Friedrich-Alexander-Universität
Technische Fakultät

Modulbeschreibung:

Netzwerkforensik

Modulbezeichnung:	Netzwerkforensik
Zertifikatsabschluss:	Hochschulzertifikat
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Modulverantwortliche(r):	Prof. Dr. Jessica Steinberger
Dozent(in):	Prof. Dr. Jessica Steinberger
Zeitraum:	Nächster Angebotszeitraum: Wintersemester 2026/2027 Dauer ca. 6 Monate
Leistungspunkte:	5 ECTS-Punkte
Zielgruppe:	Forensische Ermittler und Sicherheitsanalysten, Berufspraktiker/-innen mit und ohne Abitur, die sich in den spezifischen Fachbereichen auf akademischem Niveau passgenau im Bereich Cyber-Sicherheit weiterbilden möchten.
Studien- und Prüfungsleistungen:	Hausarbeit: Forensische Untersuchung von Netzwerkdatenverkehren eines Angriffs, Verfassen eines Projektberichts
Notwendige Voraussetzungen:	Grundlegende Programmierkenntnisse in einer Programmiersprache, Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII, Zweierkomplementdarstellung),
Empfohlene Voraussetzungen:	Grundkenntnisse in Betriebssystemen und Netzwerken
Sprache:	Deutsch
Arbeitsaufwand bzw. Gesamtworkload:	Wie viel Arbeitszeit (Workload) ist für das Modul insgesamt vorgesehen?

Präsenzstudium	15	Zeitstunden
Fernstudienanteil:	135	Zeitstunden
davon Selbststudium:	90	Zeitstunden
davon Aufgaben und Hausarbeit:	30	Zeitstunden
davon Online-Betreuung:	15	Zeitstunden
Summe:	**150**	**Zeitstunden**

30 h = 1 Leistungspunkt nach ECTS

Lerninhalte	In diesem Modul werden die folgenden Themengebiete behandelt: • Vorgehensmodell des "Network Security Monitoring" • Hashfunktionen in der Forensik • Grundlagen der Netzwerkprotokolle und deren Angriffsvektoren • Arten von Netzwerkangriffen und deren Auswirkungen im Netzwerkdatenverkehr • Einblicke in die Datengewinnung aus verschiedenen Netzwerkkomponenten • IT-forensische Analyse von Netzwerkdatenverkehr • Umgang mit Werkzeugen der Netzwerkforensik • Visualisierung von Netzwerkdaten • Erstellung forensischer Gutachten Hausarbeit**:** • Im Rahmen der Hausarbeit soll ein Netzwerkmitschnitt analysiert werden. Dabei kommen die im Modul gelehrten Techniken und Analysemethoden zur Anwendung. Die durchgeführte Analyse soll in einem möglichst vollständigen forensischen Gutachten zusammengefasst werden.
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der Netzwerkprotokolle und die verschiedenen Datenquellen, welche der IT-forensischen Analyse als Grundlage dienen können. Hierauf aufbauend lernen die Studierenden mögliche Auswirkungen von Netzwerkangriffen unter Nutzung einzelner Netzwerkprotokolle kennen und bewerten. Die Studierenden sind in der Lage die Datengewinnung aus verschiedenen Netzwerkkomponenten vorzunehmen und können sicher mit den Werkzeugen der Netzwerkforensik umgehen. Die Studierenden lernen verschiedene Methoden kennen, um netzbasierte Daten zu visualisieren. Weiterhin sind die Studierenden in der Lage eine forensische Analyse von Netzwerkdaten durchzuführen und können das Ergebnis gerichtsverwertbar dokumentieren. *Methodenkompetenz:* Die Studierenden kennen die Grundlagen und benötigten Werkzeuge für die Durchführung einer netzwerkforensischen Analyse. Sie wissen welche Datenquellen bei einer forensischen Analyse verwendet werden und wie die Netzwerkdaten gesammelt werden können. Mit diesem Wissen sind sie in der Lage aktiv umzugehen und können im Bedarfsfall ein Gutachten, welches dem Prinzip eines forensischen Vorgehensmodell folgt, selbstständig ausarbeiten. Zusätzliche Informationen können sie selbstständig aus der Literatur erarbeiten. Sie können mit dem durch das Modul erlangten Wissen sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden tauschen sich durch Gruppenarbeit in den Präsenzveranstaltungen aus und können auftretende Probleme, Fragen und Aufgaben durch fachgebundene Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit netzwerkforensische Analysen anhand des Prinzips eines forensischen Vorgehensmodells durchzuführen und sind in der Lage die Ergebnisse gerichtsverwertbar zu verschriftlichen und zu präsentieren. Des Weiteren besitzen sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf Neuerungen in dem Themengebiet reagieren.
Lehrveranstaltungen und Lehrformen:	Präsenzveranstaltung: Vorlesung, Übungen: Analyse verschiedener Netzwerkdatenmitschnitte, Vorbereitung auf die Hausarbeit

	Onlineveranstaltung: flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übungen
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literatur:	Als weiterführende Literatur wird empfohlen: • Messier, Ric: Network Forensics. New York: John Wiley \& Sons, 2017. ISBN 978-1-119-32828-5. • Forshaw, James: Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation. München: No Starch Press, 2018. -ISBN 978-1-593-27844-1. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.