Ethical Hacking e Penetration Test di Applicativi Web

Le applicazioni web rappresentano il vettore d'attacco più utilizzato da parte di criminali informatici. I motivi sono molteplici fra cui:

- enorme diffusione
- notevole superficie d'attacco
- scarsa attenzione in fase di progettazione agli aspetti di sicurezza.

Tutto questo ha portato anche alcune grandi realtà come Sony, Yahoo, Apache, ecc. a scontrarsi con fenomeni quali:

- furto di dati riservati e di carte di credito
- *defacement* di siti Web
- spionaggio industriale
- utilizzo di siti web compromessi per diffondere *Malware* e creare *Botnet*
- aumento del "*Ransom Malware*".

Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri applicativi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime. Unire così la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta ormai una necessità irrinunciabile. Saranno affrontate anche tematiche di "raccolta delle informazioni" ("Information Gathering") e tecniche e tools di cracking di password e hash. Sono previste, molte esercitazioni tratte da casi reali.

Agenda (3 giorni)

LABORATORIO

Associazioni, risorse e documentazione sulla sicurezza delle applicazioni web.

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 al Security Assessment di applicativi web.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Password/Hash Cracking.

Vulnerabilità delle applicazioni web, evasione di WAF e contromisure.

Laboratorio ("Capture The Flag!").

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

Obiettivi

Illustrare le principali e più diffuse vulnerabilità delle applicazioni web, nonché i più comuni errori nella scrittura di un applicativo web dal punto di vista della sicurezza.
Analizzare gli attuali attacchi client-side e server-side.

Destinatari

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

Reiss Romoli 2015

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.

Quota di iscrizione	Informazioni
€ 2.060,00 (+ IVA) *(Comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione).*	Segreteria Corsi – Reiss Romoli s.r.l. tel 0862 452401 - fax 0862 028308 corsi@ssgrr.com

Reiss Romoli 2015