

OSSTMM Professional Security Tester – OPST

Course description

Management Summary

The OPST certification course participants are trained to be a responsible, capable and resourceful security tester. Within the training course they acquire the technical skills necessary for security testing and the business skills necessary for providing justification, efficiency (security project management and -controlling) and understanding contemporary business and security needs. The OPST training course is based on the Open Source Security Testing Methodology Manual (OSSTMM), the most widely used, peer-reviewed, comprehensive security testing methodology in existence. The OSSTMM provides a complete, effective and practicable methodology on performing security testing. The OSSTMM strongly focuses on the business justification of IT Security investments and is designed to be tailored into single modules to suit the corporate business objectives and industry-specific regulations.

Objective

The participants are prepared for the official OPST certification exam accredited by the Institute for Security and Open Methodologies (ISECOM) and the La Salle University in Barcelona.

Audience

- Security Testers
- Security Auditors
- Security Consultants
- Security Engineers

Course Contents

- Information Security Overview
- Information Security Sections and Modules
- (Communications-, Internet Technology-, Wireless-, Process- and Physical Security)
- What is the OSSTMM?
- International Best Practices and Standards (ISO17799, BS7799, SOX 404, Basel II, BSI)
- Security Testing Definition
- Why Security Testing is not just hacking
- OSSTMM Rules of Engagement, Ethical Hacking, Security Tester Job Profile
- Definition of System- and Network Security Testing Types
- How the OSSTMM works
- OSSTMM Practical Security Testing
- Security testing tools setup under Linux and Windows
- Testing of TCP, UDP, ICMP, IP, ARP and various application level protocols such as FTP, DNS, TFTP, BOOTP, HTTP, HTTPS etc.
- Development of a Linux attack server
- Open Source Security Tools (nmap, nessus, tcpdump etc.)
- Professional security tester resources, investigating new tools and trends
- Basic Security Tests from port scanning to vulnerability testing
- Document Grinding and Information Gathering
- Privacy
- Advanced Security Tests including remote Firewall-, Router- and IDS Testing

- Denial of Service Testing, Verification Testing, Application Testing, Social Engineering, VPN-, Router-, Firewall- and IDS Testing
- Analysis and verification of test results according the OSSTMM
- How to write test reports
- OSSTMM Business Security Testing
- Security Testing Project Management
- Basics of Risk Management
- Red Team, CERTs

Agenda

6 days

Monday to Friday 08.00-12.00, 13.30-18.00

Saturday official OPST exam 09.00-13.00

Prerequisites & Preparation

Profound experience in IT Security, solid basic knowledge of networks and TCP/IP as well as experience in command line under Linux and Windows is required.

2-3 weeks before the course starts the OPST course attendees receive the course handouts (OSSTMM Methodology, OPST Workbook, Tool guide, Link list) to read in.

Certification Exam

Official ISECOM accredited “CERTIFIED OSSTMM PROFESSIONAL SECURITY TESTER” exam. The exam consists of a 4 hour open book exam including hands-on skills assessment.

The OPST certification has been accredited for the Master in Information Technology Security at La Salle - URL University, Barcelona of the international La Salle educational network which includes Manhattan College in New York and La Salle University in Philadelphia, Pennsylvania. All OPST certificates carry both the ISECOM and La Salle logos and prestige.

Contact

Dreamlab Technologies Ltd, ISECOM Affiliate Switzerland
Nicolas Mayencourt, Official OPST / OPSA / OPSETrainer
Maito: education@dreamlab.net