MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

ETHICAL HACKING

"Identify Vulnerabilities, Exploit Ethically, and Strengthen Defenses."

Schedule

Venue (InHouse)	Fees
At Your Organization Premises	Ask For The Quotation

► **Available delivery methods:** Face-to-Face & Online Training, In-House Training

Introduction

As cyber threats grow in scale and sophistication, organizations must adopt proactive approaches to find and fix security weaknesses before attackers exploit them. Ethical hacking (also known as penetration testing or red teaming) is a controlled, authorized process of simulating real-world attacks to evaluate the security posture of systems, applications, and networks.

The Certified Ethical Hacking course trains participants in offensive security techniques, legal and ethical considerations, and defensive countermeasures. Through hands-on labs, real-case scenarios, and industry-standard tools, participants learn how attackers think and operate, so they can design better protections, prioritize remediation, and improve incident response. The course balances technical depth with governance, ensuring ethical practice and compliance with laws and organizational policies.

Objectives

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

- Understand the ethical, legal, and professional responsibilities of an ethical hacker.
- Perform structured vulnerability assessments and penetration tests against networks, web apps, and endpoints.
- Use industry-standard tools and frameworks for reconnaissance, scanning, exploitation, and post-exploitation.
- Identify and exploit common vulnerabilities (OWASP Top 10, misconfigurations, weak credentials).
- Conduct wireless, mobile, and cloud security assessments.
- Execute social engineering techniques safely to test human factors.
- Document findings clearly and provide prioritized remediation recommendations.
- Support blue-team activities through threat hunting, detection tuning, and incident response collaboration.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

Organizations need skilled professionals who can test systems in a controlled, ethical manner and translate technical findings into actionable risk reduction. This course provides practical, hands-on experience that prepares participants to run effective penetration tests, improve security controls, and support compliance and risk-management objectives. It is ideal for anyone seeking to move from theory to applied offensive security.

Target Audience

This course is suitable for:

- Security analysts and penetration testers
- Network and system administrators
- Application developers and DevOps engineers
- Incident response and SOC personnel
- IT auditors and compliance officers
- Security consultants and risk managers
- Anyone pursuing a career in offensive security or aiming to solidify defensive practices

Individual Benefits

- Master practical penetration-testing skills and toolchains.
- Improve understanding of attackers' methods to better defend systems.
- Boost career prospects in cybersecurity with a recognized practical qualification.
- Learn to produce professional test reports and remediation guidance.
- Gain confidence performing authorized assessments across different environments.
- Build transferable skills for threat hunting, red teaming, and security architecture reviews.

Organizational Benefits

- Discover and remediate security weaknesses before they are exploited.
- Build internal capability for repeatable, compliant penetration testing.
- Improve incident detection and response by understanding attacker behavior.
- Reduce breach likelihood and minimize potential financial, operational, and reputational loss.
- Align security testing with regulatory and contractual requirements.
- Foster a security-aware culture through tested social engineering and training feedback.

Instructional Methodology

The course follows a hands-on, lab-centric approach combined with practical theory and reporting practice:

- Instructor-led sessions covering concepts, techniques, and legal/ethical boundaries.
- Live demonstrations of tools and attack techniques.
- Guided, hands-on labs in controlled environments (virtual machines, lab networks, web app targets).
- Scenario-based exercises (network compromise, web app exploitation, lateral movement).
- Group red-team vs blue-team workshops to practice detection and remediation.
- Assignments culminating in a full penetration-test report and remediation plan.
- Continuous assessment, debriefs, and Q&A.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Module 1: Ethics, Legal Frameworks, Engagement Scoping, and Rules of Engagement

Module 2: Reconnaissance and OSINT (open-source intelligence) techniques

Module 3: Network Scanning, Enumeration, and Vulnerability Discovery

Module 4: Exploitation Fundamentals — Buffer overflows, misconfigurations, and privilege escalation

Module 5: Web Application Security — OWASP Top 10, SQLi, XSS, CSRF, SSRF, authentication flaws

Module 6: Wireless and Mobile Security Assessments

Module 7: Network Post-Exploitation, Lateral Movement, Persistence, and Data Exfiltration

Module 8: Cloud and Container Security Testing (AWS/Azure/GCP fundamentals)

Module 9: Social Engineering and Physical Security Testing (phishing simulations, human factors)

Module 10: Malware basics, sandboxing, and safe handling of malicious artifacts

Module 11: Defensive Integration — logging, detection engineering, threat hunting collaboration

Module 12: Reporting, Risk Prioritization, and Remediation Roadmaps

Module 13: Capstone Practical — Full-scope penetration test with final professional report and remediation presentation

Certification

Upon successful completion, participants will receive a Certified Ethical Hacking certificate, recognizing hands-on competence in conducting authorized penetration tests and delivering actionable remediation guidance. Certification demonstrates practical skills in offensive security, ethical practice, and the ability to integrate findings into organizational risk management.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**