mediaservice.net
CORPORATE SECURITY & IMAGE

Approccio metodologico a Nessus

Executive Summary

Il corso di formazione **Approccio Metodologico a Nessus** fornirà ai discenti le linee guida per la gestione e la corretta esecuzione di Vulnerability Assessment dei propri sistemi e della propria rete LAN. L'impostazione del metodo di lavoro seguirà le indicazioni procedurali legate alla metodologia **ISECOM - OSSTMM** per le verifiche di sicurezza, nell'accezione di ricerca e verifica delle vulnerabilità.
Al termine del corso è previsto il rilascio di un attestato di frequenza.

Audience

I seguenti profili professionali sono stati individuati in qualità di target preferenziali per questo corso:

- Amministratori di sistema / Amministratori di rete
- Responsabili Sicurezza Informatica
- Security Staff / Security Auditor / Security Consultant
- Sviluppatori con competenze sistemistiche
- Tutti coloro che operano professionalmente nel campo della System Network Security.

Prerequisiti

- Conoscenza media della suite TCP/IP e dei suoi principali protocolli
- Conoscenza base dei principali servizi TCP/IP
- Nozioni di architetture di rete e di sicurezza
- Conoscenza base dei sistemi per la sicurezza in rete: router, firewall, IDS (Intrusion Detection System).

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 partecipante sarà in grado di installare e posizionare correttamente un server Nessus sulla propria infrastruttura e di eseguire in maniera autonoma verifiche automatiche di sicurezza. Sarà inoltre in grado di razionalizzare i risultati emersi secondo le esigenze puntuali di reportistica.

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 (2 Giorni)

Il corso si articola su 2 giorni, suddivisi in sessioni teoriche durante la mattinata e pratiche durante il pomeriggio, con ausilio del laboratorio messo a disposizione da @Mediaservice.net. Durante le giornate di corso verranno trattati i contenuti schematizzati di seguito:

Giorno 1:

- **Contestualizzazione di un Vulnerability Assessment**
  Introduzione al concetto di Vulnerability Assessment e sua applicazione all'interno di un processo di gestione del livello di sicurezza desiderato.

- **Identificazione degli elementi di verifica**
  Come identificare le linee guida nella scelta degli elementi architetturali da inserire nel piano di verifica, relativo posizionamento dei Server Nessus sulle infrastrutture campione.

- **Configurazione e scelta Plug-in di Nessus**
  Panoramica dei principali moduli di verifica previsti dall'applicativo Nessus e linee guida di configurazione relativamente alle infrastrutture LAN/ Internet.

Giorno 2:

- **Precauzioni nell'uso di Nessus**
  Creazione di politiche di scansione finalizzate a tutelare la continuità operativa degli elementi oggetto d'analisi.

- **Sessione di Laboratorio**
  Esercitazione pratica sui sistemi target predisposti in laboratorio, applicando le tecniche precedentemente acquisite.

- **Analisi della reportistica prodotta**
  Analisi dei risultati emersi durante l'esercitazione di laboratorio, in ottica di riduzione dei margini d'errore, come ad esempio, falsi positivi e falsi negativi.

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.

Costi

Prezzo di listino	1.350 € + 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 materiale didattico del corso in formato digitale
- server di laboratorio remoti e virtuali
- 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**