Training Course on Ethical Hacking for Data Scientists

Professional Development Training Course Outline

Category	Data Science	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's data-driven world, the convergence of **data science** and **cybersecurity** is paramount. As organizations increasingly rely on vast datasets for critical insights and decision-making, the potential for data breaches and malicious attacks escalates. Training Course on Ethical Hacking for Data Scientists empowers data professionals with the offensive security mindset and defensive strategies needed to proactively identify, analyze, and mitigate vulnerabilities within data systems, ensuring robust **data integrity**, **privacy**, and **system resilience**. By understanding how malicious actors exploit weaknesses, data scientists can build more secure **machine learning models**, safeguard sensitive **big data infrastructure**, and contribute significantly to an organization's overall **cyber defense posture**.

This program delves into the practical application of **penetration testing methodologies** and **vulnerability assessment techniques** specifically tailored for the unique challenges of data-centric environments. Participants will gain hands-on experience with industry-standard **ethical hacking tools** and learn to implement **secure coding practices** for data pipelines and analytics platforms. The emphasis is on fostering a proactive security culture, transforming data scientists from potential targets into frontline defenders of their most valuable asset: data.

Programme Curriculum

Training Course on Ethical Hacking for Data Scientists

Introduction

In today's data-driven world, the convergence of **data science** and **cybersecurity** is paramount. As organizations increasingly rely on vast datasets for critical insights and decision-making, the potential for data breaches and malicious attacks escalates. Training Course on Ethical Hacking for Data Scientists empowers data professionals with the offensive security mindset and defensive strategies needed to proactively identify,

analyze, and mitigate vulnerabilities within data systems, ensuring robust **data integrity**, **privacy**, and **system resilience**. By understanding how malicious actors exploit weaknesses, data scientists can build more secure **machine learning models**, safeguard sensitive **big data infrastructure**, and contribute significantly to an organization's overall **cyber defense posture**.

This program delves into the practical application of **penetration testing methodologies** and **vulnerability assessment techniques** specifically tailored for the unique challenges of data-centric environments. Participants will gain hands-on experience with industry-standard **ethical hacking tools** and learn to implement **secure coding practices** for data pipelines and analytics platforms. The emphasis is on fostering a proactive security culture, transforming data scientists from potential targets into frontline defenders of their most valuable asset: data.

Course Duration

10 days

Course Objectives

1. Learn the phases of a cyberattack and how they apply to data systems.
2. Identify common weaknesses in **databases**, **data warehouses**, **cloud data platforms**, and **API endpoints** used in data science.
3. Utilize **OSINT (Open-Source Intelligence)** and specialized tools to gather information on data targets.
4. Discover open ports, services, and devices relevant to data storage and processing.
5. Exploit vulnerabilities like **SQL Injection**, **Cross-Site Scripting (XSS)**, and insecure **API configurations** impacting data.
6. Assess and secure **cloud storage buckets (e.g., S3)**, **NoSQL databases**, and traditional **relational databases**.
7. Learn best practices for **data ingestion**, **data processing**, and **data transformation security**.
8. Identify vulnerabilities in **adversarial AI attacks**, **data poisoning**, and **model evasion**.
9. Formulate strategies for detecting, containing, and recovering from data-related security incidents.
10. Implement effective **encryption techniques** for data at rest and in transit.
11. Secure access to data resources through robust authentication and authorization mechanisms.
12. Understand the implications of **GDPR**, **HIPAA**, and other data protection laws in ethical hacking.
13. Integrate security considerations throughout the data lifecycle.

Organizational Benefits

- Proactively identify and remediate vulnerabilities in critical **data assets**, reducing the risk of costly data breaches.
- Ensure adherence to stringent **data privacy regulations** (GDPR, HIPAA, CCPA) and industry standards, mitigating legal and reputational risks.
- Cultivate a **security-aware data science team** capable of building and maintaining resilient data systems.
- Minimize the attack surface for **data exfiltration**, **ransomware**, and other malicious activities targeting data.
- Build customer trust and demonstrate a commitment to **data security** in an increasingly data-conscious market.
- Enable faster and more effective response to data-related security incidents, minimizing downtime and impact.

