

Certificazione ISECOM OPSA

Executive Summary

L'**OSSTMM Professional Security Analyst (OPSA)** è la certificazione professionale ufficiale per l'Analisi della Sicurezza, in conformità alla metodologia OSSTMM dell'ISECOM (vedi riquadro). Il conseguimento della certificazione prevede un corso di taglio sia teorico che pratico, completo di esame finale su un ambiente di laboratorio dedicato.

Lo scopo della certificazione OPSA è di fornire una specializzazione multilivello di tipo teorico e pratico al professionista che opera nel settore della sicurezza ICT ed ha a che fare costantemente con i risultati delle relative verifiche, la gestione di Red Team, la selezione di fornitori in contesti di penetration testing and ethical hacking.

Audience

I seguenti profili professionali sono stati individuati in qualità di "Suggested Target Audience" da ISECOM e @ Mediaservice.net:

- Responsabili Sicurezza Informatica
- Responsabili Privacy, Qualità e Certificazione aziendale
- Consulenti esterni e team interni di Risk Analysis e Gestione del Rischio
- Security Auditor, ISO/BSI Lead Auditor
- Senior Security Tester, Senior Security Consultant
- Security Staff di NOC e SOC
- System, Network & Security Technical Administrator
- Tutti coloro che lavorano professionalmente nel campo della System & Network Security a livello di pianificazione, strategia, rischi.

Prerequisiti

- Media conoscenza della suite TCP/IP e dei suoi principali protocolli
- Esperienza nelle problematiche di base nella sicurezza dei sistemi *NIX e Microsoft Windows
- Conoscenza generica dell'installazione e della configurazione di software di verifica ed analisi della sicurezza (specificatamente su distribuzioni *NIX); dei sopraccitati software non è richiesta un'esperienza di base nell'utilizzo pratico
- Conoscenza e comprensione delle architetture di rete
- Conoscenza base dei principali servizi TCP/IP
- Conoscenza base dei sistemi per la sicurezza in rete: router, firewall, intrusion detection system
- È consigliato l'uso di un notebook per la durata del corso per meglio fruire dei contenuti e delle esercitazioni svolte in aula.

ISECOM

Institute for Security and Open Methodologies, fondata da Pete Herzog nel 2001 con una filosofia orientata all'open source, no profit e vendor independent.

Il suo obiettivo primario è la diffusione della consapevolezza della sicurezza.

www.isecom.org

OSSTMM

Open Source Security Testing Methodology Manual è la metodologia di riferimento per l'esecuzione e misurazione delle verifiche tecniche di sicurezza.

Di carattere open source, è organizzata su 5 canali:

- Human
- Physical
- Wireless
- Telecommunications
- Data Networks

Docenti

Il corso viene tenuto da professionisti che, all'interno del team di @ Mediaservice.net, hanno maturato anni di esperienza diretta. Il docente, inoltre, possiede le certificazioni OPST, OPSA, HHS ed è insegnante autorizzato da ISECOM.

Capacità e Competenze Acquisite

Al termine del corso l'allievo saprà padroneggiare le procedure di esecuzione dei test, comprenderne i risultati ed il loro significato, verificare la provenienza e la completezza dei dati ma soprattutto saprà gestire un team di sicurezza tramite la pianificazione e la gestione dei rischi come previsto dall'OSSTMM.

Programma

Il corso si articola su 4 giorni più 1 dedicato all'esame finale. Durante le giornate di corso verranno trattati i contenuti schematizzati di seguito:

Rules of Engagement: Comprendere come applicare e gestire le regole di ingaggio (Rules of Engagement).

Assessment: Apprendere le tecniche per analizzare e correlare gli elementi durante un test di sicurezza OSSTMM già dalla fase della loro delimitazione.

Logistics: Comprendere come individuare informazioni sulla sicurezza incomplete, falsificate o impropriamente classificate, basandosi su evidenze e Report di sicurezza.

Metrica: Apprendere le conoscenze necessarie per calcolare e misurare gli elementi di protezione e le contromisure secondo metodologia OSSTMM.

Correlation: Comprendere le tecniche per correlare le informazioni per discernere tra quelle legittimamente estrapolate da quelle identificate seguendo la ricerca di un dato campione.

Verification: Apprendere le competenze necessarie per identificare elementi non eleggibili a campione, informazioni pubbliche non previste come tali e classificare le fonti da cui sono state estrapolate.

Application: Comprendere come analizzare le contromisure in essere o la loro mancanza, relativamente a servizi, applicazioni e protocolli, basandosi sulle analisi di report e logs della verifica.

Reporting: apprendere le conoscenze per poter classificare le limitazioni di sicurezza per completare e certificare il report ufficiale STAR (Security Testing Audit Report).

Riferimenti e Partnership

@ Mediaservice.net, grazie alla sua decennale esperienza nel campo della sicurezza, può supportare in modo unico l'esecuzione di ogni progetto, basandosi su metodologie e standard internazionali riconosciuti, quali:

- ISO/IEC 27001
- OSSTMM
- OWASP
- ITIL
- COBIT

@ Mediaservice.net può vantare inoltre conoscenze acquisite attraverso partnership strategiche con le principali associazioni professionali e con i centri di competenza nazionali e internazionali.



Costi

Prezzo di listino 3.200 € + iva per partecipante

Sconti 5% se si effettua il pagamento almeno 10 giorni prima della scadenza delle iscrizioni
10% soci CLUSIT o ISACA Roma
15% Forze dell'Ordine

Compreso nel prezzo:

- aula attrezzata e dispense
- accesso all'ISECOM network per la durata del corso
- rilascio del Certificato di superamento riconosciuto dall'ISECOM e dall'Università La Salle di Barcellona
- un pasto e due coffee break al giorno