



DIGITALE SPUREN SICHERN

EINFÜHRUNG IN DIE NETZWERKFORENSIK

Die Herausforderung: Straftaten im Internet und digitale Angriffe nehmen ständig zu und stellen eine ernstzunehmende Bedrohung dar. Ziele sind hierbei sowohl Behörden als auch Unternehmen und Privatpersonen. Um solche Straftaten aufzuklären bzw. Angriffe aufzuarbeiten, gilt es, die entstandenen digitalen Spuren zu finden, zu sichern und entsprechend auszuwerten. Eine der wichtigsten Quellen für digitale Spuren sind Netzwerkmitschnitte von IT-Systemen. Die Analyse dieser Daten erfordert einerseits ein fundiertes Wissen der dort verwendeten Technologien und Konzepte, wie beispielsweise der Netzwerkprotokolle, und andererseits einen sicheren Umgang mit entsprechenden forensischen Werkzeugen.

Inhalte des Seminars

Kompakte Wiederholung von relevanten Netzwerkprotokollen

Mitschneiden von Datenverkehr in drahtgebundenen und drahtlosen Netzen

Analyse von Datenverkehr

Umgang mit Wireshark

Entwicklung eigener Protokollparser

Grundlagen zu Intrusion-Detection-Systemen (IDS)

Herausforderungen der Netzwerkforensik

Praktische Aufgaben zur Netzwerkforensik

Ihr Nutzen

- » Sie können Netzwerkmitschnitte und -protokolle analysieren sowie dort vorhandene digitale Spuren extrahieren und auswerten.
- » Sie können die wichtigsten Werkzeuge im Bereich der Netzwerkforensik verwenden und verstehen.
- » Sie können einfache Aufgaben der Netzwerkforensik automatisieren und erlangen ein Verständnis für die Anwendungsfälle und das Vorgehen im Bereich der Netzwerkforensik.

INFORMATIONEN IM ÜBERBLICK

Einfache Kenntnisse von Netzwerkgrundlagen (TCP, UDP, IP, DNS etc.), Erfahrung mit Linux ist von Vorteil, aber nicht zwingend notwendig

Incident Responder, Security-Analysten*innen, IT-Admins, angehende IT-Forensiker*innen, Polizisten*innen

2 Tage Präsenz

1200,-

Bonn

Veranstaltet durch

Fraunhofer
FKIE

Referenten:

Martin Lambertz,
IT-Sicherheitsforscher,
Fraunhofer FKIE

Jan-Niclas Hilgert,
IT-Sicherheitsforscher,
Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/einfuehrung-netzwerkforensik