SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

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

## Tag der Ingenieurwissenschaften 2024

Tobias Tefke[1] und Ralf C. Staudemeyer[2]

**Hochschule Schmalkalden**

[1] t.tefke@stud.fh-sm.de
[2] r.staudemeyer@hs-sm.de

# Ausgangslage

## ...ein kurzer Überblick über aktuelle Sicherheitsvorfälle


Von Cyberangriffen betroffene Institutionen[3]

[3] https://www.hs-kempten.de/hochschule/aktuelles/artikel/hacker-angriff-auf-die-hochschule-kempten-2598
https://www.ndr.de/nachrichten/hamburg/Hackerangriff-auf-HVV-Internetseite-und-App-waren-betroffen,hvv770.html
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Cyberangriff-auf-Landesbehoerden-in-MV-Internetseiten-lahmgelegt,kurzmeldungmv15456.html
https://www.zdf.de/nachrichten/politik/deutschland/cdu-cyberangriff-verfassungsschutz-100.html

# Ausgangslage

## ...ein kurzer Überblick über aktuelle Sicherheitsvorfälle


Von CVE indizierte Sicherheitslücken[4]

[4] https://twitter.com/CVEnew/

# Ausgangslage

## Notwendigkeit einer neuen Lehrveranstaltung

SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

- Neue Lehrveranstaltung “Security Hacking” (seit SoSe 2023)
- Studenten erlernen, Softwaresysteme auf Sicherheitslücken zu überprüfen
- Ziel: Auffinden und Dokumentation/Beheben von Sicherheitslücken
- Erweiterung unseres IT-Sicherheitslabors um:
  - Verwundbare Rechner mit Sicherheitslücken
  - Rechner mit Analyseprogrammen zur Identifikation der Lücken
- Missbräuchliche Nutzung des Labors muss ausgeschlossen werden!