Target Audience

1. Data Scientists & Analysts
2. Machine Learning Engineers
3. Big Data Architects & Engineers
4. Database Administrators (DBAs).
5. Security Analysts & Consultants
6. Software Developers (with data focus).
7. IT Managers & Project Leads.
8. Anyone interested in Data Security

Course Outline

Module 1: Introduction to Ethical Hacking & Data Security Fundamentals

- Key Concepts: Ethical hacking principles, legal and ethical considerations, types of hackers.
- Information Security Principles: Confidentiality, Integrity, Availability (CIA Triad) in the context of data.
- Cyber Kill Chain for Data Systems: Understanding attack phases from a data perspective.
- Threat Landscape for Data Scientists: Common threats and attack vectors targeting data.
- **Case Study**: Analyzing a major data breach (e.g., Equifax) from an ethical hacking viewpoint.

Module 2: Reconnaissance & Footprinting for Data Discovery

- Passive & Active Reconnaissance: Techniques for gathering information about data targets.
- OSINT (Open-Source Intelligence) for Data: Google Dorking, social media analysis, public records.
- Network Footprinting: DNS enumeration, Whois lookup, domain mapping for data infrastructure.
- **Tools**: Maltego, Shodan, Recon-ng.
- **Case Study**: Discovering publicly exposed S3 buckets and sensitive data using OSINT tools.

Module 3: Network Scanning & Enumeration for Data Environments

- Network Scanning Techniques: Port scanning (TCP/UDP), vulnerability scanning.
- Identifying Data-Related Services: SQL databases, NoSQL databases, message queues.
- Enumeration Techniques: SMB, SNMP, user enumeration for data system access.
- Tools: Nmap, Nessus, OpenVAS.
- **Case Study**: Identifying open database ports and misconfigured services on a data analytics cluster.

Module 4: Vulnerability Analysis & Exploitation of Data Systems

- Vulnerability Assessment Methodologies: CVSS scoring, common vulnerability databases (CVE).
- Exploitation Frameworks: Metasploit for targeting data-centric vulnerabilities.
- Buffer Overflows & Privilege Escalation: Gaining elevated access within data environments.
- Exploiting Misconfigurations: Weak default credentials, unpatched software.
- **Case Study**: Exploiting a known vulnerability in a data visualization dashboard to gain unauthorized access to underlying data.

Module 5: Database Hacking & Data Exfiltration

- SQL Injection (SQLi): Advanced techniques for database exploitation and data extraction.
- NoSQL Injection: Attacking MongoDB, Cassandra, and other NoSQL databases.
- Database Specific Vulnerabilities: Weak configurations, insecure stored procedures.
- Data Exfiltration Techniques: Stealing sensitive data from compromised databases.
- **Case Study**: Performing a successful SQL Injection attack to retrieve customer credit card information from a vulnerable e-commerce database.

Module 6: Cloud Data Security & Penetration Testing

- Cloud Security Models: IaaS, PaaS, SaaS security considerations for data.
- AWS, Azure, GCP Data Security: Specific vulnerabilities and best practices.
- Cloud Storage Exploits: Misconfigured S3 buckets, Azure Blob storage.
- Identity and Access Management (IAM) in Cloud: Exploiting weak IAM policies for data access.
- **Case Study**: Demonstrating a cloud data exfiltration scenario due to an overly permissive IAM role.

Module 7: Web Application & API Security for Data Scientists

- OWASP Top 10 for Data Applications: Focusing on injection, broken authentication, sensitive data exposure.
- Cross-Site Scripting (XSS): Impact on data integrity and user sessions.
- Insecure Direct Object References (IDOR): Exploiting access control flaws in data APIs.
- API Security Best Practices: Authentication, authorization, rate limiting for data endpoints.
- **Case Study**: Discovering an IDOR vulnerability in a data API that allows unauthorized access to other users' datasets.

Module 8: Machine Learning & AI Model Security

- Adversarial AI Attacks: Data poisoning, model evasion, model inversion.
- Data Poisoning: Manipulating training data to corrupt model output.
- Model Evasion: Crafting inputs to bypass a trained model's detection.
- Bias in AI Models: Unintentional vulnerabilities leading to unfair or insecure outcomes.
- **Case Study**: Demonstrating a data poisoning attack on a fraud detection model to bypass its protective mechanisms.

