

Zertifizierung zum OSSTMM Professional Security Tester



Das Open Source Security Testing Methodology Manual (OSSTMM) ist der internationale Standard für Security Tests. Die Schulung zum OPST vermittelt Ihnen die korrekte Anwendung von OSSTMM, die anwendbaren Test- und Angriffstechniken, sowie die dafür einsetzbaren Tools. Als OPST sind Sie in der Lage, Security Tests nach den im OSSTMM festgelegten ethischen Grundsätzen durchzuführen und dürfen sich zu Recht zur Elite der Sicherheitstester zählen. Die praktische Anwendung der erlernten Techniken bereitet Sie auf den Umgang mit täglich veränderten, komplexen Anforderungen bestens vor. Das Ziel der Schulung ist, die vermittelte Theorie durch Übungen und Beispiele in der Praxis zu festigen und die Prüfung bestätigt Ihre Qualifikation und Fähigkeit, Sicherheits-Audits OSSTMM-konform durchzuführen.

Der Kurs beinhaltet:

- Die Methodik der Security-Testing nach OSSTMM
- Welche Tools können angewandt werden
- Wie diese einzusetzen sind („know your tools“-Grundsatz)

Zielgruppen:

- Auditoren
- Sicherheits- und Penetrationstester (externe & Red Team)
- Sicherheitsberater
- Security Engineers
- Security Analysts
- System- und Netzwerkadministratoren
- Entwickler

Trainerinformation:

Lars Heidelberg ist seit acht Jahren im IT-Security Bereich aktiv. Durch seine Tätigkeit ist er mittlerweile mit einer Vielzahl verschiedener Betriebssysteme, Technologien und Infrastrukturen bestens vertraut und kann neben einem umfangreichen Erfahrungsschatz über 70 durchgeführte Sicherheitsaudits vorweisen.

Er hält sowohl die OPST- als auch OPSA-Zertifizierung und ist als OSSTMM-Trainer bei der ISECOM registriert.



OSSTMM Einführung, Implementierung und Passive Testing

Theorie

- Einleitung
- Setup und Regeln
- Was ist OPST?
- Unterschied zwischen OSSTMM Professional Security Analyst und OSSTMM Professional Security Tester
- OPST Lern Prozess
- Was ist OSSTMM?
- Zertifikate
- Ethik (Rules of Engagement)
- Vier Punkte Prozess
- Sicherheits-Testmethoden
- Fehler Typen

Praxis

- Competitive Intelligence Scouting
- Datenschutzüberprüfung
- Document Grinding

OSSTMM Verständnis & Tools für Penetrationstests

Theorie

- Risk Assessment Value (RAV) Überblick
- Test Error Risk Margin
- Öffentlich zugängliche Informationen
- OSSTMM Terminologie
- OSSTMM Struktur
- Überblick und Aufbau der Module
- Module im Detail
- Definitionsphase
- Informationsbeschaffung
- Interaktive Schutzmechanismen
- Compliance:
 - Gesetze
 - Regulation
 - Interne Richtlinien
- Sicherheitsmetrik
- Anwendung Risk Assessment Value
- Operationelle Sicherheit
- Schutzklassen
- Sicherheitslücken
- Gegebene Sicherheit

Praxis

- Netzwerk Überblick
- Port Scanning
- Service Enumeration
- System Identification

Fortgeschrittene Techniken Penetrationstest

Theorie

- Berechnung des RAVs
- OSSTMM Audit Berichte
- Nützliche Quellen

Praxis

- Fortgeschrittene System- und Infrastrukturidentifikation
- Datenflussanalyse und Fehleridentifikation
- Schwachstellensuche
- Schwachstellentests
- Exploitnutzung

Applikations- und Netzwerkmanipulation

Praxis

- Firewall Analyse
- IDS Tests
- Denial of Service Tests
- Web Applikationstests
- Netzwerkmanipulation und Sniffing
- Password cracking

Zusammenfassung und Training

Theorie

- Zusammenfassung OPST Kurs

Praxis

- Frage und Antwort





Voraussetzungen:

Die Teilnehmer sollten solide Kenntnisse im Netzwerkbereich vorweisen können. Weiterhin sind Erfahrungen im Umgang mit gängigen Betriebssystemen (Windows, BSD, Unix, Linux), vorzugsweise auf Kommandozeilenebene, vorteilhaft, aber nicht zwingend erforderlich. Für die praktischen Teile der Schulung benötigen die Teilnehmer ein eigens mitgebrachtes Notebook.

Information:

Ort:	Düsseldorf (Langenfeld)
Dauer:	Fünf Tage + 1/2 Tag Prüfung Mo. - Fr.: Unterricht Sa.: Prüfung
Trainer:	Lars Heidelberg (OPST und OPSA, zertifizierter OSSTMM Trainer)
Qualifikation:	OSSTMM Professional Security Tester
Preis:	2.900 EUR (zzgl. MwSt.)
Limitierung:	Sechs Plätze pro Kurs
Kontakt:	education@admeritia.de

Leistungsbeschreibung:

- 40 Stunden Unterricht & Training
- Vier Stunden OPST Zertifizierungsprüfung via Internet
- Aktuellste Version des Open Source Security Testing Methodology Manuals (OSSTMM)
- Zertifizierungsgebühr ISECOM/La Salle
- Zertifikat nach erfolgreichem Abschluss
- 24-stündiger Zugang zum Testlabor während des Seminars
- Pausengetränke frei (Kaffee, Tee, Mineralwasser)

Über uns:

Die adMERITia GmbH ist spezialisiert auf die operative standardbasierte Bemessung und Produktion der Informationssicherheit von Unternehmen und Organisationen aller Branchen und unterstützt diese bei der Implementierung sowie der Integration in vorhandene Prozesse.

Dabei testet, berät, realisiert und betreibt die adMERITia GmbH Informationssicherheit für ihre Kunden unterschiedlichster Größenordnungen mit integrelem Co-Competence-Ansatz. Im Bereich der Sicherheitstests, Auditierung und Bemessung orientiert sich die adMERITia GmbH an dem weltweit einzigen Standard für Information Security Testing, das „Open Source Security Testing Methodology Manual“ (OSSTMM) von der Herausgeberin „Institute for Security and Open Methodologies (ISECOM)“.

