Hacking e Sicurezza - Livello avanzato

Praticare attacchi avanzati per difendersi meglio

A distanza

5 giorni (35 Ore)

Open : 3.590,00 € +IVA
Packaged in azienda : 8.280,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.25

Non è un caso che alcune delle società di sicurezza informatica di maggior successo abbiano degli **hacker** tra i propri dipendenti. Le persone più capaci di identificare i difetti in un sistema IT sono infatti proprio quelle che sono in grado di attaccarlo.

È su questa logica che è stata pensata questa formazione, che propone agli specialisti informatici coinvolti nella protezione di un sistema IT di **operare come degli hacker** per individuarne le possibili vulnerabilità, comprese le più recenti e implementare misure per correggerle.

A chi è rivolto

Per chi

- Consulenti per la sicurezza
- Ingegneri/Tecnici
- Amministratori di sistema/rete
- Sviluppatori

Prerequisiti

- Conoscenze base di sicurezza informatica o di haking
- La conoscenza di Linux è un plus

Programma

1 - Introduzione

- Richiami su TCP/IP

2 - Introduzione

- Vocabolario
- Database delle vulnerabilità

3 - Raccolta di informazioni

- Informazioni pubbliche
- Motori di ricerca
- Inchiesta attiva

4 - Scansione e presa dell'impronta

- Enumerazione degli host
- Scansione delle porte
- Fingerprint del sistema operativo
- Identificazione dei servizi

5 - Vulnerabilità informatiche

- Vulnerabilità dei protocolli di rete
- Vulnerabilità delle applicazioni
- Vulnerabilità del web
- Sfruttamento delle vulnerabilità
- Mantenimento dell'accesso ad un host

6 - Laboratorio pratico

- Implementazione di una strategia di attacco su un laboratorio creato appositamente per l'addestramento
- Lancio dell'attacco e tentativo di sfruttamento
- cattura la bandiera
- Studio di opportune contromisure

7 – Nuove metodologie di attacco

- Chi sono i nuovi hacker e quali risorse hanno a disposizione
- Quali sono gli obbiettivi dei nuovi attacchi
- Problemi legali e danni economici causati alle aziende
- Analisi di un attacco moderno

Obiettivi del corso

- Capire come organizzare un controllo di sicurezza e sapere dove cercare informazioni affidabili
- Identificare i "punti deboli" dei componenti del sistema IT
- Avere le competenze tecniche necessarie per eseguire diversi attacchi e quindi comprenderne le sottigliezze
- Essere in grado di proteggere il sistema IT con un sistema di opportune contromisure

Esercitazioni

- Formazione molto pratica: l'**80%** del tempo di formazione è dedicato a **workshop** pratici
- Un approccio pratico: una panoramica delle tecniche utilizzate nell'ambito delle intrusioni nelle reti aziendali, integrata da un workshop in un **laboratorio** appositamente creato per la formazione
- Ogni presentazione tecnica è accompagnata da procedure di sicurezza applicabili sotto diverse architetture
- Una pedagogia basata sulla condivisione di **esperienze** e buone pratiche da parte di un esperto di sicurezza

Date 2026

Ultimi posti Edizione garantita

dal 17 giu al 26 giu
- dal 17 giu al 19 giu
- dal 25 giu al 26 giu

dal 16 nov al 24 nov
- dal 16 nov al 18 nov
- dal 23 nov al 24 nov