Sécurité Réseaux Microsoft

Format :
Présentiel et/ou Distanciel

Durée :
3 jours / 21 h

Référence :
PRO-SEC-0047

Public :
Techniciens et administrateurs réseaux.

Personnes en situation de handicap :
Vous êtes en situation de handicap et vous souhaitez faire une formation ?
Merci de bien vouloir nous contacter en amont afin d'étudier ensemble vos besoins et les solutions les plus adaptées.

Objectifs de développement des compétences :
Sécuriser une infrastructure Microsoft.

Pré-requis :
Avoir une connaissance du support technique des serveurs et postes de travail Microsoft.

Méthodes Pédagogiques mobilisées :
Les prestations de formation sont assurées par des formateurs professionnels qui utilisent des moyens pédagogiques adaptés.
Dans le cadre de session intra entreprise, possibilité de travailler sur vos projets afin de répondre à vos besoins spécifiques.
Supports de cours pédagogiques imprimés et/ou numérisés.

Répartition du temps (environ) :
Théorique 45%, Pratique 55%

Modalités d'évaluation :
Questionnaire d'auto-positionnement:
Un questionnaire d'auto-positionnement est adressé aux stagiaires en amont de la formation afin de l'adapter aux besoins et attentes des participants.

Évaluation à chaud par le biais de travaux pratiques.

- Exercices, tests d'évaluations (QUIZZ ou QCM ...).

Moyens techniques mobilisés :

Salle(s) de cours équipée(s) des moyens audiovisuels avec le matériel adapté à la formation (si besoin, ordinateur par stagiaire).

Modalité et délai d'accès à la formation :

Sur inscription.
UNIVERS FORMATION s'engage à prendre en charge votre demande sous un délai de 48h et à proposer des dates d'entrée en formation sous un délai de 15 jours, en fonction de vos disponibilités et de celles du formateur pressenti.
Votre rapidité de réponse sur toutes les questions administratives et questionnaires de positionnement permettra d'accélérer le démarrage de votre formation.

Tarif :

Nous contacter pour devis personnalisés.

Programme de la formation

1. Analyser les attaques

Expliquer les flux NTFS
Découvrir et définir les différents types de failles

2. Expliquer les méthodes d'intrusions utilisées

Analyser les ports pour identifier les services
Utiliser les failles de sécurité connues et inconnues ou les défauts de configuration
Attaquer la pile TCP/IP
Faire un déni de services
Intercepter et rechercher des mots de passe
Définir les différents types d'authentification
Utiliser les méthodes de capture et de recouvrement de mots de passe
Attaquer en brut force
Démontrer les méthodes : chevaux de Troie, RootKit et Backdoor
Gérer un proxy

3. Protection antivirale

Types de virus
Protection antivirale (précautions, antivirus scanner et/ou résidant, filtrage sur les pare feux et serveur de messagerie

4. Configurer des serveurs

Réduire la surface d'attaque par les serveurs core
Avoir des stratégies de mots de passe
Utiliser des outils sécurisant les mots de passe
Configurer les stations de travail et les applications : Office, navigateurs, client de messagerie

5. Configurer et installer des mises à jour

Installer Windows System Update Services
Utiliser les outils MBSA, et les scanneurs de vulnérabilités

6. Sécurisation des réseaux pour le transfert des données

Utilisation d'IPSec
Création de tunnels
Sécurisation d'un réseau Wifi avec une infrastructure de clépublique et serveur Radius

7. Sauvegarder et restaurer

Mettre en place une politique de sauvegarde et programmerles exécutions

8. Récupérer des données supprimées

Découvrir des outils fournissant un service de récupération

9. Crypter des fichiers et des disques

Définir EFS et Bitlocker
Configurer EFS et Bitlocker

Nous contacter :

UNIVERS FORMATION : 05 24 61 30 79

Version mise à jour le 24/07/2023