Sicurezza dei sistemi e delle reti - I fondamenti

Proteggersi dagli attacchi e garantire l'affidabilità dei propri dati

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.23

Con Internet le reti sono ora aperte e di conseguenza molto più esposte ad attacchi virali o ad altri atti di pirateria. È diventato quindi essenziale sapere come affrontare questi diversi rischi al fine di proteggere i dati dell'azienda e garantire l'integrità e il corretto funzionamento del suo sistema informativo.

Durante questa formazione i partecipanti scopriranno i **principali concetti** relativi alla sicurezza della rete e **gli strumenti** per proteggere le infrastrutture aziendali.

A chi è rivolto

Per chi

- Responsabili IT
- Amministratori di rete
- Tecnici
- Webmaster
- Responsabili della sicurezza informatica

Prerequisiti

È necessaria una buona conoscenza generale delle reti e dei sistemi operativi comuni

Programma

1 - L'ambiente

- Il perimetro (reti, sistemi operativi, applicazioni)
- Gli attori (hacker, responsabili della sicurezza, revisori, fornitori ed editori)
- La vecchia tecnologia
- Organi ufficiali

2 - Metodologie di attacco

- Scenari di attacco intrusione, DDoS, ecc.
- Attacchi ai protocolli di rete
- Debolezze dei servizi: Web, VoIP, Messaging
- Il codice vandalico: virus, worm, cavalli di Troia, ransomware/crypto locker
- Nuove metodologie di attacco

3 - Sicurezza degli accessi, Firewall, WAF, Proxy, NAC

- Accesso stazione alle reti aziendali, 802.1x, NAC
- I diversi tipi di firewall
- Regole di filtro
- Regole di NAT
- L'implementazione di una zona demilitarizzata (DMZ)
- Rilevamento e monitoraggio con IDS
- Integrazione di un firewall nella rete aziendale
- Gestione e analisi dei log

4 - Sicurezza dei sistemi operativi

- Hardening di Windows
- Hardening di Linux
- Hardening dei mobile: IOS/Android

5 - Sicurezza applicativa con esempi di architetture

- Server Web e client
- Messaggistica elettronica
- VoIP IP PBX e telefoni

6 - Sicurezza degli scambi, crittografia

- Lo scopo della crittografia e le funzioni di base
- Algoritmi simmetrici
- Algoritmi asimmetrici
- Algoritmi hash
- Metodi di autenticazione (pap, chap, Kerberos)
- L'HMAC e la firma elettronica
- Certificati e PKI
- Protocolli IPSEC SSL
- VPN site-to-site e mobile, Zero Trust Network Access (ZTNA)

Obiettivi del corso

- Essere in grado di valutare i rischi interni ed esterni associati all'uso di Internet
- Comprendere i meccanismi che garantiscono l'affidabilità e la riservatezza dei dati grazie alle varie soluzioni sicure
- Avere un primo approccio ai concetti tecnici, per comprendere la sicurezza dei sistemi informativi

Esercitazioni

- L\'assimilazione di una **metodologia** per l\'implementazione della sicurezza di rete ad alte prestazioni.
- Una formazione scandita da una pedagogia basata su **esempi** concreti.
- **Consigli** dei consulenti esperti di sicurezza IT.

Date 2026

Ultimi posti Edizione garantita

dal 16 mar al 24 mar
- dal 16 mar al 17 mar
- dal 23 mar al 24 mar

dal 2 nov al 10 nov
- dal 2 nov al 3 nov
- dal 9 nov al 10 nov