Hacking e Sicurezza - Livello esperto

Proteggere un sistema informativo passo dopo passo

A distanza

5 giorni (35 Ore)

Open : 3.640,00 € +IVA
Packaged in azienda : 8.380,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.26

Le notizie ci ricordano quasi quotidianamente che esistono **intrusioni** nei sistemi informatici pubblici o privati. E molto spesso le aziende che ne sono vittime vengono additate per non essere state in grado di proteggere adeguatamente i propri dati. Se il rischio zero non esiste, sembra quasi ovvio che testando regolarmente il proprio sistema IT, i team incaricati di garantire la sicurezza potrebbero rilevare nuovi difetti o minacce e quindi implementare contromisure ad hoc...

Durante questa formazione molto pratica che consiste di una serie di workshop scanditi da scambi di esperienze, i partecipanti avranno a disposizione **un ambiente tecnico complesso che potranno attaccare a proprio piacimento**, imparando quindi a proteggerlo come un sistema end-to-end.

A chi è rivolto

Per chi

- Sviluppatori
- Amministratori di sistema/rete
- Ingegnere della sicurezza
- Consulente per la sicurezza

Prerequisiti

Conoscenze base di sicurezza informatica o di hacking

Programma

1 - Introduzione

- Definizione di hacking
- Panoramica 2022/2023
- Repository di sicurezza (NVD, ENISA)
- I diversi tipi di hacker
- I diversi tipi di attacchi
- I diversi strumenti utilizzati dall'hacker
- Schema di un attacco informatico
- Analisi di un moderno attacco informatico

2 - Hacking

- Scansione rete/porte/versioni
- Sfruttamento di vulnerabilità
- Elevazione del privilegio

- Attivazione di una backdoor
- Recupero di informazioni, dizionario delle password + Bruteforce
- Payload con Metasploit
- Man In The Middle (MITIM)
- VLAN Hopping (yersinia e/o tabella overflow)

3 - I pilastri della sicurezza

- Confidenzialità
- Integrità
- Disponibilità
- Tracciabilità

4 - I principi fondamentali della sicurezza

- Autenticazione
- Bisogno di sapere
- Minimo privilegio
- Non ripudio
- Defense in depth

5 - Sicurezza fisica

- Concetto di sicurezza fisica
- Corrispondenza dei concetti con i principi precedenti

6 - Mettere in sicurezza la rete

- Sicurezza di livello 2: sicurezza delle porte, VLAN, SSH, DHCP snooping, difesa da arp MITM, sicurezza per DTP, CDP, VTP, STP.
- Sicurezza di livello 3: IPSec, firewall, UTM e Next Generation Firewall
- Sicurezza di Livello 7: Application Firewall
- Intrusion Detection & Prevention (IDS/IPS)
- Proxy, Reverse Proxy, Web Application Firewall (WAF)
- SASE: Secure Access Service Edge (SD-WAN, ZTNA, FWaaS, ecc.)
- Integrazione con End Point Protection

7 - Messa in sicurezza dei sistemi

- Hardening di Linux
- Hardening di Windows
- Host-based Intrusion Detection System (HIDS)
- PAM: Privileged Access Management

8 - Proteggere i dati

- Crittografia
- DLP: Data Lost Protection
- Backup Immutable e Off-site

8 - Vigilanza sulla sicurezza

- SoC: Security Operation Center
- MDR: Managed Detection and Response
- SIEM: Security Information Management System
- XDR: eXtended Detection and Response

9 - Risposta agli incidenti

- Ripeti gli attacchi

- Analizza i log
- Implementa contromisure specifiche
- Formazione e Security Awareness

Obiettivi del corso

- Sapere come proteggere il proprio sistema informativo
- Comprendere come proteggere tutti gli aspetti di un sistema IT: rete, applicazioni e Web
- Acquisire le conoscenze e le competenze necessarie per rilevare vulnerabilità e attuare contromisure
- Saper reagire correttamente in caso di attacco
- Essere in grado di applicare le competenze tecniche acquisite nell'ambito di un intervento professionale

Esercitazioni

- **Rassegna** delle principali tecniche e strumenti di difesa utilizzati
- L'uso di strumenti di analisi e automazione degli attacchi
- Formazione molto **pratica**: la maggior parte della formazione si concentrerà su contromisure tecniche concrete che ognuno può implementare nella propria azienda.
- Il contributo di consulenti **esperti** negli audit tecnici di sicurezza

Date 2026

Ultimi posti Edizione garantita

dal 13 mag al 22 mag
- dal 13 mag al 15 mag
- dal 21 mag al 22 mag

dal 21 set al 29 set
- dal 21 set al 23 set
- dal 28 set al 29 set