La sécurité des réseaux TCP/IP

T130

Réf :	T130-030
Durée :	2 jours

Public

Equipes réseaux, systèmes, sécurité.

Vous serez capable de

Evaluer les risques internes et externes liés à l'utilisation de l'Internet.
Préserver votre réseau des attaques.
Garantir la disponibilité, la confidentialité et l'intégrité de vos données.

Pré-requis

Avoir des connaissances de base sur TCP/IP et maîtriser un système d'exploitation.

CONTENU PEDAGOGIQUE

Pourquoi sécuriser votre réseau d'entreprise

- Les risques, les attaques
- La dissimulations et vols de mots de passe
- Les virus, la propagation par e-mail
- Le cheval de troie
- La circulation des données dans l'entreprise
- D'où vient l'attaque : de l'extérieur ou de l'intérieur ?
- Quelques chiffres
  - Estimations de coûts d'immobilisation

Les risques inhérents à TCP/IP et à l'Internet

- La circulation des données en clair
- La substitution des adresses IP (IP spoofing)
- Les attaques par IP, ICMP, TCP, UDP
- Les failles connues des applications FTP, SMTP, DNS
- Risques liés aux réseaux locaux sans fils (802.11)

Ouvrir son réseau d'entreprise à l'Internet

- La gestion des adresses privées / publiques
  - RFC 1918
  - Masquer son plan d'adressage privé
  - Les translations d'adresses N vers 1 ou N vers N
- Les solutions routeur filtrant
  - Filtrage sur paquets IP (adressage)
  - Filtrage sur segment de transport (ports applicatifs)
  - Translation d'adresse NAT
  - Les solutions Firewall
  - Fonctionnalités des Firewalls
  - Firewall à état
  - Firewall matériel vs Firewall logiciel
  - Les firewalls tout en un
- Les solutions serveur Proxy
- Qu'est ce qu'un Proxy
- Qu'apporte un Proxy en terme de sécurité
- Où positionner un Proxy ?
- Complémentarité serveur Proxy/Firewall
- Les IDS/IPS
- DMZ
- Pourquoi une DMZ ?
- Comment créer une DMZ

Protéger les données de l'entreprise

- Confidentialité
- Signature
- Intégrité
- Non répudiation
- Infrastructure à clefs publiques (PKI)
- Exemple applicatif : SSL, EFS, IPSec etc.
- La cryptographie : jusqu'où peut on aller en France ?

Protéger le réseau local

- Architecture (VLAN etc.)
- Sécurisation de postes de travail
- Sécurisation des serveurs
- Politique anti-virale
- Chiffrement des données sensibles
- Sauvegarde
- Chiffrement des flux sensibles

Permettre l'accès à son réseau pour les utilisateurs nomades

- Accès via RTC ou Numéris
  - Avantages
  - Inconvénients
- Accès via GSM ou GPRS
  - Avantages
  - Inconvénients
- Sécurité de connexion
  - Call back
  - Authentification
- CHAP
- PAP
- SecureID
- Les réseaux privés Virtuels (VPN)
  - Avantages
  - Inconvénients
  - Techniques de VPN
- Site à site
- Nomade à site
- Protocole PPTP
- Protocole L2TP/IPSec
- VPN SSL
- Principe des VPN SSL
- Avantage
- Limitation
- Application Web
- Application métier
- Accès à sa messagerie de façon sécurisé via Internet

Bâtir son Intranet en utilisant un réseau public

- La sécurité des informations transportées
- Routeurs ou Firewall
- Les solutions VPN du marché

Les sites majeurs de la sécurité

- CERT, ITPRC etc.

Qu'apporte IPV6 en matière de sécurité ?