mediaservice.net
CORPORATE SECURITY & IMAGE

Propedutico ISECOM - OPST

Executive Summary

Il percorso formativo propedeutico al corso di certificazione OPST è il metodo più efficace per colmare eventuali lacune e prepararsi al meglio ad affrontare il successivo processo di certificazione.
Il percorso formativo completo è composto da 5 giornate ed è suddiviso in 2 moduli (**Base** ed **Intermedio**), relativamente di 2 e 3 giorni. Questa suddivisione permette di affrontare gli argomenti in modo progressivo, lasciando libero il discente di scegliere, conseguentemente alle proprie conoscenze pregresse sulla materia, se seguire entrambi i moduli o solo quello intermedio.

Audience

ISECOM e **@Mediaservice.net** hanno individuato quali target preferenziali per i contenuti di questo corso i seguenti profili professionali:

- Candidati al corso di certificazione **ISECOM - OPST** che vogliano o debbano colmare eventuali lacune.
- Amministratori di rete
- Security staff di NOC e SOC
- Consulenti IT Security
- Tutti coloro che, pur operando professionalmente nell' ambito della System & Network Security, devono colmare eventuali lacune nella loro preparazione di base.

Prerequisiti

- Dimestichezza nell'uso del personal computer
- Conoscenza base della lingua inglese
- Propensione ad affrontare tematiche tecnologiche

Tutti i partecipanti devono presentarsi al corso dotati di un notebook predisposto per ospitare un sistema Linux, sia esso virtualizzato o già installato su disco rigido, con la possibilità di aggiungere software durante il corso.

Capacità e competenze acquisite

Al termine del corso il discente sarà in grado di gestire il proprio sistema per l'esecuzione delle verifiche automatiche di sicurezza. Avrà inoltre ottenuto le conoscenze necessarie per poter usufruire al meglio dei contenuti del corso di certificazione OPST.

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.

OPST

OSSTMM Professional Security Tester è la certificazione professionale per apprendere la modalità per l'esecuzione ed il reporting di test di sicurezza conformi alla metodologia ISECOM - OSSTMM.

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, OPSE, HHST ed è insegnante autorizzato da ISECOM.

Programma Base (2 Giorni)

Fondamenti Linux: Apprendere come un sistema Linux interagisce con l'architettura hardware ed i principali metodi di gestione del sistema stesso in modalità grafica e tramite linea di comando.
Linux e sicurezza: Conoscere le dinamiche di gestione e manutenzione del sistema in ottica di sicurezza per preservare in modo appropriato tutte le evidenze raccolte durante le operazioni di verifica.
Fondamenti di rete: Comprendere le basi di funzionamento reale di reti LAN ed Internet e le loro principali implementazioni architetturali, apprendere i concetti di switching e di routing legati alla funzionalità di rete.
Analisi TCP/IP: Apprendere i dettagli operativi dei vari protocolli di trasporto della suite TCP/IP in ottica di funzionalità e sicurezza, comprendere le chiavi di lettura per l'interpretazione dei listati di rete.

Programma Intermedio (3 Giorni)

Tools di Sicurezza: Apprendere natura e funzionalità dei principali programmi Open Source utilizzati in ambito di network security, scegliendo i mezzi più appropriati per ottenere informazioni in base alle operazioni di sicurezza svolte.
Procedure di verifica base: Comprendere come utilizzare al meglio i programmi Open Source di sicurezza per completare le operazioni di verifica, sperimentando direttamente su sistemi di laboratorio gli effetti e i risultati dell'applicazione delle nozioni acquisite.
Utilizzo dei vulnerability scanner: Apprendere le nozioni di base sull' utilizzo e la preparazione dei tools Open Source per l'identificazione delle problematiche di sicurezza in modo automatizzato.
Approccio metodologico all'uso di Nessus: Apprendere, tramite l'applicativo Nessus, la gestione e la corretta esecuzione di "Vulnerability Assessment" dei sistemi e della rete LAN sui quali si opera quotidianamente.
Ottiche di sicurezza: Apprendere le linee guida conformi alle principali normative di sicurezza e alla legislazione nazionale.
Introduzione all'OSSTMM: Apprendere le corrette chiavi interpretative dell'approccio alla sicurezza secondo la metodologia **ISECOM - OSSTMM**, così da poter fruire efficacemente dei contenuti del manuale di riferimento.

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:

- PCI-DSS (QSA e ASV)
- 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.

OWASP The Open Web Application Security Project
ISECOM INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES
Clusit Associazione Italiana per la Sicurezza Informatica
UNINFO
PCI Security Standards Council

Costi

Prezzo di listino	1400 € (modulo intermedio) / 2150 € (corso completo) + iva per partecipante
Sconti	5% se si effettua il pagamento almeno 10 giorni prima della scadenza delle iscrizioni 10% soci CLUSIT, Forze dell'Ordine e Studenti Universitari

Compreso nel prezzo:

- aula attrezzata e dispense
- accesso al test network di @Mediaservice.net per la durata del corso
- un pasto e due coffee break al giorno
- attestato di frequenza.

mediaservice.net CORPORATE SECURITY & IMAGE

@Mediaservice.net S.r.l. con Socio Unico
Via Santorelli, 15 - 10095 Grugliasco (TO)
Tel +39 011-3272100 - Fax +39 011-3246497
info@mediaservice.net - **www.mediaservice.net**