

Sécurité TCP/IP

Durée: 5 jours

Prix et dates: nous consulter

Public:

Toute personne souhaitant maîtriser la sécurité sur TCP/IP, et plus particulièrement les administrateurs et les architectes réseaux.

Objectifs:

Savoir mettre en œuvre les mécanismes de sécurité, analyser les traces, configurer les systèmes de protection, concevoir une architecture de réseau fiable.

Connaissances préalables nécessaires:

Il est demandé aux participants de connaître les bases de TCP/IP.

Programme:

- Introduction** : Analyse des risques.
Exemples avec l'étude des flux: tcpdump, sniffit,
TP: visualisation des mots de passe transitant par le réseau.
- Contrôle des accès système** : Protection de services réseaux: telnet, tftp, snmp, ftp, ...
Le 'tcp wrapper'
Verrouillage des accès physiques à distance.
Connexions sécurisée: SSH (configuration, connexion automatique), ssl, sftp, scp, tunneling X11
Contrôle de la messagerie: clamAV, p3scan, pop3s, imap4s
Gestion des accès: Radius
- Architecture de sécurité** : : Coupe feux: DMZ, Proxy. Pose de filtres sur un routeur.
TP: mise en place d'un proxy ftp
iptables, PAT, stunnel, VPN (openvpn, freeSWAN), VLAN
Les apports d'IPsec.
TP: mise en place d'une architecture openVPN
- Sécurisation échanges** : Chiffrage des données, mécanisme des certificats
- Surveillance** : Le protocole SNMP; la surveillance d'applications
TP: écriture d'un analyseur de topologie
Contrôle des flux. Analyseurs de trames: ethereal, tcpdump,
analyse de failles: nessus