CYBERSÉCURITÉ : SOLUTIONS TECHNIQUES ET ARCHITECTURES

IRE68 | 3 jours (21h) 1 695,00 €HT

Objectifs

Acquérir la maîtrise globale de la sécurisation d'un réseau et de son interconnexion avec des réseaux extérieurs • Disposer des techniques permettant de mettre en place la cybersécurité : gestion des identités et des accès, interconnexion, cryptographie, systèmes, applicatifs, surveillance et défense

Profil Stagiaire(s)

administrateurs systèmes et réseaux, responsables de sécurité, responsables informatiques et chefs de projets inter-intranet

Pré-requis

connaissance préalable des réseaux internet/intranet

Profil Animateur(s)

consultant spécialisé dans la sécurité des SI

PROGRAMME

Introduction et rappel sur les aspects juridiques
Panorama général de la Sécurité des SI
Respect de la vie privée / CNIL
Répression des délits en matière de SI
Responsabilités des dirigeants
Accès internet, charte et enregistrements de journaux

Se protéger avec la bonne cryptographie : principes et mise en oeuvre
Principes de bases
Fondements mathématiques
Algorithmes et résistance
Découverte d'algorithmes
État de l'art
TP : tester la solidité d'un mot de passe

Élaborer une politique d'authentification
L'authentification n'est pas que pour les utilisateurs
Méthodes utilisées par les différents OS
Comment Mimikatz débusque les mauvais choix de Microsoft
Authentification forte
Certificats, PKI, SSO la solution ultime ?

Protéger l'accès au réseau
Problématique d'un accès sur Ethernet
Les insuffisances d'ethernet et d'IP v4
Authentifier les utilisateurs et les machines
Les éléments du NAC (Network Access Control)

Concevoir une interconnexion sécurisée
Firewalls et DMZ
Adapter l'architecture au niveau de sécurité souhaité
Segmenter son réseau pour le protéger
La défense en profondeur
TP : Wireshark, Nmap, Netcat

Contactez-nous

Conseiller formation
09 88 66 10 00
inscriptions@demos.fr

Nos sessions

15 - 17 sept. 2021 : Paris / A Distance

17 - 19 nov. 2021 : Paris / A Distance

CYBERSÉCURITÉ : SOLUTIONS TECHNIQUES ET ARCHITECTURES

IRE68 | 3 jours (21h) 1 695,00 €HT

Sécuriser les accès distants
Vpn et sécurité des liaisons
Les vpn SSL (OpenVPN)
IpSec technologies et implémentations
Routage et authentification dans un contexte d'accès distant

Administrer de façon sécurisée
Infrastructure
Authentifier c'est aussi responsabiliser
Le point sur les outils courants Rdp, vnc, telnet, ssh

Sécuriser la navigation internet
DNS : un protocole fondamental et sensible
Recommandations pour les principaux navigateurs
Le maillon faible : sensibiliser les utilisateurs en quelques bonnes pratiques
Le proxy : un besoin réglementaire et une solution technique

Protéger ses serveurs applicatifs et Web
Les certificats : gestion et mise en œuvre
Reverse proxy
TP : Metasploit

Durcir les systèmes d'exploitation
Sécurité du poste de travail
Windows 10
Microsoft Active Directory
Linux

Virtualisation et sécurité
Fonctionnalité de la virtualisation et sécurité
Impacts sur les critères DICT
Modification de la perception des réseaux (Ethernet, IP, …)
Recommandations pratiques pour la configuration de Vmware ESX

Architecture d'une messagerie
SMTP, un protocole peu sécurisé
La messagerie reste un vecteur d'attaque très important
Les bonnes pratiques utilisateurs sont déterminantes
Segmentation réseau mais aussi applicative, dns, opérateurs télécom

Surveiller et défendre en exploitant les logs et journaux des systèmes
Le protocole Netflow
SysLog Serveur
Exploitations des logs : les outils d'analyse et de corrélation
Quelques outils : Splunk, SEC
Sondes IDS, IPS, boîtiers dédiés (appliance)
Quelques outils : Snort, OSSEC, Prelude IDS

Se préparer à répondre aux crises
Les dispositifs PCA et PRA

CYBERSÉCURITÉ : SOLUTIONS TECHNIQUES ET ARCHITECTURES

IRE68 | 3 jours (21h) 1 695,00 €HT

Méthode pédagogique

Cette formation sécurité réseaux comporte les ateliers pratiques suivants
- Mise en œuvre d'éléments de la sécurité du poste de travail
- Mise en œuvre de la sécurité IP
- Mise en œuvre d'un VPN
- Mise en évidence des failles de sécurité protocolaire (http, SMTP, POP3, FTP, ..) par analyse de trames sous Wireshark

Pour les formations "A distance", elles sont réalisées avec un outil de visioconférence de type Teams ou Zoom selon les cas, permettant au formateur d'adapter sa pédagogie.
Retrouvez sur notre site internet toutes les précisions sur les sessions à distance ou les classes virtuelles.

Moyens pédagogiques et techniques de mise en œuvre

Nos formateurs DEMOS sont recrutés conformément aux spécifications mentionnées pour chaque formation. Ce sont des professionnels en activité et/ou des experts dans leur domaine.
Ils utilisent des méthodes et outils appropriés aux formations qu'ils dispensent et adaptent leur pédagogie au public accueilli.
Par ailleurs, nos centres de formation DEMOS sont tous équipés :

- Salles de formation lumineuses, spacieuses, design, ergonomiques, mobiles et équipées d'écrans plasma, de PC portables/fixes si nécessaire à la formation suivie.
- Accès au wifi haut débit sur l'ensemble des lieux
- Espace de co-learning et webcorners
- Cafés, collations et rafraîchissement sont offerts

Et tous sont accessibles aux personnes à mobilité réduite

Le dispositif de suivi et d'évaluation

Pour assurer un suivi individuel, Demos a mis en place 2 types d'évaluation :

- Des évaluations des acquis en cours et en fin de formation

Elles peuvent être faites de différente manière selon le contenu de la formation suivie :
Quiz, exercice pratique, étude de cas, jeu de rôles, mise en situation, soutenance devant un jury pour les formations à finalité certifiante.

- Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

En complément

Après cette formation vous pourrez suivre :

- Évaluer votre Niveau de Sécurité : Tests d'Intrusions et Audit Technique