

INSTALLER ET ADMINISTRER DES SOLUTIONS DE SÉCURITÉ

Durée	19 jours	Référence Formation	4-IT-IASS
--------------	-----------------	----------------------------	------------------

Objectifs

Installation et administration de solutions sécurité

Participants

Toute personne en charge de cybersécurité

Pré-requis

Pas de prérequis spécifique à cette formation

Moyens pédagogiques

Réflexion de groupe et apports théoriques du formateur

Travail d'échange avec les participants sous forme de réunion-discussion

Utilisation de cas concrets issus de l'expérience professionnelle

Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.

Remise d'un support de cours.

PROGRAMME

Introduction aux Critères Communs

- Projet Critères Communs, ses origines à son organisation actuelle
- Acteurs clés et sa déclinaison dans le schéma français géré par l'ANSSI
- Historique des principes de certification, du projet CC, des normes et des accords internationaux
- Philosophie de l'évaluation d'un produit et la terminologie CC
- Organisation du schéma français et les concepts de cible de sécurité

Remise à niveau Linux

- Système de fichiers
- Commandes de base
- Gestion des fichiers et répertoires
- Permissions Unix
- Gestion des entrées/sorties
- Gestion des tâches
- Edition de texte VI/VIM
- Archivage et la compression
- Authentification et comptes utilisateurs
- Shell
- Création et l'application de patch sur du code source
- Installation de packages
- Modules de sécurité
- Sécurisation des services
- Journalisation
- Pare-feu local

Conception, implémentation et sécurisation d'une infrastructure Windows Server

- Planifier et mettre en œuvre une infrastructure de déploiement serveur

CAP ÉLAN FORMATION

www.capelanformation.fr - Tél : 04.86.01.20.50

Mail : contact@capelanformation.fr

Organisme enregistré sous le N° 76 34 0908834

version 2024

- Planifier et mettre en œuvre les services de fichiers et de stockage
- Concevoir et mettre en œuvre une solution DHCP
- Concevoir et gérer une solution de gestion des adresses IP
- Mettre en œuvre une solution d'accès distant
- Concevoir et mettre en œuvre une solution de protection réseau
- Concevoir et mettre en œuvre une infrastructure de forêt et de domaine
- Concevoir une politique de stratégie de groupe
- Concevoir une stratégie de contrôleur de domaine
- Concevoir et mettre en œuvre une infrastructure pour une succursale
- Powershell
- Recommandations de sécurité
- Scénarios d'attaque classiques

Sécurité des systèmes et des réseaux

- Fondamentaux
- Architectures réseaux(rappels sur les réseaux IP, Couches OSI, Adressage, ARP, DNS, principales faiblesses de la pile TCP/IP, sécurisation des réseaux, les routeurs, virtualisation, équipements réseau, segmentation, filtrage, architecture (ANSSI)
- Périmètre (réseaux, systèmes d'exploitation, applications)
- Acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Risques, la protection, la prévention, la détection et la réaction

Durcissement Windows

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles
- Définir une politique de mises à jour sur les produits Microsoft
- Surveiller les mises à jour de sécurité des produits non-Microsoft
- Restreindre l'accès distant au parc Windows
- Mise en place d'alertes de sécurité sur le parc Windows
- Utilisation du pare-feu et d'un antivirus sur Windows
- Restreindre l'exécution des applications
- Utiliser les politiques de groupes (GPO)
- Auditer les politiques de groupes (GPO) avec Microsoft Security Compliance Manager
- Protection physique (clés USB, BIOS...)

Durcissement Linux

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles
- Définir une politique de mises à jour du noyau Linux
- Définir une politique de mises à jour des applicatifs tiers sur Linux
- Restreindre l'accès distant au parc Linux
- Mise en place d'alertes de sécurité sur le parc Linux avec un HIDS
- Utilisation du pare-feu et d'un antivirus Linux
- Restreindre l'exécution des applications et des commandes sur Linux
- Auditer les configurations

Mise en œuvre VPN

- Fondamentaux
- Mise en œuvre des différents types de VPN

Cryptographie

- Historique
- Introduction et enjeux de la cryptographie asymétrique
- Introduction au RSA, usage pour la distribution de clé et la signature
- Introduction à l'échange de clé Diffie-Hellman et aux courbes elliptiques.
- Génération des paramètres : nombres premiers, factorisation, etc.
- Cryptographie post-quantique

- Introduction et enjeux de la cryptographie symétrique
- Notions de chiffrement par blocs et chiffrement par flux

Mise en œuvre PKI

- Introduction
- Systèmes cryptographiques
- Infrastructure de gestion de clés
- Règles et recommandations générales

Virologie

- Introduction aux malwares (historique et évolution)
- Vecteurs d'infection
- Outils pour analyser les malwares