

Kennziffer: INFO-4129	Modultitel Pentesting Pentesting		Lehrform(en) Vorlesung						
ECTS-Punkte	3								
Arbeitsaufwand -Kontaktzeit -Selbststudium	Arbeitsaufwand 90 h	Kontaktzeit 30 h / 2 SWS	Selbststudium 60 h						
Veranstaltungsdauer	ein Semester								
Häufigkeit des Angebots	unregelmäßig, Blockveranstaltung in der vorlesungsfreien Zeit								
Unterrichtssprache	Deutsch								
Prüfungsform	Klausur (bei kleiner Teilnehmerzahl mündliche Prüfung)								
Inhalt	<p>Um Netzwerke oder Applikationen abzusichern, benötigt ein Administrator oder Entwickler Kenntnisse über vorhandene Schwachstellen. Durch simulierte Hacker-Angriffe, sogenannten Penetrationstests, lassen sich diese effizient aufdecken. Neben theoretischen Grundlagen über die Planung und Durchführung von Penetrationstests vermittelt diese Vorlesung tiefgehende praktische Kenntnisse moderner Angriffswerkzeuge, aktueller Schwachstellen und der Methodik, diese auszunutzen. Das Spektrum reicht dabei vom Footprinting"über den eigentlichen Angriff bis zum Platzieren von Hintertüren in ein kompromittiertes System. Neben dem Einsatz fertiger"Werkzeuge wie Nmap oder Metasploit kommt auch der Entwicklung eigener Exploits mit dem Debugger eine große Bedeutung zu. Vorlesung und Übungen finden als eng miteinander verzahnte Blockveranstaltung statt.</p> <p>Themen sind: Gestaltungsmöglichkeiten, Testmodule, Abschätzung des Testaufwands, Bewertung von Ergebnissen und Dokumentation, Nachverfolgung von Schwachstellen, ethische und Rechtliche Aspekte, Penetration Testing Standards, Footprinting, Portscanning, Enumeration, Sniffing, Angriffe gegen Verschlüsselung, häufige konfigurative Schwachstellen, Schwachstellen in Webapplikationen, Umgang mit Metasploit, Angriffe gegen Windows-Netzwerke, Privilege Escalation, Backdoors, online- und offline-Angriffe gegen Passwörter, Schwachstellenanalyse, Pentesting von WLAN-Netzen, Ausnutzung von Buffer-Overflow-Schwachstellen</p> <p>Die Veranstaltung wird von Herrn Schreiber (SysS GmbH) und seinem Team durchgeführt.</p>								
Qualifikationsziele	Die Studierenden haben ein umfangreiches Verständnis über das Prinzip und die Organisation von Penetration Tests. Sie können wichtige Begriffe des Fachgebiets richtig anwenden.								
Vergabe von Leistungspunkten / Benotung		Lehrform	Status	SWS	LP	Prüfungsform	Prüfungsdauer	Benotung	Berechnung Modulnote (%)
	Vorlesung	V	o	2	3	K	60	b	100

(noch INFO-4129)

Teilnahmevoraussetzungen	INF4341 Vorlesung Kommunikationsnetze
Dozent	Menth
Literatur	<i>keine</i>