BLACKBIRD FOR TRAINING

Ethical Hacking and Penetration Testing Masterclass

15 – 19 November 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



www.blackbird-training.com

Ethical Hacking and Penetration Testing Masterclass

Ref: 3255277_201646 **Date:** 15 – 19 November 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

In an era where cyber threats are constantly evolving, organizations face an ongoing challenge to protect their digital assets from sophisticated attacks. Ethical hacking and penetration testing have become essential practices for identifying and addressing vulnerabilities before they can be exploited by malicious actors.

The Ethical Hacking and Penetration Testing Masterclass provides participants with the technical expertise and practical experience required to evaluate and strengthen the security posture of networks, systems, and applications. The course combines theoretical foundations with intensive hands-on exercises, equipping learners with the skills to simulate real-world cyberattacks, identify weaknesses, and implement effective countermeasures.

This masterclass is designed for cybersecurity professionals, IT administrators, and security managers who seek to build proactive defense capabilities and enhance their understanding of modern hacking techniques in a controlled, ethical environment.

Course Objectives

By the end of this course, participants will be able to:

- Understand the core concepts and methodologies of ethical hacking.
- Identify and analyze security vulnerabilities across networks and applications.
- Utilize advanced penetration testing tools and frameworks effectively.
- Conduct ethical hacking engagements safely and systematically.
- Document and report findings with actionable recommendations.
- Apply countermeasures to mitigate and prevent discovered threats.
- Align ethical hacking practices with organizational cybersecurity strategies.

Course Outlines

Day 1: Fundamentals of Ethical Hacking and Cybersecurity Concepts

- Introduction to ethical hacking and its professional significance.
- Types of hackers and the difference between ethical and malicious hacking.
- Phases of penetration testing: reconnaissance, scanning, exploitation, and reporting.
- Legal and ethical considerations in ethical hacking.
- Overview of penetration testing tools and lab setup.



Day 2: Information Gathering and Reconnaissance

- Techniques for collecting information about target systems.
- Passive and active reconnaissance methods.
- Network mapping and discovery of potential vulnerabilities.
- Identifying open ports, services, and operating systems.
- Tools for reconnaissance: Nmap, Whois, and OSINT frameworks.

Day 3: Vulnerability Assessment and Exploitation

- Introduction to vulnerability scanning and analysis.
- Using automated tools like Nessus and OpenVAS.
- Exploiting discovered vulnerabilities through manual and automated methods.
- Privilege escalation techniques and bypassing security controls.
- Case study: Exploiting and patching a vulnerable system.

Day 4: Web Application and System Penetration Testing

- Understanding web application architectures and attack surfaces.
- Common web vulnerabilities: SQL injection, XSS, CSRF, and command injection.
- Testing authentication and session management mechanisms.
- System-level penetration testing and post-exploitation strategies.
- Real-world lab exercises simulating attacks on web applications.

Day 5: Reporting, Remediation, and Best Practices

- Documenting penetration testing results professionally.
- Writing clear, actionable security recommendations.
- Prioritizing vulnerabilities based on risk levels.
- Developing remediation plans and verifying fixes.
- Final review and hands-on assessment of a complete ethical hacking cycle.

Why Attend This Course: Wins & Losses!

- Gain practical experience in ethical hacking and penetration testing.
- Learn to identify, exploit, and mitigate real-world vulnerabilities.
- Master industry-standard tools and testing methodologies.
- Strengthen your ability to assess and secure enterprise networks.
- Develop professional reporting and communication skills for cybersecurity.
- Improve your organization’s resilience against cyberattacks.
- Understand how hackers think and act to build proactive defenses.
- Earn skills that are in high demand in cybersecurity careers.



Conclusion

The Ethical Hacking and Penetration Testing Masterclass offers a comprehensive and practical pathway to mastering the art of ethical hacking. It empowers professionals to adopt a proactive approach to cybersecurity—understanding attacker techniques, identifying weaknesses, and building stronger defenses.

Through a balance of theory and extensive hands-on exercises, participants will leave this course equipped with the skills to conduct penetration tests, analyze vulnerabilities, and implement robust security strategies.

In a world where cyber threats continue to grow in complexity, ethical hackers play a vital role in protecting organizations and ensuring the integrity of digital ecosystems. This course provides the knowledge and confidence to be at the forefront of that mission.

