MAWA EVENTS

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

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

OSCP (OFFENSIVE SECURITY CERTIFIED PROFESSIONAL)

"Master Ethical Hacking with the Industry's Most Respected Penetration Testing Certification"

Schedule

Date	Venue	Fees (Face-to-Face)
13 – 17 Jul 2026	Dubai, UAE	USD 3495 per delegate

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

Introduction

The Offensive Security Certified Professional (OSCP) is a globally recognized ethical hacking certification that demonstrates practical, hands-on penetration testing skills. This 5-day bootcamp-style training prepares participants to earn the OSCP by teaching advanced hacking methodologies, network penetration techniques, and exploit development—within a controlled, legal, and ethical framework.

This course is ideal for professionals looking to enhance their offensive security expertise, pursue careers in penetration testing, or meet cybersecurity compliance and red teaming requirements.

Objectives

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

- Understand the full penetration testing process, from reconnaissance to exploitation
- Discover and exploit vulnerabilities in Linux and Windows environments
- Develop and customize exploits, payloads, and privilege escalation techniques
- Practice lateral movement, persistence, and data exfiltration
- Prepare for and attempt the 24-hour OSCP certification exam

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 deep hands-on skills in ethical hacking and penetration testing
- Learn real-world techniques used by threat actors and red teams
- Prepare for the OSCP exam through guided labs and expert instruction
- Enhance your career profile with a globally respected certification
- Strengthen your ability to defend systems by learning how attackers operate

Target Audience

This program is designed for:

- Cybersecurity professionals and ethical hackers
- Penetration testers and red team specialists
- Security analysts and incident responders
- IT administrators seeking offensive security expertise
- Professionals preparing for the OSCP certification

Individual Benefits

Key competencies that will be developed include:

- Vulnerability assessment and exploitation
- Post-exploitation tactics and privilege escalation
- Active Directory enumeration and attacks
- Report writing and documentation of security findings
- Use of Kali Linux, Metasploit, and custom scripting

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Stronger internal red teaming and security assessment capabilities
- Improved preparedness for external penetration testing and compliance audits
- Enhanced technical security posture through advanced testing skills
- Reduced exposure to real-world cyber threats and exploits
- Better collaboration between offensive and defensive cybersecurity teams

Instructional Methodology

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

- Strategy Briefings – Ethical hacking frameworks, attack vectors, OSCP standards
- Case Studies – Real-world breaches, exploitation chains, post-mortems
- Labs – Hands-on penetration testing in dedicated virtual environments
- Peer Exchange – Red vs blue team knowledge sharing
- Tools – Kali Linux, Nmap, Netcat, Burp Suite, Metasploit, custom scripts

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: Foundations of Offensive Security

- Module 1: Introduction to Penetration Testing and OSCP Methodology (07:30 – 09:30) • Legal scope, testing phases, ethics, tools overview
- Module 2: Information Gathering and Enumeration (09:45 – 11:15) • DNS, whois, scanning, service discovery
- Module 3: Vulnerability Scanning and Analysis (11:30 – 01:00) • Nikto, Nmap, open ports and service vulnerabilities
- Module 4: Lab – Perform Enumeration on Target Machine (02:00 – 03:30) • Mapping services and attack surface

Day 2: Exploitation Techniques

- Module 5: Exploiting Linux Systems (07:30 – 09:30) • Buffer overflows, shellcode injection, privilege escalation
- Module 6: Exploiting Windows Systems (09:45 – 11:15) • SMB, RDP, PowerShell, UAC bypass
- Module 7: Client-Side Attacks and Web Exploitation (11:30 – 01:00) • XSS, SQLi, LFI, RCE techniques
- Module 8: Lab – Compromise and Escalate Privileges (02:00 – 03:30) • Real OSCP-style challenge

Day 3: Post-Exploitation and Lateral Movement

- Module 9: Maintaining Access and Credential Harvesting (07:30 – 09:30) • Meterpreter, backdoors, keyloggers
- Module 10: Active Directory Attacks and Pivoting (09:45 – 11:15) • Pass-the-hash, Kerberoasting, RDP hopping
- Module 11: Data Exfiltration and Covering Tracks (11:30 – 01:00) • File transfers, logs clearing, tunneling
- Module 12: Lab – AD Environment Exploitation (02:00 – 03:30) • Practice lateral movement and domain compromise

Day 4: Custom Exploits and Scripting

- Module 13: Writing and Modifying Exploits (07:30 – 09:30) • Exploit-db, shellcode crafting, buffer overflow demos
- Module 14: Bash, Python, and PowerShell Scripting (09:45 – 11:15) • Automating enumeration and exploits
- Module 15: AV/EDR Bypass Techniques (11:30 – 01:00) • Obfuscation, payload encoding, MSFvenom
- Module 16: Lab – Build and Deploy a Custom Exploit (02:00 – 03:30) • Realistic simulation

Day 5: OSCP Exam Preparation and Reporting

- Module 17: OSCP Exam Strategy and Format (07:30 – 09:30) • Lab overview, point allocation, reporting requirements
- Module 18: Writing the Penetration Test Report (09:45 – 11:15) • Documentation templates, sample reports
- Module 19: Final Capstone Lab – 24-Hour Style Challenge (11:30 – 01:00) • Simulated mini-exam
- Module 20: Wrap-Up – Review, Feedback & Certification Briefing (02:00 – 03:30) • Action plan, next steps for OSCP certification

Certification

Participants will receive a Certificate of Completion in OSCP (Offensive Security Certified Professional) Training, validating their readiness to attempt the official OSCP exam and their practical skills in ethical hacking and penetration testing.

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.

MAWA EVENTS

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

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

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