Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

DATA SECURITY

Kali Linux Essentials for Security Professionals Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE
P.O. Box 102802-00101, Nairobi, Kenya
Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy
Tel: +254 724 527 104 | +254 734 969 612
Email: training@datastatresearch.org
www.datastatresearch.org

Kali Linux Essentials for Security Professionals Training Course

Data Security • 5 Days Intensive • Accredited Certification

Course Overview

Kali Linux Essentials for Security Professionals Training Course provides security professionals with foundational mastery of Kali Linux, the industry-standard distribution for penetration testing and vulnerability assessment

Key Skills & Software Tools Covered

Kali Linux • penetration testing tools • ethical hacking

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
29 Dec 2025 – 2 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
29 Dec 2025 – 2 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Accra	Classroom / 5d	**$4,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
5 Jan 2026 – 9 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Kali Linux Essentials for Security Professionals Training Course

Introduction

The landscape of modern cybersecurity demands practitioners who can transition seamlessly from defense to offense to understand true organizational risk. Kali Linux Essentials for Security Professionals Training Course provides security professionals with foundational mastery of Kali Linux, the industry-standard distribution for penetration testing and vulnerability assessment. Participants will gain practical, hands-on experience with essential tools for network reconnaissance, exploitation, and post-exploitation activities in a controlled, ethical environment.

This course is engineered for the future of offensive security, focusing on real-world lab scenarios and leveraging trending cybersecurity tools within the Kali ecosystem. By learning to wield the core capabilities of this powerful platform, security analysts and aspiring ethical hackers will sharpen their ability to identify critical weaknesses, understand the attacker's perspective, and effectively fortify defenses against complex threats, including modern ransomware and cloud-native vulnerabilities.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

- Master the Linux command line interface for efficient security operations.
- Install, configure, and harden Kali Linux in a virtualized environment.
- Perform comprehensive network reconnaissance and footprinting using professional-grade tools.
- Conduct detailed vulnerability analysis to identify critical system weaknesses.
- Execute ethical hacking techniques on simulated target systems legally and responsibly.
- Understand and prevent common web application vulnerabilities.
- Utilize the Metasploit Framework for efficient exploitation and payload delivery.
- Implement post-exploitation strategies for persistence and privilege escalation.
- Perform password cracking and hash analysis using specialized tools like John the Ripper.
- Apply techniques for wireless network auditing and defense against common Wi-Fi attacks.
- Develop basic Bash and Python scripts for security automation and custom tool development.
- Establish robust digital forensics practices for evidence collection and preservation.
- Integrate Kali Linux findings into a professional Penetration Test Report.

Target Audience

- Aspiring Penetration Testers/Ethical Hackers
- Junior Security Analysts and SOC Analysts
- Network Administrators and System Engineers
- IT Auditors and Compliance Officers
- Forensics Investigators
- Blue Team members
- Software Developers
- Cloud Security Engineers

Course Modules

Module 1: Kali Linux & Foundational Security Setup

- Secure Virtualization Setup.
- Linux CLI Mastery
- System Hardening & Best Practices.
- Initial Network Configuration & Troubleshooting
- Case Study: "Securing the Lab" - Hardening a newly installed Kali instance to meet corporate baseline standards before any penetration testing begins.

Module 2: Network Reconnaissance and Footprinting

- Passive Reconnaissance.
- Active Scanning with Nmap.
- Vulnerability Scanning Fundamentals.
- DNS Enumeration and Network Mapping.
- Case Study: "Mapping the Target" - Using Nmap, WHOIS, and DNS tools to create a detailed network topology and service map for a publicly available corporate network.

Module 3: Vulnerability Assessment and Exploitation Basics

- Vulnerability Classification.
- Introduction to the Metasploit Framework.
- Exploitation Workflow.
- Avoiding Detection.
- Case Study: "Exploiting an Outdated Service" - Using Metasploit to exploit a known vulnerability found during a vulnerability scan, demonstrating a full exploit chain.

Module 4: Web Application Penetration Testing Essentials

- Introduction to Burp Suite Community Edition.
- OWASP Top 10 Overview

- SQL Injection Attacks using SQLMap.
- Authentication & Session Hijacking.
- Case Study: "E-Commerce Data Breach Simulation" - Performing a simulated SQL Injection attack on a vulnerable web application to extract customer data.

Module 5: Password Cracking and Access Attacks

- Understanding Hashes and Salt.
- Offline Password Cracking with John the Ripper and Hashcat.
- Online Brute-Forcing with Hydra.
- Credential Harvesting and Social Engineering Toolkit.
- Case Study: "Cracking the Weak Link" - Performing an effective dictionary and brute-force attack on a captured password hash file to highlight the risk of weak password policies.

Module 6: Wireless and Network Attacks (MITM)

- Wireless Network Auditing.
- Cracking WPA/WPA2-PSK.
- Man-in-the-Middle (MITM) Attacks.
- Network Sniffing and Packet Analysis with Wireshark.
- Case Study: "The Rogue Access Point" - Executing a controlled MITM attack to intercept non-HTTPS credentials over a simulated public Wi-Fi network and analyzing the captured traffic with Wireshark.

Module 7: Post-Exploitation and Maintaining Access

- Privilege Escalation Techniques.
- Pivoting and Tunneling.
- Covering Tracks.
- Creating Persistent Backdoors.
- Case Study: "From Shell to Root" - A multi-step lab where a low-privilege shell is exploited, a local privilege escalation technique is used to gain root access, and persistence is established.

Module 8: Security Automation and Professional Reporting

- Scripting for Security.
- Introduction to Digital Forensics Tools.
- Developing an Incident Response Plan.
- Penetration Test Reporting.
- Case Study: "The Final Report" - Taking the findings from all previous modules to generate a professional, high-impact Vulnerability Management and Penetration Test Report for a simulated C-level audience.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/kali-linux-essentials-for-security-professionals-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.