

Introduction complète à la sécurité des réseaux

Objectif :

A la fin de cette formation, vous saurez :

- Evaluer la nature des risques introduits par les réseaux IP dans les SI,
- Vous approprier la terminologie et les concepts de la sécurité des réseaux IP,
- Mettre en oeuvre des équipements de sécurité.

Participants :

Décideur, architecte, administrateur réseaux et systèmes concernés par les problèmes de sécurité, Responsable de l'audit Informatique, Chef de Projet Informatique

Durée : 3 jours (21 heures) **Référence : RISR**

Contenu de la formation :

Concepts fondamentaux de la sécurité :

Protection de l'information,
Domaines de sécurité (physique, logique, réseaux, systèmes),

Transactions,

Problèmes de sécurité liés à IP (réseaux et applications),
Menaces, risques, vulnérabilités.

Types d'attaques :

Attaques passives, Attaques actives,
Parades aux attaques.

Services de sécurité :

Critères DICP,
Analyse de risques.

Technologies de Filtrage :

Principes,
Niveaux de filtrage : réseaux, applications, données,
FireWall/Proxy/ Anti-virus : principes, fonctions.

Technologies de scellement :

Intégrité des données

Algorithme de hachage (MD5, SHA-1, etc.).

Technologies de chiffrement :

Chiffrement symétrique,
Chiffrement asymétrique,
Infrastructure des clés publiques (PKI).

Architectures de sécurité :

VLAN,
Mode : bastion, DMZ, DMZ étendue,
VPN,
Etude de cas Internet/Intranet/Extranet : architectures, règles de sécurité.

Ipssec :

Fonctions de sécurité,
Architecture,
Modes : transport, tunnel,
Protocoles : AH, ESP,
Gestion des clés : IKE.

Protocoles de sécurité sur Internet/Intranet :

S-HTTP, S-MIME, SSL, PCT, TLS, PGP, etc., - RADIUS.

Dimension organisationnelle et juridique de la sécurité :

Conduire une Politique de sécurité réseau,
Aspects juridiques,
Projet sécurité.

TRAVAUX PRATIQUES :

*Mise en oeuvre de règles de sécurité au niveau FireWall et Proxy,
Déclenchement d'une attaque et parade associée, translation d'adresses, filtrage d'adresses réseau
via une ACL, filtrage applicatif via un proxy.*