mediaservice.net
CORPORATE SECURITY & IMAGE

Sicurezza delle reti

Executive Summary

L'obiettivo del corso consiste nella presentazione ai partecipanti di una panoramica sui principali vettori di attacco che normalmente vengono sfruttati dagli agenti di minaccia verso le infrastrutture IT.

Verranno inoltre presentati approfondimenti tecnici in grado di aumentare la percezione delle problematiche di sicurezza ed al tempo stesso saranno fornite delle linee guida per attuare contromisure tecnologiche con il fine di eliminare e/o mitigare le criticità esposte.

Alla fine del corso è previsto il rilascio di un attestato di frequenza.

Audience

- Amministratori di sistema
- Amministratori di rete
- Responsabili Sicurezza Informatica
- Security staff di NOC e SOC
- Security auditor
- Security consultant

Prerequisiti

Per la partecipazione al corso si prevedono dei requisiti minimi relativamente alle conoscenze tecniche dei partecipanti; in particolare si richiede la conoscenza dei seguenti argomenti:

- Media conoscenza 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).

Capacità e Competenze Acquisite

- Comprendere le principali tecniche di attacco e di elusione delle strumentazioni di sicurezza
- Conoscere i vettori di attacco normalmente sfruttati dagli agenti di minaccia
- Comprendere le evoluzioni tecnologiche strutturali e implementative delle infrastrutture IT in ottica di valutazione della sicurezza
- Apprendere le principali contromisure finalizzate a mitigare le criticità presentate

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.

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 (4 Giorni)

Il corso si articola su 4 giorni. Durante le giornate di corso verranno trattati i contenuti schematizzati di seguito:

Architetture di sicurezza
Analisi degli elementi di sicurezza base (firewall, intrusion detection/prevention system, antivirus, proxy, antispam) e delle potenziali criticità dovute all'assenza o al cattivo utilizzo di ciascuno di essi

Vettore di attacco IP
Introduzione alle principali tecniche utilizzate per verificare l'esposizione di una rete e individuare sistemi e servizi attivi (tecniche di finger printing, port scanning, service identification e version scanning)

Vettore di attacco WEB
Analisi delle principali minacce legate all'esposizione delle applicazioni web e disamina delle principali tecniche di elusione delle strumentazioni di sicurezza standard

Vettore di attacco Interno
Introduzione alle principali minacce che possono provenire da un vettore di attacco interno (ad esempio un dipendente infedele o un consulente esterno)

Vettore di attacco VoIP
Analisi dei principali standard proprietari VoIP (Cisco SCCP/Skinny, SIP, Skype) e introduzione dei principali attacchi mirati al disservizio, all'intercettazione e alla falsificazione del traffico voce (tecniche di ARP Spoofing e network sniffing)

Vettori di attacco non convenzionali
Introduzione ad alcuni vettori di attacco che normalmente non vengono presi in considerazione, quali: Servizi di accesso remoto RAS, Centralini telefonici, Linee ISDN, Accessi APN, Blackberry

Vettore di attacco wireless
Introduzione alle principali criticità legate all'adozione delle tecnologie wireless: Wi-Fi, Bluetooth e RFID

Gestione dei log e correlazione
Analisi delle tecniche relative all'attivazione ed al *fine tuning* sui diversi sistemi e dispositivi di logging (sistema operativo, web server, IDS)

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	2.300 € + 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
- rilascio attestato di frequenza nominale
- un pasto e due coffee break al giorno

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**