Ethical Hacking e Penetration Test: dalla teoria alla pratica

La sicurezza informatica non può risolversi solo nella progettazione ed ingegnerizzazione di un'architettura di rete ed applicativa, basata sul principio meglio conosciuto come "Sicurezza Difensiva". Questo modo di procedere rappresenta una forte limitazione, producendo a volte danni economici e d'immagine, quali: furto di carte di credito furto di dati riservati violazione di sistemi web, scada, rete, ecc. spionaggio industriale, governativo o militare "Malware Banking" "Ransom Malware". che non hanno risparmiato grandi realtà come Sony, Yahoo,™ Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri sistemi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime.Unire la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta una necessità irrinunciabile.

Agenda (5 giorni)

Associazioni, risorse e documentazione utili ad un Penetration Tester.

Metodologia ed analisi di tipo "Black-Box"/"White Box".

"Modus Operandi" e l'importanza del pensiero "out-of-the-box".

La distribuzione Linux BackTrack: concetti di base, architettura generale e panoramica dei principali tools installati.

Altre distribuzioni Linux utili ad un Penetration Tester.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Attacchi di reti di tipo M.I.T.M.

Buffer Overflow.

Vulnerabilità delle applicazioni web.

Password / Hash Cracking.

V.A., Exploitation e Post-Exploitation.

Cenni al funzionamento ed evasione di programmi Antivirus.

Indicazioni per la scrittura di un report finale di un Penetration Test.

Obiettivi

Alla fine del corso i partecipanti acquisiscono tecniche e metodologie utilizzate durante una attività di Penetration Test di applicativi, rete e sistemi e sono in grado di realizzare in autonomia i Penetration Test.

Destinatari e Prerequisiti

A chi è rivolto

Personale che si occupa della verifica della sicurezza di applicativi e sistemi, IT Security Engineer, responsabili della sicurezza IT.

Prerequisiti

Conoscenze di base dei concetti relativi al funzionamento di applicativi e sistemi e di rete. Conoscenze di base delle principali problematiche della IT security.

Iscrizione

Quota di Iscrizione: 3.490,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com