

Sécurité des réseaux

Référence : **SEC008**

Durée : **3 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- 1- Connaissances en réseau. • 2- Administration d'équipements réseau.

PROFIL DES STAGIAIRES

- 1- Administrateurs réseau / système. • 2- Techniciens réseau / système. • 3- Ingénieurs réseau / système.

OBJECTIFS

- Sécuriser les réseaux d'entreprise : Bien comprendre les vulnérabilités, Déployer des configurations robustes et appliquer les bonnes pratiques, Protéger efficacement les utilisateurs, Défendre les points d'entrée extérieurs, Configurer correctement les équipements de protection.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Présentation des enjeux de la sécurité des réseaux

Démonstration des attaques ciblant les équipements de niveau 2 et leurs contre-mesures

- ARP
- VLAN
- CDP
- Spanning Tree, etc.

JOUR 2

Attaque et protection des équipements et protocoles de niveau 3

- Ipv4 & Ipv6
- RIP
- OSPF
- EIGRP
- BGP

JOUR 3

Attaques et contre-mesures sur les passerelles virtuelles

- VRRP
- HSRP
- GLBP

Attaques et contre-mesures sur les VPN

Chiffrement des communications: utilisations et bonnes pratiques

Les outils de protection réseau

- Pare-feu
- IDS/IPS
- Serveur mandataire