

# SECURITE RESEAU

## OBJECTIFS

Implémenter une architecture réseau sécurisé, dans un environnement Windows/Linux.

Comprendre les problématiques liées aux attaques réseau.

Intégrer des outils de sécurité et de surveillance réseau.

Déployer des solutions Firewall, VPN, PKI, IDS, Proxy sous Linux et Windows.

## PARTICIPANTS

Ingénieurs, Techniciens, Administrateurs systèmes et réseaux.

## PRE-REQUIS

Connaissances de la suite des protocoles TCP/IP.

## METHODE PEDAGOGIQUE

Théorie : 50%

Pratique : 50%

## MOYENS PEDAGOGIQUES ET TECHNIQUES :

Salle informatique équipée pour 8 participants et son formateur.

Support de cours compris

## Architecture réseau sécurisée

### PROGRAMME

- ✓ Système Sécurisé : Définition / Méthodologie / Les patches de sécurité sous Windows, Solaris, Linux, HP-UX & Système BSD / Les logs sous Windows, Solaris & Linux
- ✓ L'authentification : Sous Windows : Active Directory / Sous Unix : LDAP + Samba
- ✓ Rendre plus sûr son système : L'antivirus / L'anti-spyware / Le firewall / Les alternatives / Hardening the OS
- ✓ Les dangers qui nous guettent : Les Trojans nouvelles versions / Les attaques connues / Le social engineering / La notion d'exploit / Les keyloggers / Les rootkits.
- ✓ Les attaques de type réseau : Recherche d'une cible / L'énumération / Les conséquences
- ✓ Les Firewalls d'entreprise (Considérations et mise en place) : Les méthodologies de Firewalling / ISA 2004 / Checkpoint / Les solutions libres / Les solutions avancée
- ✓ Les IDS : intrusion detection system : Principe de L'IDS / Les méthodes de détection / Les limites des IDS / Les techniques d'évasion / Installation et visualisation des logs avec SNORT
- ✓ Les PROXY : Proxy transparent sous Linux / Mise en place d'un proxy avec authentification sous ISA 2004
- ✓ Les protocoles réseaux courants contre les attaques : La DMZ / NAT / Port Forwarding / DNS interne / Les zones de décontamination / Cryptages du trafic
- ✓ PKI (Public Key Infrastructure)
- ✓ Les VPN

