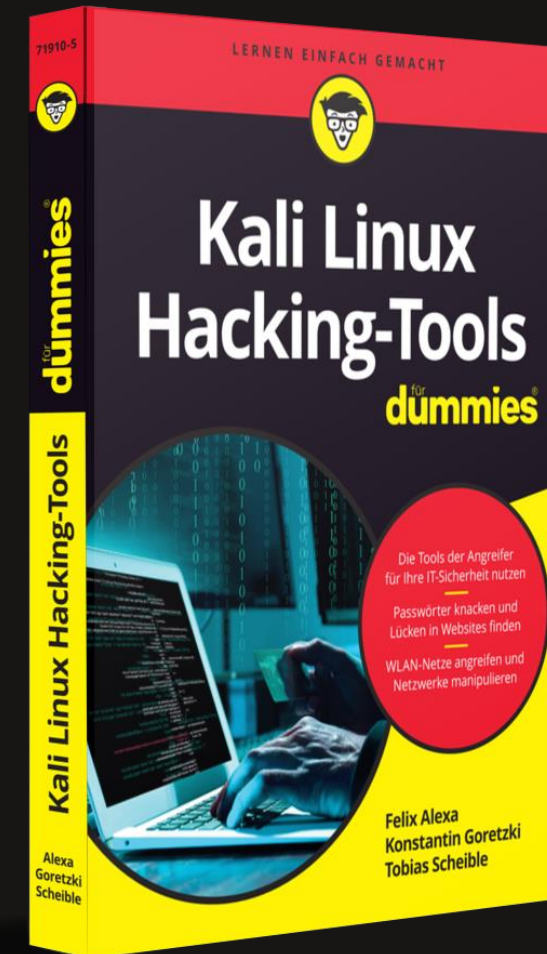


Offensive IT-Sicherheit – Kali Linux

VDI Zollern-Baar 07. Juni 2023

Über uns

- **Felix Alexa**
 - Kali Linux – System einrichten und kennenlernen
 - Sniffing und Spoofing – Netzwerke unterwandern
- **Konstantin Goretzki**
 - Web Application Analysis – Websites untersuchen
 - Wireless Attacks – WLANs angreifen / Sicherheit testen
- **Tobias Scheible**
 - Information Gathering – verdeckte Informationen sammeln
 - Password Attacks – Passwörter knacken
 - Forensics – IT-Forensik-Analysen



Agenda

- 01. Offensive IT-Sicherheit mit Kali Linux
- 02. Kali Linux Hacking-Tools
- 03. Erweiterte Einsatzgebiete

01. Offensive IT-Sicherheit mit Kali Linux

Offensive IT-Sicherheit

Offensive IT-Sicherheit

- Nicht nur passive Schutzmaßnahmen umsetzen
- Perspektivwechsel - Sicht des Angreifers
- Proaktiver und angreifender Ansatz
- Gleiche Tools und Vorgehensweisen wie Angreifer
- Computersysteme, Netzwerke und Menschen

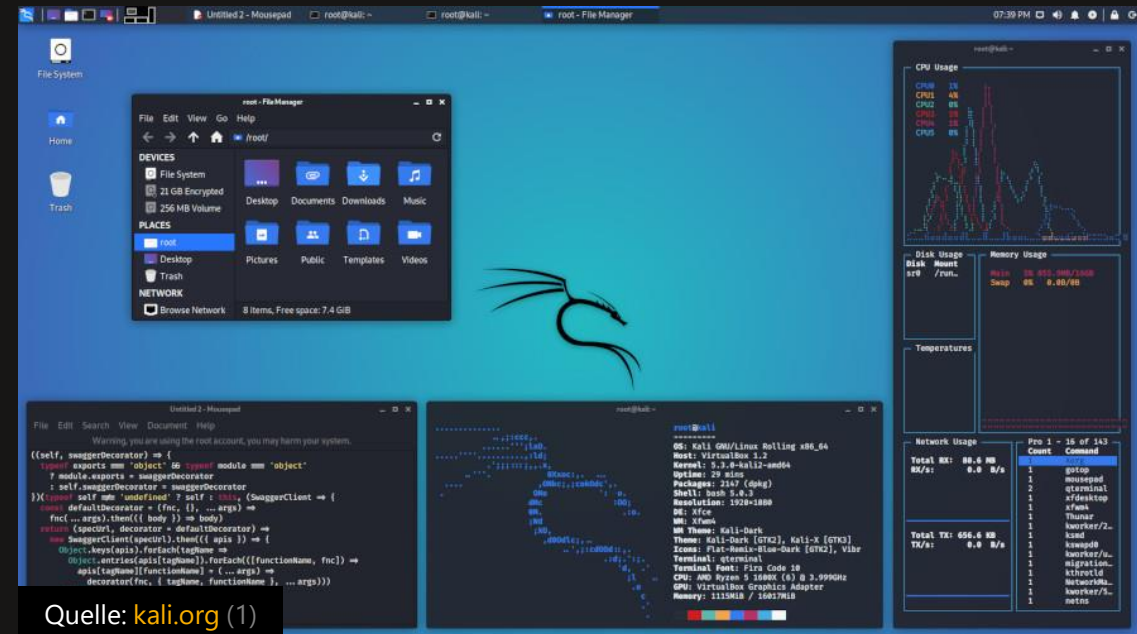
Penetrationstest (Pentest)

