Hacking Lab Challenges for „Linux Cyber Security“

Studiengang: BSc in Informatik
Betreuer: Prof. Dr. Benjamin Fehrensen

Mit der zunehmenden Verbreitung von IT-Systemen wird deren Absicherung immer wichtiger. Beinahe täglich liest man in Newsportalen, dass eine Firma gehackt wurde. Diese Hacks geschehen aus verschiedenen Gründen und das Ausmass ist von Fall zu Fall unterschiedlich. Um IT-Systeme zu schützen, müssen sich Informatiker*innen in die Rolle der Hacker versetzen. An diesem Punkt setzt die Bachelorthesis an.

Einleitung

Im Rahmen der Bachelorthesis wurden sogenannte «Hacking Challenges» erstellt. Dabei handelt es sich um Aufgaben, die von Studierenden gelöst werden müssen. Ziel ist es, eingebaute Schwachstellen in einem System auszunutzen – genau wie es Hacker tun. Der Fokus liegt auf den weit verbreiteten Linux-Systemen. Zum hosten der Challenges wurde die Hacking-Lab-Plattform von der Firma Compass Security genutzt.

Didaktik

Ziel der Arbeit ist es, Studierende zu schulen. Es ist sinnvoll, dies mit einer Lernmethode zu machen, welche möglichst effizient ist. Grob wird zwischen zwei verschiedenen Ansätzen unterschieden:

Passives Lernen (z.B Frontalunterricht)
Aktives Lernen (z.B durch «Hands on Experience»)

Das Lösen von Challenges ist dem aktiven Lernen zuzuordnen. Gemäss Studien ist diese Lernmethode effizienter als das traditionelle, passive Lernen. Neben der Effizienz steigt durch das direkte Engagement und das Erfolgserlebnis mit dem Abschliessen einer Challenge bei vielen Studierenden auch die Motivation, weitere Challenges zu meistern.

Challenges

Insgesamt wurden sieben Challenges erstellt. Diese sind alle sehr unterschiedlich. Bei der Auswahl der Challenges wurde darauf geachtet, dass die Studierenden ein möglichst breites Wissen gewinnen können. Folgende Sicherheitsaspekte werden in den Labs beleuchtet:

- Einsatz von veralteten Softwareversionen
- Fehlkonfigurationen
- Web-Security
- Übermässige Berechtigungen

Die Labs sind über Docker-Container zugänglich. Ziel aller Labs ist es, ein dynamisch generiertes «Flag» aufzuspüren, welches eingegeben werden kann, um die Challenge abzuschliessen.

Folgende Challenges wurden im Rahmen der Bachelorthesis erstellt.

SUID Lab Unauthorized File Read: Ziel dieser Challenge ist es, eine Datei zu lesen, auf welche man nicht berechtigt ist, weil sie sensible Informationen enthält.
SUID Lab Privilege Escalation: Bei dieser Challenge müssen sich die Studierenden Zugriff auf den root-Benutzer verschaffen. Dieser Benutzer besitzt die höchstmöglichen Berechtigungen auf dem System.
SSH Privilege Escalation: Diese Challenge besteht aus zwei Teilen. Zuerst müssen die Studierenden sich via SSH Zugriff auf das System verschaffen. Anschließend gilt es, durch eine Misskonfiguration Zugang zum root-Benutzer zu erlangen.
OpenSSL Heartbleed: Heartbleed ist ein sehr bekannter Bug, welcher die Netzwelt im Jahre 2014 erschüttert hat. In dieser Challenge ist dieser Bug eingebaut und er muss ausgenutzt werden, um an das Flag zu gelangen und dieses zu entschlüsseln.
Webserver RCE: Ein Bug im Apache Webserver ermöglichte eine Remote Code Execution, durch die unberechtigte Benutzer grossen Schaden verursachen können. Dieser Bug muss ausgenutzt werden.
Sneaky XSS: Bei einem XSS-Angriff können bösartige Scripts in den Code einer Webseite eingeschleust werden.
Psychic Signature: Im Java-Code gab es einen Implementationsfehler bei der Prüfung der Signatur, wodurch fälschlicherweise eine leere Signatur erfolgreich validiert wurde. Ziel der Challenge ist es, sich mit FIDO2 als Benutzer anzumelden, ohne dessen privaten Schlüssel zu kennen.

Séverin Jan Dufaux
Distributed Systems and IoT

Mark Flury
Distributed Systems and IoT