Module 9: Cryptography & Data Encryption

- Fundamentals of Cryptography: Symmetric vs. Asymmetric encryption.
- Hashing and Digital Signatures: Ensuring data integrity and authenticity.
- Data Encryption at Rest: Disk encryption, database encryption, cloud storage encryption.
- Data Encryption in Transit: TLS/SSL for secure data communication.
- **Case Study**: Implementing strong encryption for a sensitive customer database and testing its resilience against brute-force attacks.

Module 10: Secure Data Engineering & MLOps Practices

- Secure Data Ingestion: Validating and sanitizing incoming data.
- Secure Data Transformation: Protecting data during ETL/ELT processes.
- Secure MLOps Pipelines: Integrating security checks into model deployment.
- Container Security for Data Applications: Docker, Kubernetes best practices.
- **Case Study**: Identifying and patching a vulnerability in a data processing script that could lead to data corruption.

Module 11: Insider Threats & Social Engineering in Data Environments

- Understanding Insider Threats: Malicious vs. negligent insiders.
- Social Engineering Techniques: Phishing, pretexting, baiting targeting data professionals.
- Protecting Against Social Engineering: Security awareness training for data teams.
- Data Loss Prevention (DLP): Tools and strategies to prevent unauthorized data exfiltration.

- **Case Study**: Analyzing a phishing attempt designed to trick a data scientist into revealing database credentials.

Module 12: Incident Response & Digital Forensics for Data Breaches

- Incident Response Lifecycle: Preparation, detection, containment, eradication, recovery.
- Data Breach Triage: Identifying the scope and impact of a data breach.
- Digital Forensics Fundamentals: Collecting and preserving evidence from data systems.
- Log Analysis for Data Incidents: Identifying suspicious activity in database and application logs.
- **Case Study**: Simulating a data breach scenario and initiating incident response procedures, including forensic data collection.

Module 13: Legal, Ethical & Compliance Aspects of Data Security

- Data Privacy Regulations: Deep dive into GDPR, CCPA, HIPAA, and their impact on data handling.
- Ethical Disclosure of Vulnerabilities: Responsible disclosure policies.
- Legal Consequences of Cybercrime: Understanding data protection laws and penalties.
- Building a Culture of Security: Promoting ethical hacking principles within organizations.
- **Case Study**: Navigating the legal and ethical considerations when discovering a critical vulnerability in a client's data system.

Module 14: Advanced Data System Exploitation (Red Teaming)

- Adversary Simulation: Emulating real-world threat actor techniques.
- Lateral Movement in Data Networks: Gaining deeper access within an organization's data infrastructure.
- Persistence Techniques: Maintaining access to compromised data systems.
- Covering Tracks: Evading detection and removing forensic evidence.
- **Case Study**: A full red team exercise targeting a mock data analytics environment, from initial access to data exfiltration.

Module 15: Future Trends in Data Security & Ethical Hacking

- AI in Ethical Hacking: Automated vulnerability scanning, AI-powered threat detection.
- Quantum Computing and Cryptography: Future challenges and solutions for data security.
- Blockchain for Data Integrity: Exploring decentralized data security solutions.
- Zero Trust Architecture for Data: Implementing a "never trust, always verify" model.
- **Case Study**: Discussing the security implications of emerging data technologies like homomorphic encryption and federated learning.

Training Methodology

This course employs a highly interactive and hands-on training methodology, integrating:

- **Lectures & Discussions**: Clear explanations of concepts, theories, and real-world examples.
- **Live Demonstrations**: Expert-led demonstrations of ethical hacking tools and techniques on simulated environments.
- **Hands-on Labs**: Extensive practical exercises and guided labs using industry-standard tools (Kali Linux, Metasploit, Wireshark, Nmap, Burp Suite, etc.). Participants will work on dedicated lab environments replicating real-world data systems.
- **Case Studies & Scenarios**: Analysis of real-world data breaches and security incidents to understand attack vectors and defense strategies.

- **Capture The Flag (CTF) Challenges**: Engaging, problem-solving exercises to apply learned skills in a competitive, gamified environment.
- **Group Projects**: Collaborative exercises to simulate team-based ethical hacking engagements on data systems.
- **Q&A Sessions**: Dedicated time for participants to ask questions and deepen their understanding.
- **Certification Preparation**: Guidance and resources for relevant ethical hacking and data security certifications.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

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 Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com