- Planung / Planning
- Aufklärung / Reconnaissance
- Schwachstellenausnutzung / Exploitation
- Rechteauserweiterung / Privilege Escalation
- Dokumentation / Documentation

Kali Linux

Betriebssystem

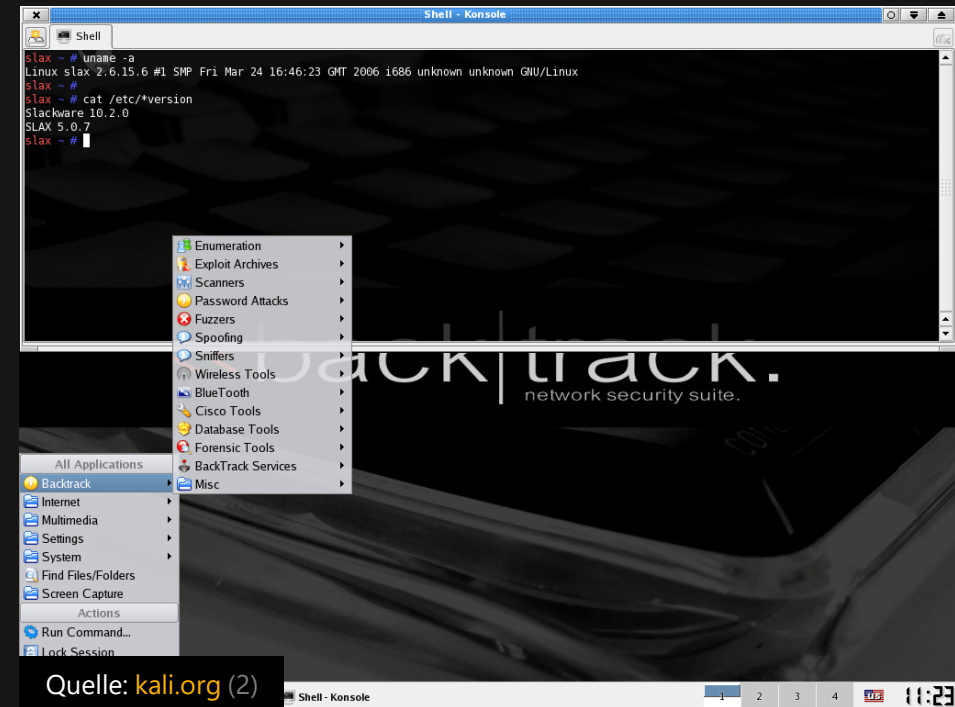
- Fokus auf Penetrationstests & IT-Forensik
- Enthält zahlreiche Sicherheitstools
- Beliebt in der Cyber Security Community
- Aktive Community und regelmäßige Updates
- Ermöglicht umfassende Sicherheitsprüfungen



Kali Linux

Entstehung

- 2004 Whoppix (White-Hat and knOPPIX)
- 2005 Whax livesecurity ressourcen (Slax)
- 2005 Auditor Security Collection (Knoppix)
- 2006 BackTrack (Slax > Ubuntu)
- 2013 Kali Linux (Debian)

