BLACKBIRD FOR TRAINING

# Ethical Hacker

28 February – 4 March 2027
Amman (Jordan)

UK Traininig
PARTNER



www.blackbird-training.com

# Ethical Hacker

**Ref:** 3255450_203723 **Date:** 28 February – 4 March 2027 **Location:** Amman (Jordan) **Fees:** 4900 GBP

## Introduction

In today's highly interconnected digital environment, organizations face increasing pressure to safeguard their systems, data, and networks from emerging cyber threats. As cyberattacks evolve in complexity and sophistication, leaders across various industries are recognizing the importance of equipping their teams with the advanced skills and practical techniques needed to protect organizational assets. This is where the role of the ethical hacker becomes essential—providing organizations with the capability to identify vulnerabilities before malicious actors exploit them.

This program is designed for executives, department managers, team leaders, cybersecurity practitioners, IT specialists, risk professionals, project coordinators, and individuals working across diverse sectors that rely heavily on digital operations. These professionals aim to strengthen their defensive capabilities, understand threat landscapes, and adopt proactive strategies that mitigate risks. The Ethical Hacker course fulfills the needs of individuals seeking professional certifications, practical tools, and modern methodologies that improve organizational resilience and operational security.

The course offers a comprehensive, practice-oriented learning experience that explores ethical hacking methodologies, penetration testing processes, vulnerability assessment frameworks, and advanced attack-simulation techniques. Through structured modules and real-world scenarios, participants learn how to evaluate system weaknesses, design strong security controls, and develop defensive measures that strengthen cyber readiness.

## Course Objectives

By the end of the program, participants will be able to:

- Understand the foundational principles and responsibilities of an Ethical Hacker.
- Recognize different types of cyber threats and attack methodologies.
- Conduct vulnerability assessments on systems, applications, and networks.
- Perform penetration testing using structured and ethical approaches.
- Identify security gaps and recommend appropriate remediation strategies.
- Apply methodologies for analyzing and interpreting security testing results.
- Understand the phases of ethical hacking and how they support risk reduction.
- Use cybersecurity tools to test system resilience and detect weaknesses.
- Build comprehensive reports that highlight vulnerabilities and corrective actions.
- Strengthen organizational readiness through proactive security planning.



# Course Outlines

## Day One: Foundations of Ethical Hacking

- Introduction to ethical hacking, principles, and legal considerations.
- Understanding the role of ethical hacking in modern cybersecurity.
- Key terminology, threat types, and attacker profiles.
- Overview of hacking phases and structured testing approaches.
- Identifying system vulnerabilities and common entry points.
- Building a security mindset for proactive threat detection.

## Day Two: Vulnerability Assessment and Information Gathering

- Methods of gathering security-related intelligence.
- Identifying weaknesses in systems, devices, and applications.
- Techniques for mapping system structures and network architectures.
- Understanding open ports, services, and system exposure.
- Tools and techniques for detecting misconfigurations.
- Documenting findings and preparing for deeper security testing.

## Day Three: Penetration Testing Techniques

- Understanding the penetration testing workflow.
- Simulating cyberattacks using structured methodologies.
- Exploiting system vulnerabilities in a controlled and ethical manner.
- Assessing password strength, authentication systems, and user policies.
- Testing web applications for cross-site scripting and SQL injection.
- Evaluating the organization’s incident response readiness.

## Day Four: Advanced Security Testing and Defense Strategies

- Conducting advanced exploitation techniques in secure environments.
- Testing network devices, routers, firewalls, and wireless infrastructures.
- Evaluating cryptography practices and identifying encryption gaps.
- Detecting malware signatures and abnormal system behavior.
- Strengthening internal defenses through layered protection strategies.
- Building comprehensive mitigation plans for identified weaknesses.



### Day Five: Reporting, Recommendations, and Strategic Planning

- Developing detailed vulnerability and penetration testing reports.
- Prioritizing risks based on severity and potential impact.
- Communicating findings effectively with leadership and technical teams.
- Designing long-term security improvement roadmaps.
- Practical review of real-world case studies and testing scenarios.
- Final assessment and reflection on key learning outcomes.

## Why Attend This Course? Wins & Losses!

- Gain a professional understanding of ethical hacking principles and practices.
- Learn how to detect risks before they become critical threats.
- Strengthen your ability to protect organizational assets and systems.
- Acquire hands-on skills that apply directly to real-world cyber challenges.
- Gain access to structured, practical methodologies used by professionals.
- Enhance your cybersecurity decision-making and risk-analysis capabilities.
- Build strong foundations that support advanced cybersecurity certifications.
- Improve your readiness to contribute to organizational security strategies.

## Conclusion

The Ethical Hacker course provides a comprehensive framework for understanding, identifying, and addressing vulnerabilities across digital environments. By mastering ethical hacking methodologies, participants gain the ability to evaluate system weaknesses, design meaningful mitigation strategies, and contribute effectively to organizational security.

Through practical learning modules, structured simulations, and in-depth analysis, this program equips learners with the skills and confidence required to navigate evolving cyber threats. The knowledge gained empowers participants to support security teams, enhance operational resilience, and ensure that digital environments remain robust, secure, and aligned with organizational needs.

**This course is designed to elevate professional capabilities, strengthen cyber readiness, and prepare participants to play an essential role in safeguarding digital infrastructures in a rapidly changing technological world.**

