Hacking e Sicurezza - I fondamenti

Conoscere i diversi tipi di attacchi di sistema per proteggersi meglio

A distanza

4 giorni (28 Ore)

Open : 2.490,00 € +IVA
Packaged in azienda : 7.250,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.24

L'origine dell'**hacking** risale alla metà degli anni '50, quando i primi computer disponibili nelle università americane caddero rapidamente preda di studenti desiderosi di appropriarsi dei sistemi. Nacquero così gli hacker che, approfittando dell'avvento di Internet decenni dopo, continuarono a prendere di mira sistemi informatici sempre più sofisticati, arrivando anche ad hackerare quelli governativi. Per far fronte a queste minacce in costante aumento, i CIO si aspettano che ingegneri e tecnici siano in grado di **proteggere efficacemente i sistemi IT** delle loro organizzazioni. Lo scopo di questo corso è proprio quello di **fornire loro le competenze e le conoscenze** che consentiranno loro di svolgere questa missione.

A chi è rivolto

Per chi

- Consulenti per la sicurezza
- Ingegneri/Tecnici
- Amministratori di sistema/rete
- Chiunque sia interessato alla pratica della sicurezza

Prerequisiti

Conoscenza base di Windows o Linux

Programma

1 – Introduzione

- Ethical Hacking
- Modialità di esecuzione e rischi legali
- Obbiettivi
- Schema di un attacco tradizionale

2 – Raccolta informazioni

- Metodologie di raccolta delle informazioni
- Informazioni pubbliche
- Individuare i sistemi di destinazione
- Enumerazione dei servizi attivi
- Spoofing, Social Engineering, Phishing e Spear Phishing

3 - Attacchi a distanza

- Intrusione remota dei client sfruttando le vulnerabilità dei servizi o assumendo il controllo mediante Trojan
- Brute force attack e altri attacchi ai sistemi di autenticazione
- Vulnerability Assessment
- Exploit e Proof of Concept

3 - Attacchi ai sistemi

- Attacco locale
- Cracking delle password
- Raccolta informazioni
- Privilege escalation

4 - Messa in sicurezza del sistema

- Strumenti di base per garantire la sicurezza minima del tuo sistema informativo
- Hardening dei sistemi
- Crittografia
- Rilevamento di attività anomale
- Firewall/VPN
- Backup dei sistemi
- Introduzione ad altri sistemi di sicurezza

Obiettivi del corso

- Capire come è possibile entrare fraudolentemente in un sistema remoto
- Conoscere quali meccanismi sono coinvolti in caso di attacchi al sistema
- Acquisire le competenze necessarie per impostare un sistema globale che garantisca la sicurezza dei sistemi

Esercitazioni

- Formazione molto **pratica**: il 70% del tempo di formazione è dedicato a workshop
- Particolare enfasi è posta sulla pratica delle **diverse forme** di attacchi esistenti
- Ogni presentazione tecnica è accompagnata da procedure di sicurezza applicabili sotto diverse architetture (Windows e Linux).
- **Feedback** dei professionisti della sicurezza.

Date 2026

Ultimi posti Edizione garantita

dal 9 apr al 17 apr
- dal 9 apr al 10 apr
- dal 16 apr al 17 apr

dal 3 dic al 11 dic
- dal 3 dic al 4 dic
- dal 10 dic al 11 dic