MAWA EVENTS

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

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

PENETRATION TESTING: INVOLVES SIMULATED ATTACKS ON A SYSTEM TO IDENTIFY AND EXPLOIT VULNERABILITIES.

""Simulating Cyber Attacks to Identify and Exploit System Vulnerabilities""

Schedule

Date	Venue	Fees (Face-to-Face)
13 – 17 Apr 2026	London, UK	USD 3495 per delegate

Introduction

Penetration testing, also known as ethical hacking, is a crucial practice in identifying and addressing vulnerabilities within systems and applications. This 5-day course is designed for IT security professionals who wish to master penetration testing techniques. Participants will learn how to simulate cyberattacks on a system, uncover vulnerabilities, and exploit weaknesses to understand potential security threats. Through hands-on training, participants will develop the skills needed to conduct ethical hacking and improve their organization\'s cybersecurity defenses.

The course covers the key principles of penetration testing, including reconnaissance, vulnerability scanning, exploitation, and post-exploitation. Participants will gain practical experience in applying penetration testing tools and methodologies to assess and secure IT environments.

Objectives

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

- Understand the principles and methodologies of penetration testing.
- Conduct penetration testing on various systems, networks, and applications.
- Use tools and techniques for identifying vulnerabilities and exploiting weaknesses.
- Perform reconnaissance and scanning to uncover attack surfaces.
- Simulate real-world attacks to assess the security of IT systems and applications.
- Report findings and recommend remediation measures to improve system security.

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

- Gain hands-on experience in penetration testing and ethical hacking.
- Learn to identify and exploit vulnerabilities in networks, systems, and applications.
- Improve your ability to assess the security of IT environments and uncover potential security flaws.
- Master the tools and techniques used by penetration testers to simulate cyberattacks.
- Enhance your skills in identifying weaknesses before malicious attackers can exploit them.
- Develop a deep understanding of common attack vectors and how to protect against them.

Target Audience

This program is designed for:

- IT security professionals and network administrators
- Penetration testers and ethical hackers
- Security analysts and consultants
- IT auditors and compliance officers
- Anyone looking to develop expertise in penetration testing and cybersecurity

Individual Benefits

Key competencies that will be developed include:

- Proficiency in penetration testing tools and techniques.
- In-depth understanding of security vulnerabilities and how to exploit them.
- Advanced skills in reconnaissance, scanning, and exploiting systems.
- Expertise in conducting vulnerability assessments and identifying critical security gaps.
- Ability to generate detailed reports on penetration testing findings and recommend corrective actions.

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Enhanced ability to conduct comprehensive penetration tests on systems and applications.
- Improved security posture by identifying and mitigating system vulnerabilities.
- Increased ability to simulate and respond to real-world cyberattacks.
- Stronger organizational defenses against malicious cyberattacks.
- Improved compliance with cybersecurity regulations and industry standards.

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – In-depth discussions on penetration testing principles, methodologies, and industry best practices.
- Case Studies – Real-world examples of cyberattacks and penetration testing scenarios.
- Workshops – Hands-on exercises using penetration testing tools to simulate attacks and exploit vulnerabilities.
- Peer Exchange – Group discussions and collaborative learning on penetration testing challenges and solutions.
- Tools – Practical use of industry-standard tools for penetration testing, including Kali Linux, Metasploit, Nmap, Burp Suite, and others.

MAWA EVENTS

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

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

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

Training Hours: 7:30 AM – 3:30 PM Daily Format: 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Introduction to Penetration Testing

- Module 1: Understanding Penetration Testing (07:30 – 09:30)
- Key principles and objectives of penetration testing
- Differences between ethical hacking and malicious hacking
- The ethical hacker’s role in cybersecurity
- Module 2: Penetration Testing Methodology (09:45 – 11:15)
- Overview of the penetration testing lifecycle: reconnaissance, scanning, exploitation, post-exploitation
- Developing a penetration testing plan and strategy
- Tools and techniques for conducting penetration tests
- Module 3: Legal and Ethical Considerations (11:30 – 01:00)
- Legal implications of penetration testing and ethical hacking
- Understanding consent and authorization in penetration testing
- Best practices for ensuring legal and ethical compliance

Day 2: Reconnaissance and Scanning

- Module 1: Information Gathering and Reconnaissance (07:30 – 09:30)
- Techniques for gathering information about target systems (OSINT)
- Tools for conducting reconnaissance: Nmap, WHOIS, DNS interrogation, etc.
- Mapping the attack surface through reconnaissance
- Module 2: Vulnerability Scanning and Enumeration (09:45 – 11:15)
- Introduction to vulnerability scanning tools: Nessus, OpenVAS, Nikto
- Scanning for open ports, services, and potential vulnerabilities
- Identifying exposed services and security weaknesses
- Module 3: Identifying Attack Vectors (11:30 – 01:00)
- Understanding common attack vectors: SQL injection, cross-site scripting (XSS), etc.
- Mapping and prioritizing vulnerabilities based on risk assessment
- Using reconnaissance data to identify exploitation opportunities

Day 3: Exploitation and Post-Exploitation

- Module 1: Exploiting Vulnerabilities (07:30 – 09:30)
- Exploiting known vulnerabilities in systems and applications
- Using Metasploit and other tools to exploit weaknesses
- Privilege escalation techniques and strategies
- Module 2: Post-Exploitation Techniques (09:45 – 11:15)
- Maintaining access after exploitation
- Establishing persistence and backdoors in compromised systems
- Escalating privileges and pivoting through the network
- Module 3: Reporting Findings and Impact (11:30 – 01:00)
- Documenting and reporting exploited vulnerabilities and findings
- Assessing the business impact of vulnerabilities and exploitation
- Best practices for providing actionable recommendations for remediation

Day 4: Advanced Penetration Testing Techniques

-

Module 1: Web Application Penetration Testing (07:30 – 09:30)

- Techniques for testing web application vulnerabilities: SQL injection, XSS, CSRF, etc.
- Tools for web application penetration testing: Burp Suite, OWASP ZAP
- Attacking web applications and identifying common security flaws
- Module 2: Wireless and Network Penetration Testing (09:45 – 11:15)
- Penetration testing for wireless networks: WPA/WPA2 cracking, man-in-the-middle attacks
- Techniques for network penetration testing: sniffing, spoofing, denial of service (DoS)
- Tools and techniques for assessing network security
- Module 3: Advanced Exploitation Techniques (11:30 – 01:00)
- Exploiting advanced vulnerabilities and zero-day exploits
- Techniques for bypassing security mechanisms (firewalls, intrusion detection systems, etc.)
- Using advanced exploitation tools and techniques

Day 5: Wrapping Up and Reporting

- Module 1: Conducting Final Penetration Testing (07:30 – 09:30)
- Final penetration testing activities: exploitation, reporting, and remediation recommendations
- Understanding post-test actions and system cleanup
- Wrapping up the engagement and handing over findings to the client
- Module 2: Writing Penetration Testing Reports (09:45 – 11:15)
- Best practices for writing clear, actionable penetration testing reports
- Structuring a report to include findings, risk assessments, and remediation strategies
- Communicating technical findings to non-technical stakeholders
- Module 3: Certification Review and Final Q&A (11:30 – 01:00)
- Recap of key concepts and techniques covered in the course
- Final Q&A session to clarify any remaining questions
- Preparing for certification exam and next steps in ethical hacking

Certification

Upon completing the training course, participants will receive a Certificate of Completion in Penetration Testing, recognizing their ability to conduct penetration tests, identify vulnerabilities, and implement security measures to protect systems from cyber threats.

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**