Vorlesungsbeschreibung Wahlpflicht: Penetration Testing

Lernergebnisse

Bei Abschluss des Lernprozesses werden die Studierenden in der Lage sein, einen Penetrationstest mithilfe gängiger Hacking Tools nach Best-Practice-Vorgehensweise durchzuführen und zu dokumentieren. Gleichermaßen soll ein Verständnis dafür geschaffen werden, wie Ergebnisse eines Penetrationstests zu bewerten sind und welche Handlungsempfehlungen daraus resultieren.
Die Studierenden entwickeln eine ausgeprägte Problemlösungs- und Beurteilungskompetenz

Inhalte

Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themenbereichen vermittelt:

- Kenntnisse über potenzielle Cyber-Risiken
- Angreifertypen: Von Script Kiddies bis Advanced Persistant Threats
- Vorstellung von Standards und Best-Practice-Ansätzen zur Durchführung von Penetrationstests
- Rechtliche Rahmenbedingungen
- Testverfahren und Aggressivität
- Vorstellung gängiger Hacking Tools (Nmap, OWASP Zed, Metasploit, Nessus u. a.)
- Live-Hacking
- Durchführung eines Penetrationstests
- Fundierte Einschätzung der Ergebnisse
- Dokumentation und Handlungsempfehlungen
- Advanced Cyber Defense

Lehrmethoden

Vorlesung, Übungen in Kleingruppen.

Lehrsprache

Deutsch

Studien-/Prüfungsleistung

Hausarbeit oder Referat/Präsentation bzw. mündliche Prüfung; die genaue Prüfungsform wird zu Beginn des Semesters bekannt gegeben.

Credits

3
(90 h = 30 h Präsenz- und 60 h Eigenstudium, inkl. Prüfungsvorbereitung und Prüfung)

Literatur

- Kevin R. Fall, W. Richard Stevens 2011: TCP/IP Illustrated Volume 1: The Protocols (978-0321336316)
- Jon Erickson 2008: Hacking - Die Kunst des Exploits (978-3- 89864-536-2)
- Andrew S. Tannenbaum, David J. Wetherall 2012: Computernetzwerke (978-3-86894-137-1)
- Holger Reibold 2015: Hacking Kompakt - Die Kunst des Penetration Testing (978-3-95444-161-7)
- Michael Messner 2015: Hacking mit Metasploit – Das umfassende Handbuch zu Penetration Testing und Metasploit (978-3-86490-224-6)