

Linux Forensik mit Kali Linux

Trainings-ID: LIFK

[Zum Seminar →](#)

Das nehmen Sie mit

Unternehmen schützen ihre IT-Systeme mit umfangreichen Sicherheitsmaßnahmen. Trotzdem geschieht es immer wieder, dass Hacker oder Mitarbeiter erfolgreich einbrechen und Schaden anrichten. Darum ist es wichtig dass jede*r Administrator*inn forensische Analysen auf seinen Computer Systemen durchführen kann. Solche Analysen sind nicht nur für die Strafverfolgung interessant, sondern auch eine wichtige Tätigkeit, die Pentester, Security Spezialisten und Linux Troubleshooter durchführen müssen um feststellen zu können ob Systeme manipuliert wurden.

In dieser Schulung erlernen Sie die Grundlagen der Linux Computer Forensik und erhalten einen Einblick in die zahlreichen kostenlosen Forensik Werkzeuge. Die durchgeführten Analysen vertiefen darüber hinaus das Verständnis über die Linux Architektur. Dieser Kurs ist somit jedem fortgeschritten SUSE, Red Hat, und Debian Admin hilfreich.

Nach Abschluss dieses Seminars haben die Teilnehmer*innen Wissen zu folgenden Themen:

- Grundlagen der Computer Forensik
- Open Source Forensik Werkzeuge
- Standard Linux Werkzeuge für Forensiker
- Hard Disk
- Dateisystem Layout
- Forensische Daten Dumps mit dd, dcfldd und dc3dd erstellen
- Wiederherstellen von gelöschten Dateien
- MAC Time Analysen
- Sleuth Kit
- Forensische Dateisystem Analyse mit Sleuth Kit (ext2/3/4 und NTFS Dateisysteme)

- Memory Dump
- Volatility Framework
- Auswerten eines Linux Memory Dumps

Das nehmen Sie mit

Unternehmen schützen ihre IT-Systeme mit umfangreichen Sicherheitsmaßnahmen. Trotzdem geschieht es immer wieder, dass Hacker oder Mitarbeiter erfolgreich einbrechen und Schaden anrichten. Darum ist es wichtig dass jede*r Administrator*inn forensische Analysen auf seinen Computer Systemen durchführen kann. Solche Analysen sind nicht nur für die Strafverfolgung interessant, sondern auch eine wichtige Tätigkeit, die Pentester, Security Spezialisten und Linux Troubleshooter durchführen müssen um feststellen zu können ob Systeme manipuliert wurden.

In dieser Schulung erlernen Sie die Grundlagen der Linux Computer Forensik und erhalten einen Einblick in die zahlreichen kostenlosen Forensik Werkzeuge. Die durchgeführten Analysen vertiefen darüber hinaus das Verständnis über die Linux Architektur. Dieser Kurs ist somit jedem fortgeschritten SUSE, Red Hat, und Debian Admin hilfreich.

Nach Abschluss dieses Seminars haben die Teilnehmer*innen Wissen zu folgenden Themen:

- Grundlagen der Computer Forensik
- Open Source Forensik Werkzeuge
- Standard Linux Werkzeuge für Forensiker
- Hard Disk
- Dateisystem Layout
- Forensische Daten Dumps mit dd, dcfldd und dc3dd erstellen
- Wiederherstellen von gelöschten Dateien
- MAC Time Analysen
- Sleuth Kit
- Forensische Dateisystem Analyse mit Sleuth Kit (ext2/3/4 und NTFS Dateisysteme)
- Memory Dump
- Volatility Framework

- Auswerten eines Linux Memory Dumps

Zielgruppen

Linux Administrator*innen

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
11.12.2024-13.12.2024	3 Tage	Wiener Neustadt	Trainingspreis (Vor Ort)	€ 1.935,-
11.12.2024-13.12.2024	3 Tage	Wiener Neustadt	Trainingspreis (Online)	€ 1.935,-
13.01.2025-15.01.2025	3 Tage	Wiener Neustadt	Trainingspreis (Vor Ort)	€ 1.838,-
13.01.2025-15.01.2025	3 Tage	Wiener Neustadt	Trainingspreis (Online)	€ 1.838,-