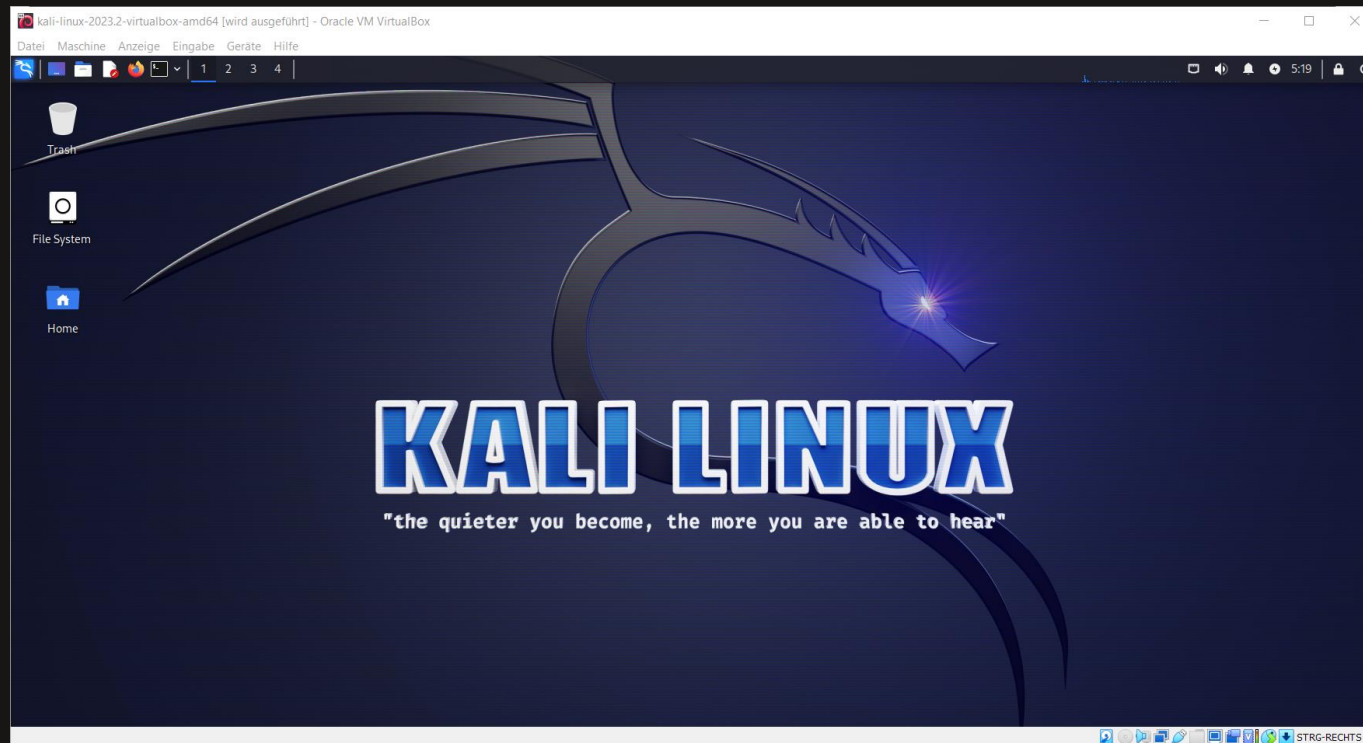


Verwendung



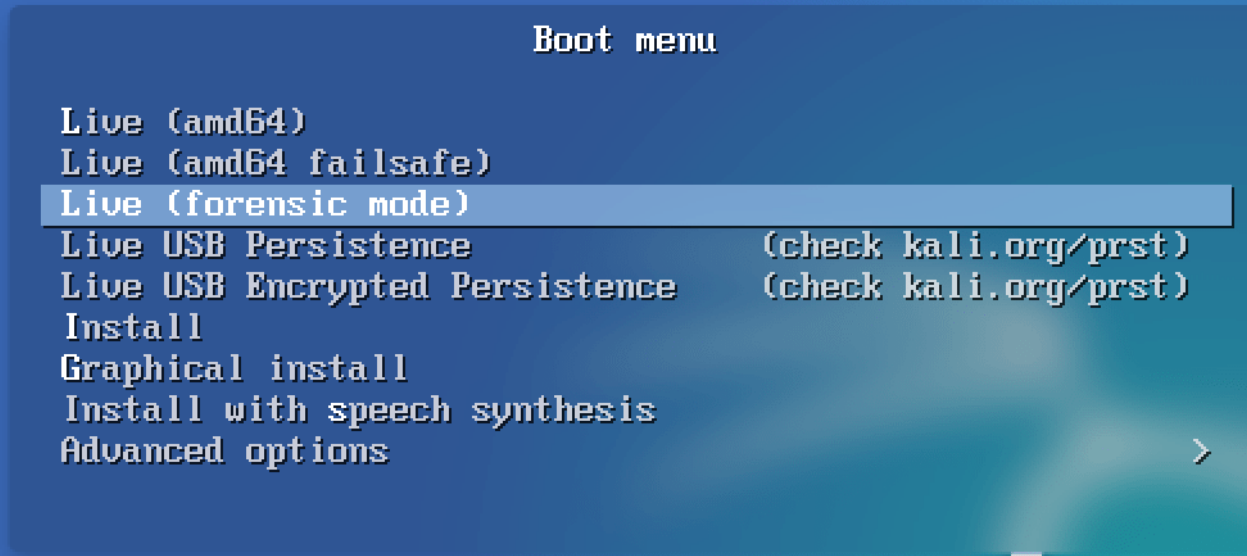
02. Kali Linux Hacking-Tools

LIVE Kali Linux Praxisbeispiele



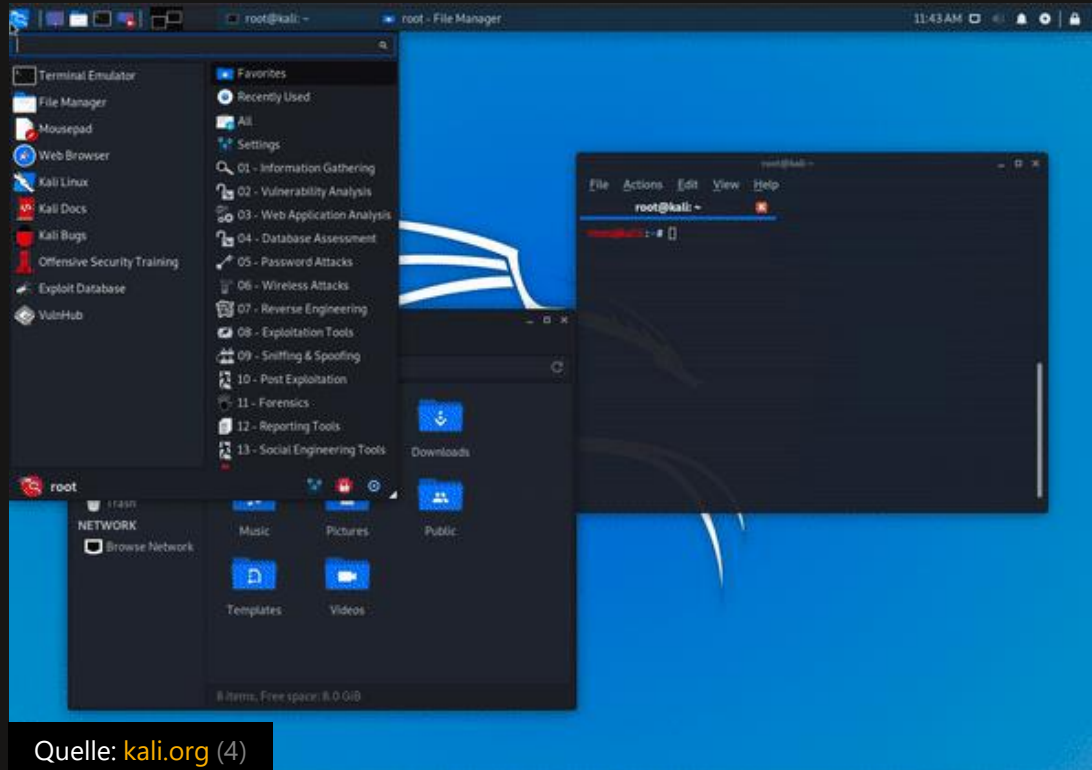
03. Erweiterte Einsatzgebiete

Forensics Mode



Quelle: kali.org (3)


Undercover



Nethunter Pro





Cloud


 **Cloud**


Kali Cloud images can quickly be deployed in multiple different cloud provider's infrastructures. This allows easy access to a Kali install in a modern environment with strong hardware resources. These are often used for short term Kali installs that are quick to deploy and quick to tear down.