# Problemlösung

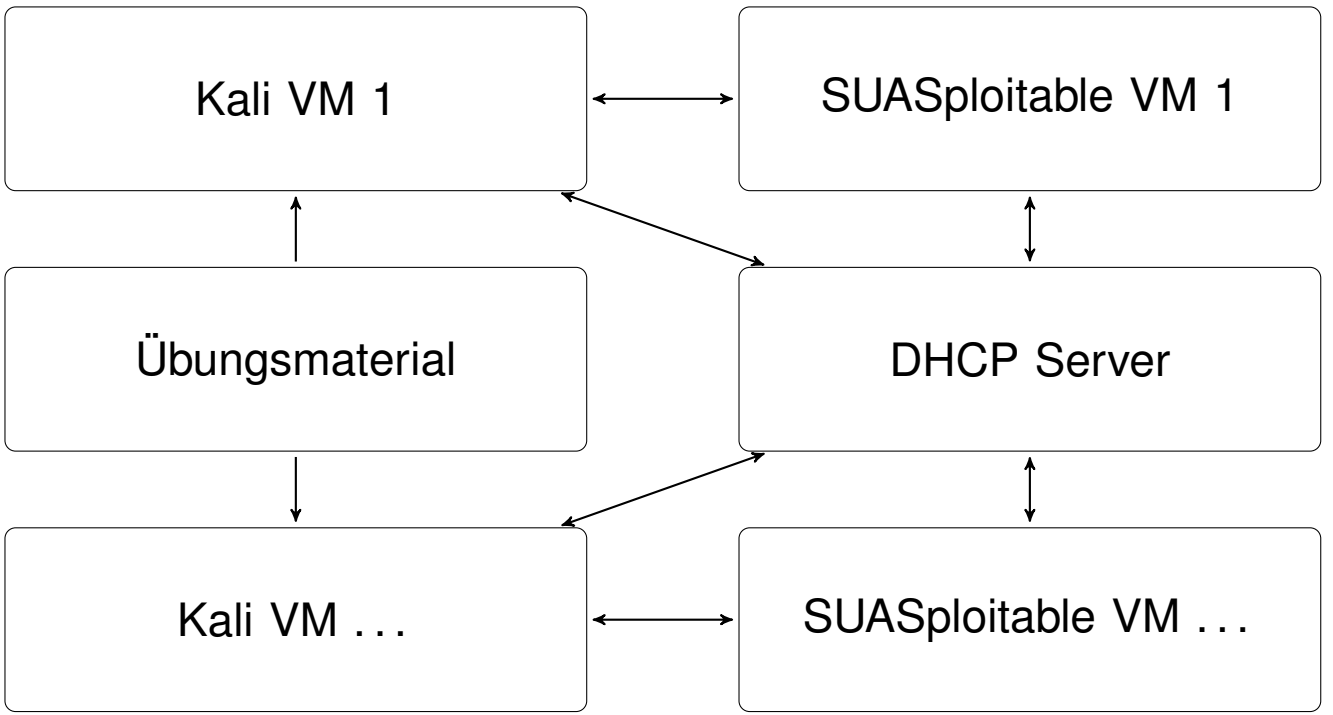
## Aufsetzen neuer virtueller Maschinen

SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

- Kali Linux:
  - Hacking-System zur Schwachstellenanalyse
  - Ermöglicht Identifikation und Ausnutzen von Sicherheitslücken
- SUASploitable:
  - Schwer verwundbares Softwaresystem
  - Enthält unsichere Konfigurationen weit verbreiteter Systeme
- Netzwerkisolation:
  - Jeweils eine Kali-Linux und eine SUASploitable-Maschine pro Netzwerk
  - Netzwerkisolation verhindert missbräuchliche Nutzung der Programme
- Regelmäßiges Zurücksetzen der virtuellen Maschinen

# Problemlösung

## Aufsetzen neuer virtueller Maschinen



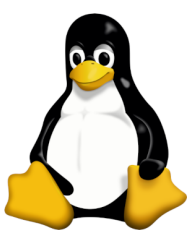

Struktur des Labornetzwerkes

# Problemlösung

## Aufsetzen neuer virtueller Maschinen

SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

- Zufällige Erzeugung von VMs (Cloud, CMs, allgemein)
- Zufällige Auswahl von Sicherheitslücken
- Hinterlegung von Flags in den VMs



docker

Seafile

Nextcloud

NGINX

MySQL

Drupal

php

APACHE HTTP SERVER PROJECT

MariaDB

WordPress

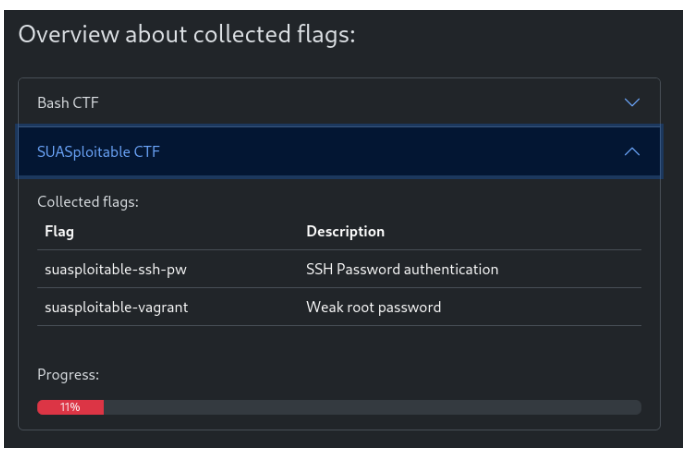
Überblick über in den VMs installierte Programme

# Problemlösung

## Capture-the-Flag-Umgebung

SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

- Jeder Nutzer enthält einen Laboraccount zum Zugriff auf die Laborumgebung
- Pro Sicherheitslücke ist in den VMs eine Flag (Zeichenkette) versteckt
  $\rightarrow$ zufällige Auswahl der Sicherheitslücken $\rightarrow$ zufällige Flags
- Mit Entdeckung der Flag kann Sicherheitslücke als gefunden vermerkt werden
- Laborsystem überprüft Flags und dokumentiert Lernfortschritt




Capture-the-Flag-Umgebung

# Problemlösung
## Arbeitsumgebung


Virtueller Laborarbeitsplatz über bestehendes Online-Labor

# Verwertbarkeit

## Weiternutzung der gefundenen Lösung

SCHMALKALDEN UNIVERSITY OF APPLIED SCIENCES

- Mitnutzung des Hacking-Bereichs durch weitere Institutionen möglich.
- Bereitstellung der Laborsoftware auf *GitHub*[5].
- Auf Basis des von uns entwickelten Labors können eigene Online-Labore aufgesetzt werden.
- Zur Umsetzung anderer Anwendungsfälle kann in den virtuellen Rechnern andere Software installiert werden.

[5] `https://github.com/SUASecLab`