LES ESSENTIELS DE LA CYBERSÉCURITÉ

Durée	5 jours	Référence Formation	4-IT-CYBA

Objectifs

Présentation des Cyber-menaces actuelles et sites de référence sur la cybersécurité
Directives et exigences de conformité
Cyber rôles nécessaires à la conception de systèmes sûrs
Cycle des attaques processus de gestion des risques
Stratégies optimales pour sécuriser le réseau d'entreprise
Zones de sécurité et solutions standards de protection

Participants

Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité

Pré-requis

Connaissances en réseaux TCP/IP

PROGRAMME

・Le champ de bataille
La croissance d'Internet dans le monde entier
Principes et objectifs de sécurité
Terminologie des menaces et de l'exposition
Documents et procédures de gestion des risques
・Structure de l'Internet et TCP/IP
Normes de conformité juridique
Internet Leadership IANA
Modèle TCP/IP
・Évaluation de la vulnérabilité et outils
Vulnérabilités et exploits
Outils d'évaluation de la vulnérabilité
Techniques d'attaques avancées, outils et préventions
・Sensibilisation à la cyber sécurité
Ingénierie sociale : Objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
Sensibilisation à la cyber sécurité : Politiques et procédures
・Cyber-attaques : Footprinting et scannage
Footprinting
Identification du réseau cible et sa portée
Techniques de scannage de port
・Cyberattaques : Effraction
Attaque des mots de passe, escalade des privilèges
Authentification et décodage du mot de passe
・Cyberattaques : Porte dérobée et cheval de Troie (Backdoor and Trojans)
Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
Communications secrètes
Logiciel anti-espion
Pratiques de lutte contre les logiciels malveillants
・Évaluation et gestion des risques cybernétiques
Actifs protégés : CIA Triad

CAP ÉLAN FORMATION - Marseille – Toulon
www.capelanformation.fr - Tél : 04.86.01.20.50
Mail : contact@capelanformation.fr
Organisme enregistré sous le N° 76 34 0908834
[version 2022]

Processus de détermination de la menace
Catégories de vulnérabilités
Actifs de l'entreprise vs risques
・Gestion des politiques de sécurité
Politique de sécurité
Références de politiques
・Sécurisation des serveurs et des hôtes
Types d'hôtes
Directives de configuration générale et correctifs de sécurité
Renforcement des serveurs et périphériques réseau
Renforcement de l'accès sans fil et sécurité des VLAN
・Sécurisation des communications
Application de la cryptographie au modèle OSI
Tunnels et sécurisation des services
・Authentification et solutions de chiffrement
Authentification par mot de passe de systèmes de chiffrage
Fonctions de hachage
Avantages cryptographiques de Kerberos
Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques
・Pare-feu et dispositifs de pointe
Intégration de la sécurité générale
Prévention et détection d'intrusion et défense en profondeur
Journalisation
・Analyse criminalistique
Gestion des incidents
Réaction à l'incident de sécurité
・Reprise et continuité d'activité
Types de catastrophes et Plan de reprise d'activité (PRA)
Haute disponibilité
Documentation de collecte de données
Plan de Reprise d'Activité et Plan de Continuité d'Activité
・Cyber-révolution
Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?
・LABS
Lab1: Installation du lab
Lab 2 : Comprendre TCP/IP
Lab 3 : Evaluation de la vulnérabilité
Lab 4 : Sensibilisation à la cybersécurité
Lab 5 : Scannage
Lab 6 : Cyber-attaques et mots de passe
Lab 7 : Cyber-attaques et portes dérobées
Lab 8 : Évaluation des risques
Lab 9 : Stratégies de sécurité
Lab 10 : Sécurité hôte
Lab 11 : Communications secrètes
Lab 12 : Authentification et cryptographie
Lab 13 : Snort IDS
Lab 14 : Analyse criminalistique
Lab 15 : Plan de continuité des affaires

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.