[Kali-Cloud Documentation >](#)


Amazon AWS
[Marketplace](#) [Docs](#)


Digital Ocean
[Documentation](#)


Linode
[Marketplace](#) [Docs](#)


Microsoft Azure
[Marketplace](#) [Docs](#)


Generic Cloud Image
Run in any virtualized environment
[↓](#) [WEL](#) [torrent](#) [sum](#)

Quelle: [kali.org](#) (6)

Pi-Tail



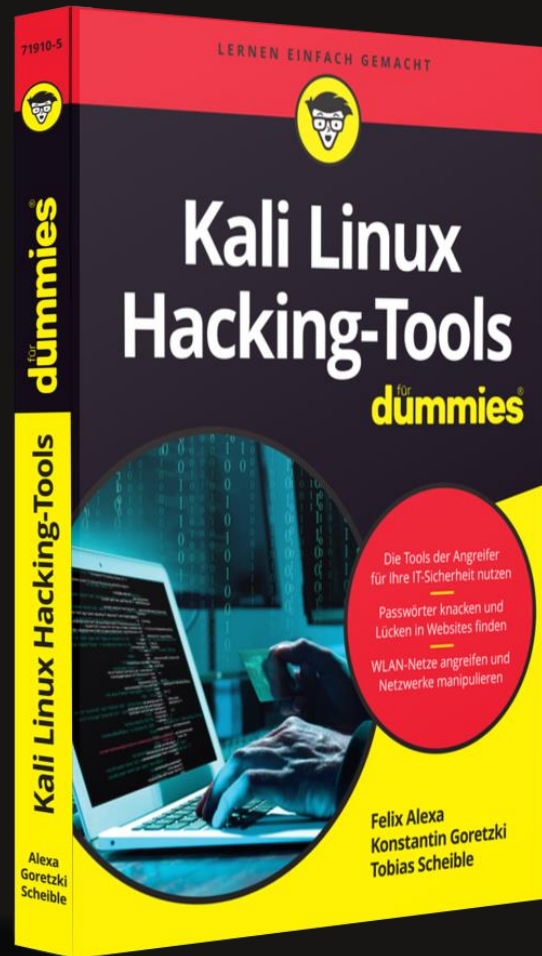
Quelle: kali.org (7)

Kali Linux Purple



Offensive IT-Sicherheit – Kali Linux

Noch Fragen?



Kali Linux

Laden Sie Kali Linux herunter und richten Sie sich eine virtuelle Maschine für Experimente ein.

Probieren Sie die Hacking-Tools von Kali Linux selbst aus, um Ihre Systeme zu testen.

„Kali Linux Hacking-Tools“ ist im Verlag Wiley-VCH erschienen:

www.wiley-vch.de/de/dummies

Quellen

- 1) <https://www.kali.org/>, abgerufen am 07.06.2023
- 2) <https://www.kali.org/blog/10-years/>, abgerufen am 07.06.2023
- 3) <https://www.kali.org/docs/general-use/kali-linux-forensics-mode/>, abgerufen am 07.06.2023
- 4) <https://www.kali.org/docs/introduction/kali-undercover/>, abgerufen am 07.06.2023
- 5) <https://www.kali.org/blog/kali-linux-2022-4-release/#kali-nethunter-pro-release>, abgerufen am 07.06.2023
- 6) <https://www.kali.org/get-kali/#kali-cloud>, abgerufen am 07.06.2023
- 7) <https://www.kali.org/docs/arm/raspberry-pi-zero-w-pi-tail/>, abgerufen am 07.06.2023
- 8) <https://www.kali.org/blog/kali-linux-2023-1-release/>, abgerufen am 07.06.2023