

OSSTMM Professional Security Tester – OPST

Kursbeschreibung

Management Summary

Der OPST Zertifizierungskurs bereitet die Teilnehmer darauf vor verantwortungsvolle, fähige und kenntnisreiche Sicherheitstester zu werden. In dem Kurs werden die Teilnehmer die für die Sicherheitstest erforderlichen technischen Kompetenzen erwerben und ebenso die erforderlichen kaufmännischen Kompetenzen um die Rechtfertigung und die Effizienz (im Zusammenhang mit dem Management und der Überwachung von Sicherheitsprojekten) sicherzustellen; so werden die Teilnehmer befähigt die heutigen Anforderungen im geschäftlichen Bereich und im Sicherheitsbereich zu verstehen. Der OPST Kurs basiert auf dem Open Source Security Testing Methodology Manual (OSSTMM); es handelt sich dabei um die am weitesten verbreiteste, umfassendste und von Fachkollegen revidierte Methodologie für Sicherheitstests die zur Zeit existiert. OSSTMM ist eine vollständige, wirksame und praktisch durchführbare Methodologie für die Ausführung von Sicherheitstests. Die geschäftliche Rechtfertigung von Investitionen in die Datensicherheit wird bei OSSTMM vorrangig berücksichtigt; diese Methodologie ist so ausgerichtet dass sie in einzelne Modulen organisiert werden kann um die Anpassung an die spezifischen Geschäftsziele des Unternehmens und an branchenspezifische Vorschriften zu ermöglichen.

Ziel

Die Teilnehmer werden auf die offizielle OPST Zertifizierungsprüfung vorbereitet. Diese Prüfung wird vom Institute for Security and Open Methodologies (ISECOM) sowie von der La Salle Universität in Barcelona anerkannt.

Zielgruppe

- Sicherheitstester
- Sicherheitsrevisoren
- Sicherheitsberater
- Sicherheitsingenieure

Kursinhalte

- Übersicht über Datensicherheitsfragen
- Abschnitte und Module zum Thema Datensicherheit (Sicherheitsfragen beim Datenaustausch, bei der Internettechnologie, bei der kabellosen Datenübertragung sowie physische Sicherheit und Verarbeitungssicherheit)
- Was ist OSSTMM?
- Optimierte internationale Normen und Bräuche (ISO17799, BS7799, SOX 404, Basel II, BSI)
- Definition von Sicherheitstests
- Warum Sicherheitsprüfung nicht nur hacken beinhaltet?
- OSSTMM Verpflichtungen, Ethisches Hacken, Jobprofil des Sicherheitstesters
- Definition von Testtypen für System und Netzwerk
- Wie OSSTMM funktioniert
- OSSTMM Praktische Sicherheitstests
- Erstellung von Sicherheitstestwerkzeugen unter Linux und Windows
- Testen von TCP, UDP, ICMP, IP, ARP sowie von verschiedenen Protokollen auf der Anwendungsebene wie FTP, DNS, TFTP, BOOTP, HTTP, HTTPS usw.
- Entwicklung eines Linux Angriffsservers
- Freizugängliche Sicherheitswerkzeuge (nmap, nessus, tcpdump usw.)

- Professionelle Betriebsmittel für Sicherheitstester, Erforschung neuer Werkzeuge und Trends
- Elementare Sicherheitstests vom Abtasten von Anschlüssen bis zur Überprüfung von Anfälligkeiten
- Durchforsten von Dokumenten und Sammlung von Information
- Vertraulichkeit
- Fortgeschrittene Sicherheitstests inklusive der Überprüfung von Firewall, , Router und IDS
- Überprüfung der Angriffe auf Serverdienste, Nachprüfungen, Anwendungsüberprüfungen, Ausspähen persönlicher Daten, VPN-, Router-, Firewall- und IDS Überprüfungen
- Analyse und Verifikation von Testergebnissen nach dem OSSTMM
- Schreiben von Testberichten
- Überprüfung der geschäftlichen Sicherheit nach OSSTMM
- Management von Sicherheitstestprojekten
- Grundlagen des Risikomanagements
- Red Team, CERTs

Zeitplan

6 Tage
Montag bis Freitag 08.00 -12.00, 13.30 -18.00,
am Samstag offizielle OPST Prüfung 09.00 -13.00

Voraussetzungen und Vorbereitung

Gründliche Erfahrung im Bereich der IT Sicherheit, solide Grundkenntnisse im Bereich der Netzwerke und der Protokolle TCP/IP sowie Erfahrung in der Anwendung von Befehlen unter Windows und Linux Befehlen werden vorausgesetzt.

2-3 Wochen vor Kursbeginn erhalten die OPST Kursteilnehmer die Unterrichtsmaterialien (OSSTMM Methodologie, OPST Arbeitsbuch, Werkzeughandbuch, Liste der Links) zum Lesen.

Zertifizierungsprüfung

Die bestandenen Prüfung führt zum Titel "CERTIFIED OSSTMM PROFESSIONAL SECURITY TESTER" (übersetzt: Zertifizierter professioneller Sicherheitstester nach OSSTMM); diese Qualifikation wird von der ISECOM anerkannt. Die Prüfung dauert 4 Stunden und beinhaltet auch praktische Aufgaben; die Verwendung von Büchern ist gestattet.

Die OPST Zertifizierung wurde für das Master in Information Technology Security Diplom der La Salle – URL Universität in Barcelona anerkannt; diese Einrichtung gehört zum internationalen La Salle Bildungsnetzwerk zu dem auch der Manhattan College in New York und die La Salle University in Philadelphia, Pennsylvania gehören. Alle OPST Zertifikate tragen sowohl das ISECOM Logo als auch die La Salle Logos und das damit verbundene Prestige.

Kontakt

Dreamlab Technologies Ltd, ISECOM Affiliate Switzerland
Nicolas Mayencourt, Offizieller OPST / OPSA / OPSE Trainer
Maito: education@dreamlab.net