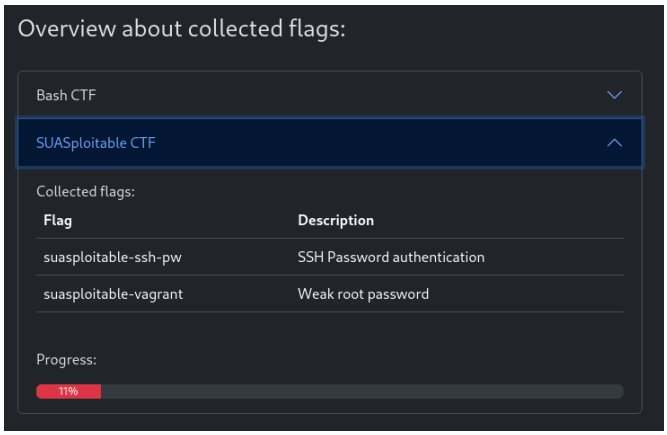
- vollständig isolierte Lernumgebung
- im Labor verfügbare virtualisierte Rechner:
  - Rechner mit “Hacking-Tools” zur Schwachstellenidentifikation
  - verwundbare Rechner mit bekannten Sicherheitslücken
- als virtuelle Maschinen (VM) verfügbar:
  - *Kali Linux*-VMs (“Hacker”-System zur Schwachstellensuche)
  - *SUASploitable*-VMs (div. stark verwundbare Softwaresysteme)
- Virtualisierung mit *QEMU* und *KVM*
- Übungsmaterialien verfügbar in den *Kali-Linux*-VMs
- Strikte Netzwerkisolation zwischen VMs und Rest des Labors:
  - jedes Netzwerk mit eigenen *Kali Linux* und *SUASploitable*-VMs
  - jeder Student arbeitet im eigenen, isolierten Netzwerk
  - VMs werden automatisiert repliziert und zurückgesetzt (immer frische VMs)
- Lernstandserhebung durch eine Capture-the-Flag (CtF)-Umgebung:
  - versteckte Zeichenketten im zu analysierenden System (sog. “Flags”)
  - Flags lassen sich nur unter Ausnutzung von Schwachstellen finden
  - gesammelte Flags können im System einlöst werden
  - eingelöste Flags werden zur Lernstandserhebung angezeigt
- weltweiter Zugriff möglich über bestehendes “SUASecLab” (Online-Labor)

Verwertbarkeit

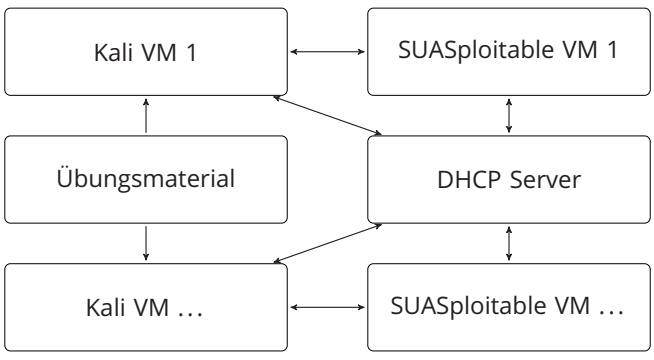
- Mitnutzung des Labors durch weitere Institutionen möglich
- Bereitstellung der Laborsoftware auf *GitHub*
- Entwicklung eigener Labore auf Basis unseres Systems

Hacking-Arbeitsumgebung

Fortschrittsanzeige



Struktur des Labornetzwerkes



SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

t.tefke@stud.fh-sm.de

r.staudemeyer@hs-sm.de

SUASecLab