

Forschungsseminar Informatik / Advanced Practical IT Security

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw-mannheim.de, Raum 149B
Version: 22SEA (2. Semester)
Modul: *W3WI_SE411*
Unterlagen: Moodle

Teaser

In dieser Veranstaltung werden wir uns mit den Grundlagen praktischer Angriffe und Verteidigungsmaßnahmen im Bereich IT Security auseinandersetzen. Wir werden uns der Frage widmen wie, wann und in welcher Form man - auf den ersten Blick abgesicherte Systeme - einerseits angreifen (🚩 *to exploit*) kann und wie man die Sicherheit weiter erhöhen kann.

Wir werden uns in diesem und dem nächsten Semester ausgewählten Themen widmen, die von der Sicherheit von Passwörtern und Angriffen auf selbige bis hin zu der Sicherheit von Netzwerken und Webanwendungen reichen. Wir werden uns dabei insbesondere an gängigen Angriffsszenarien orientieren.

Wir werden uns somit auf praktische Aspekte der IT Sicherheit fokussieren. Das Kennenlernen der theoretischen Grundlagen von Verschlüsselungsalgorithmen, Hashalgorithmen, Zertifikaten und Vergleichbarem ist nicht primärer Fokus dieser Veranstaltung.

Hinweis

Für diese Veranstaltung sind Grundkenntnisse in Linux hilfreich aber nicht notwendig. Notwendig ist aber Interesse an tiefergehenden technischen Details.

Grober Ablauf

- 1. Semester: 6 Termine; (50% der Note)
- 2. Semester 5 Termine; (50% der Note)

Genereller Ablauf


1. Einführung in ein für die IT-Sicherheit relevantes Thema in Hinblick auf praktische Anwendung
2. Aufgaben, die jeder für sich lösen muss/soll
3. Abgabe, die genau beschreibt wie Sie die Aufgabe gelöst haben. Darüber sammeln Sie Teilnoten, die am Ende verrechnet werden. D. h. es gibt Teilnoten pro Aufgabe. Die Punkte sind zwischen den Aufgaben nicht untereinander vergleichbar.
4. Jeder muss präsentieren.

Inhalte

Hinweis

Diese Veranstaltung ist ergänzend zur Veranstaltung SE III IT-Sicherheit zu sehen. D. h. Inhalte die dort vermittelt werden, werden hier nicht noch einmal behandelt, sind aber potentiell relevant.

1. Semester

1. Passwortwiederherstellung ( *Password Recovery*)
2. Reverse Engineering 101

2. Semester

Pentesting von Webanwendungen

Was passiert wann im 1. Semester..

26. Aug 2024:

Einführung & Passwortwiederherstellung (Teil 1)

(Ggf. Linux Shell und Reguläre Ausdrücke.)

9. Sep 2024:

Passwortwiederherstellung (Teil 2)

Ausgabe der Übung - Notenanteil: 15%

23. Sep 2024:

Einführung in Reverse Engineering (und Netzwerkanalyse)

Ausgabe der Übung - Notenanteil: 20%

7. Oct 2024:

Online (*Optional* - Unterstützung bei der Bearbeitung der Aufgaben)

BBB: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>

21. Oct 2024:

Online (*Optional* - Unterstützung bei der Bearbeitung der Aufgaben)

BBB: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>

28. Okt. 2024:

Abgabe der Lösungen für alle Aufgaben als PDF Dokument (Moodle)

(Ich werde am 29. zuteilen wer welchen Teil präsentiert; bitte schauen Sie in Moodle. Sollten Sie am 30. Okt. bis 22:00 Uhr weder eine Nachricht in Moodle noch eine E-Mail von mir erhalten haben, dann melden Sie sich bitte umgehend bei mir.)

4. Nov 2024:

Abschlusspräsentationen

Die Präsentationsdauer ist am Inhalt zu orientieren; darf max. 30 min pro Person jedoch nicht überschreiten. Jeder soll in der Lage sein alle Schritte nachvollziehen zu können. D. h. die Präsentation kann auch eine „Live-Demo“ sein, die zeigt wie die Aufgabe gelöst wurde.

Die Präsentation ist bis zum 3. Nov. 2024 23:59 Uhr in Moodle hochzuladen. Sollten Sie eine Live-Demo machen, dann zeichnen Sie Ihren Probelauf auf und laden Sie diesen als Zip-Datei hoch. Alternativ können Sie Ihre Video auch in Youtube stellen oder per OneDrive, Dropbox, ... zur Verfügung stellen. In diesem Falle laden Sie eine Textdatei mit der URL zum Video hoch! Nutzen Sie nicht Moodle für die Videos, da diese häufig Probleme bereitet!

Erste Tips zur Gestaltung von Vorträgen finden Sie hier.

Notenanteil: 15%

Was passiert wann im 2. Semester..

19. Feb 2025

- Ausgabe der Themen zur Bearbeitung
- Kurze Einführung in das Thema Pentesting.

24. Feb 2025

Bearbeitung der Themen mit dem Ziel „Hands-on“; bei Bedarf stehe ich für Rückfragen *online* zur Verfügung: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>.

12. Mar 2025

- Halten der Präsentationen - Notenanteil: 20%
- Vergabe der Aufgabe für das Pentesting

Achtung!

Die Vorträge müssen am Abend vorher hochgeladen sein.

31. Mar 2025

Durchführung des Pentesting; bei Bedarf stehe ich für Rückfragen *online* zur Verfügung: <https://bbb.dhbw.de/mannheim/eic-mn5-hvh-7qd>.

23. Apr 2025

Vorstellung der mittels Pentesting gefundenen Lücken - Notenanteil: 20%

Achtung!

Die Vorträge müssen am Abend vorher hochgeladen sein.

Ende des Semesters

Abgabe der Dokumentation der Ergebnisse des Pentesting inkl. Bewertung als PDF Dokument (Moodle) - Notenanteil: 10%

Vortragsthemen

- **Nmap (und ncat)** (1 Person)
(Network discovery and security auditing.)
- **Zed Attack Proxy (ZAP)** (1 Person)
(Web App Scanner)
- **Burp Suite inkl. Dastardly** (1 Person)
(Penetration testing toolkit.)
- **Metasploit** (2 Personen)
(Penetration testing framework.)

Dauer pro Person: 25 Minuten

Bewertungskriterien

Für die Präsentationen

- Vermittelt die Präsentation einen guten ersten Einblick in das Tool (Fähigkeiten und Grenzen)
- Qualität der (Live-)Demonstration (und ggf. des Backups)
(ggf. ist das Aufsetzen einer (kleinen) virtuellen Maschine sinnvoll/notwendig.)
- Reduktion auf das Wesentliche
- Qualität der Beantwortung von Fragen
- Persönliches Auftreten
- Einhaltung der Dauer der Präsentation

für das Pentesting

- Anzahl der gefundenen Schwachstellen
- Qualität der Präsentation der Schwachstellen
- Beantwortung von Fragen

für die Dokumentation

- Qualität der Dokumentation (leserlich, strukturiert, frei von Tippfehlern, ...)
- Ist die Einschätzung der Lücken nachvollziehbar